A Guerra de Nova Geração Russa

Dissuasão e vitória no nível tático

James Derleth, Ph.D.

No século XXI, vemos uma tendência ao obscurecimento da linha divisória entre os estados de guerra e de paz.
[...]
As próprias "regras da guerra" mudaram. O papel de meios não militares na consecução de objetivos políticos e estratégicos cresceu, tendo, em muitos casos, ultrapassado o poder da força das armas em termos de sua eficácia.
[...]
Os engajamentos frontais entre grandes formações de forças nos níveis estratégico e operacional vêm sendo, gradativamente, relegados ao passado.
[...]
O emprego de ações assimétricas foi amplamente difundido, possibilitando a neutralização das vantagens de um inimigo em conflitos armados. Entre tais ações estão o uso de forças de operações especiais e da oposição interna para criar uma frente em operação permanente em todo o território do Estado inimigo e ações, dispositivos e meios informacionais em contínuo aperfeiçoamento.
[...]
As diferenças entre níveis estratégico, operacional e tático e entre as operações ofensivas e defensivas estão sendo eliminadas.

– General Valery Gerasimov,
Chefe do Estado-Maior Geral russo

A visão russa da dissuasão se baseia no emprego integrado de instrumentos não militares, convencionais e nucleares.[1] Em contrapartida, a concepção ocidental tradicional de dissuasão está alicerçada no desdobramento e emprego de forças convencionais e nucleares.[2] Uma diferença crucial é que a Rússia não acredita que a dissuasão cesse após a eclosão de um conflito. Ela continuará a empregar esses instrumentos ao longo de todas as fases de uma crise político-militar, na tentativa de controlar sua escalada e garantir condições favoráveis à Rússia. Portanto, para promover a dissuasão e prevalecer caso ela falhe, os Estados Unidos da América (EUA) devem ter a capacidade de enfrentar instrumentos em todas as áreas (não militar, convencional, nuclear), em todos os níveis (tático, operacional, estratégico) e ao longo de todas as fases de um conflito.[3] Embora enfrente desafios complexos, dinâmicos e em múltiplos domínios no atual ambiente operacional, o Exército dos EUA tem, de modo geral, concentrado seu sistema de instrução e treinamento em dissuadir e, se necessário, derrotar adversários com poder de combate quase equiparado em operações de combate em larga escala (*large-scale combat operations*, LSCO). Conforme se observou desde a Crimeia até a Geórgia, esse foco na dissuasão de nível mais elevado de forças convencionais e nucleares permitiu que a Rússia alcançasse seus objetivos nacionais por meio de uma variedade de instrumentos não letais.

Cabe observar que instrumentos não letais como a guerra de informação não foram integrados nos programas de instrução e treinamento do Exército dos EUA, como já é o caso de sistemas convencionais e nucleares. No entanto, tais instrumentos afetariam significativamente a capacidade das formações táticas para dissuadir ou vencer, no caso de um conflito.[4] Tradicionalmente, na doutrina militar estadunidense, as atividades de informação têm sido vistas como uma

"Tirei essa foto durante uma missão na nação da Geórgia, que coincidiu com o aniversário do Dia da Vitória na Europa. Em russo, perguntei aos pensionistas se falavam inglês. Não falavam. Perguntei, então, como podiam fazer um cartaz em inglês se não falavam a língua. Disseram que 'amigos' haviam feito os cartazes para eles. Para mim, é uma imagem muito poderosa, que mostra a extensão da guerra de informação russa. O que nossas forças fariam caso fossem confrontadas por esse grupo ao apoiarem a Geórgia em um conflito contra a Rússia?"

—James Derleth

Manifestação pró-Rússia e anti-OTAN no aniversário do Dia da Vitória na Europa, 9 de maio de 2019, em frente ao Museu Josef Stalin em Gori, na Geórgia. (Foto: autor)

função de apoio, facilitando e possibilitando as operações de combate. Em contrapartida, a Rússia sempre teve uma abordagem holística e integrada em relação à guerra de informação.[5] A revolução na tecnologia da informação só reforçou essa perspectiva. Os líderes militares russos acreditam que os combates decisivos de um conflito estão na dimensão, ou domínio, informacional e que as operações de informação nas fases iniciais são mais decisivas do que o combate convencional posterior. A guerra de informação, como forma decisiva de manobra, tem como alvo as vulnerabilidades e o centro de gravidade de um adversário, sendo as operações letais executadas para produzir um efeito informacional, em lugar de um efeito letal.[6] Dessa forma, os papéis das duas dimensões foram invertidos. Em vez de representarem uma operação de apoio, as campanhas de informação passaram a ser a operação apoiada.[7] Em consequência, a superioridade de informações é fundamental para aumentar a utilidade das ferramentas em todos os domínios durante todas as fases de um conflito.[8] Sem ela, é impossível obter êxito no combate.

A guerra de informação pode gerar ou tirar proveito do apoio militar e político local, desacreditar a liderança, retardar o processo decisório, fomentar a discordância, moldar a opinião pública, estimular ou manipular fontes locais de instabilidade e mobilizar populações locais contra forças estrangeiras. Tudo isso minimiza a probabilidade de confrontos letais ou melhora a probabilidade de êxito, caso eles ocorram.[9] Em suma, a guerra de informação pode ser o prelúdio de um conflito armado, uma preparação do campo de batalha que precede o desdobramento de forças ou um fim em si mesmo, por meio do qual a Rússia e outros adversários enfraquecem as forças superiores dos EUA sem disparar um tiro.

Embora a doutrina do Exército dos EUA assinale que "no conflito moderno, a informação passou a ser tão importante quanto a ação letal para determinar o resultado das operações", os integrantes de formações táticas têm uma capacidade limitada para compreender ou influenciar o ambiente informacional.[10] Observe-se que a doutrina se baseia no pressuposto de que a guerra de informação só será executada nos níveis operacional ou estratégico. Isso é questionável, considerando o atual ambiente de ameaças.[11] Como as formações táticas serão significativamente afetadas pela guerra de informação do inimigo independentemente da fase do conflito, elas devem ter a capacidade de entender e influenciar o ambiente informacional. Sem essa capacidade, os adversários continuarão a definir as condições da competição e conflito futuros.

A ameaça: um estudo de caso

Em uma eleição nacional na Estônia, o país assistiu a um partido nacionalista pró-estoniano assumir o controle do governo.[12] Frustrada com o resultado da eleição e sua falta de acesso à cidadania, a minoria étnica russa, que representava 20% da população, realizou manifestações contra o governo. O governo russo divulgou declarações de apoio; lançou uma campanha velada para moldar percepções com mais de 200 mil contas no Twitter, enviando 3,6 milhões de tuítes com a *hashtag* #protectRussiansinEstonia; e iniciou exercícios não anunciados de forças russas terrestres, navais e aéreas na região.

Uma semana depois, um grupo de manifestantes se reuniu na praça principal da cidade de Narva, no leste da Estônia, na fronteira com a Rússia. Reclamando que seus direitos humanos haviam sido violados, os manifestantes exigiram autonomia para Narva, status oficial para o idioma russo e cidadania estoniana. Quando a polícia estoniana chegou para dispersar a manifestação, ela foi confrontada por um grupo de homens armados em idade militar, falantes de russo. Temendo a morte de inocentes, a polícia deixou a área. Ao mesmo tempo, um grupo de manifestantes armados atacou o posto de controle de fronteira estoniano na divisa com a Rússia, obrigando que o abandonassem. Um terceiro grupo de manifestantes se apossou do centro de telecomunicações local (bloqueando o tráfego de internet, rádio, telefone e televisão para dentro ou fora de Narva), cercou a delegacia de polícia e invadiu a prefeitura, forçando o prefeito Tarmo Tammiste a renunciar. Georgi Zhukov, porta-voz dos manifestantes, declarou o estabelecimento da República Popular de Narva. Pediu à Rússia que lhes prestasse assistência "para garantir a paz e a ordem pública contra nacionalistas e fascistas". Essas ações foram apoiadas por uma série de ataques cibernéticos que sobrecarregaram as redes do governo, economia, imprensa, telecomunicações e forças armadas estonianas por todo o país. Os ataques cibernéticos incapacitaram o comando e controle do governo, bem como sua capacidade para se comunicar com sua população e aliados. Os ataques cibernéticos incluíram a divulgação de vídeos que, supostamente, mostravam forças de segurança estonianas massacrando habitantes estonianos de ascendência russa. Esses produtos proliferaram na internet por meio de bots, incitando opiniões antiestonianas e antiestadunidenses entre populações não alinhadas e favoráveis à Rússia em toda a Europa. O governo estoniano declarou ser ilegal a criação da República Popular de Narva, exigindo que devolvessem o controle às autoridades eleitas.

James W. Derleth, Ph.D., é assessor sênior de treinamento interagências no Joint Multinational Readiness Center em Hohenfels, na Alemanha. Suas responsabilidades incluem instruir e treinar militares e funcionários civis em guerra de nova geração russa, operações de estabilização e operações civis-militares; integrar desafios de segurança contemporâneos em exercícios; e interagir com missões diplomáticas, organizações internacionais e organizações não governamentais para integrá-las no treinamento. Concluiu o mestrado pela The American University e o doutorado pela University of Maryland em 1990.

Uma semana após o posto de fronteira ter sido abandonado, o setor de inteligência estoniano estimou que algumas centenas de pessoas vestindo fardas sem insígnia entraram na região a partir da Rússia. Em resposta, o governo da Estônia convocou uma reunião de emergência do Conselho do Atlântico Norte (CAN) para invocar a cláusula de defesa coletiva (artigo 5º) do Tratado do Atlântico Norte. O CAN recusou o pedido da Estônia devido à falta de clareza quanto à nacionalidade do grupo armado e à origem dos ataques cibernéticos. Apesar da recusa do CAN, os EUA concordaram em enviar o 2º Regimento de Cavalaria (2º RC) para a Estônia. Sua missão era apoiar o exército estoniano, as forças de segurança locais e o governo local na consecução destes quatro objetivos:

- preservar a integridade territorial estoniana;
- apoiar a legitimidade do governo estoniano;
- promover a segurança interna; e
- impedir a escalada do conflito.

Enquanto o 2º RC se preparava para sair de seu aquartelamento em Vilseck, na Alemanha, apareceram vários vídeos nas redes sociais, os quais supostamente mostravam atos de agressão sexual contra alemães menores de idade por militares estadunidenses. Os vídeos pareciam implicar alguns líderes-chave dentro do regimento, levando as autoridades políticas alemãs a exigir uma investigação. Manifestações dos cidadãos locais irromperam do lado de fora dos portões do aquartelamento do 2º RC, retardando o desdobramento da unidade.

Durante o deslocamento do 2º RC, houve ataques de guerra eletrônica (GE) contra sua rede de comunicações, que limitaram a capacidade de seus integrantes para se comunicar entre si e com as forças de segurança locais. Visando grupos antiguerra estadunidenses e europeus, contas "patrióticas" não rastreáveis em redes sociais publicaram vídeos que mostravam animais e plantações de moradores de etnia russa sendo atacados e a interrupção de serviços essenciais (água, eletricidade, saneamento) em Narva. Essas mensagens mudaram a opinião pública estadunidense e europeia, que passou de oposição à agressão ao apoio à cidadania e uso do idioma russo para a minoria residente na Estônia.

> Os papéis das duas dimensões foram invertidos [operações letais e operações de informação]. Em vez de representarem uma operação de apoio, as campanhas de informação passaram a ser a operação apoiada.

Após sua chegada à Estônia, o 2º RC se mudou para sua área de acantonamento em Jõhvi, 50 km a noroeste de Narva. No dia seguinte à chegada do 2º RC, um veículo aéreo não tripulado não identificado foi visto sobrevoando a base do regimento. Pouco depois, os integrantes do regimento perderam o acesso à rede local em seus celulares e começaram a receber mensagens de texto que lhes diziam para saírem da área para evitarem sua "destruição".

Em resumo, *antes* de o 2º RC chegar à área de acantonamento, o inimigo já havia executado operações em múltiplos domínios que estabeleceram sua superioridade de informações, geraram oposição local e internacional à presença do regimento, limitaram a capacidade deste para se comunicar com o governo local ou com suas formações, estimularam distúrbios civis e obtiveram o controle sobre infraestruturas essenciais. A operação decisiva de guerra de informação da Rússia começou quando o 2º RC, com suas limitadas capacidades, instrução e treinamento nessa área, chegou com suas formações focadas em ações letais. Em outras palavras, o 2º RC cedeu a iniciativa à Rússia antes mesmo de a primeira viatura Stryker sair pelo portão. Isso limitou, significativamente, o poder de combate do comandante do 2º RC e sua capacidade para executar a missão.

Essa não é uma ameaça hipotética! A relação entre guerra contemporânea e guerra de informação pode ser claramente vista na tomada da Crimeia pela Rússia em fevereiro de 2014. As ações de guerra de informação incluíram o envolvimento da população local por meio de entrevistas, "pesquisas de opinião", comícios de referendo e reuniões

pró-Rússia; disseminação em massa de cartazes, panfletos, folhetos e mensagens de texto; corte de cabos de fibra óptica; tomada de controle do ponto de troca de tráfego de internet da cidade de Simferopol; desativação das instalações de canais de televisão ucranianos, substituindo-os por canais russos; ataques de guerra eletrônica contra sistemas de comunicações militares ucranianos; desfiguração de sites ucranianos e da Organização do Tratado do Atlântico Norte (OTAN); divulgação de gravações telefônicas e e-mails entre autoridades da Ucrânia, União Europeia e EUA; criação de sites falsos em que a Rússia visou organizações militares ucranianas utilizando as contas de redes sociais de seus integrantes; utilização de sites reais (Facebook, Twitter, Odnklassniki, Vkontakte) para espalhar o pânico e boatos; e ataques distribuídos de negação de serviço em que se enviaram milhares de mensagens de texto e chamadas telefônicas para os celulares de líderes militares e civis, a fim de impedi-los de se comunicar e responder às ações russas. Essa superioridade de informações também garantiu que apenas informações provenientes de fontes russas estivessem disponíveis, levando uma parcela significativa da população a acolher as tropas russas. Essas atividades, aliadas a ações não letais de reconhecimento e desestabilização por forças especiais *Spetsnaz*, enfraqueceram o moral e a eficácia de combate das forças armadas ucranianas, levando à rendição de 16 mil soldados.[13] Esse foi um excelente exemplo de um caso em que operações em múltiplos domínios se estenderam por todo o espectro informacional. Em consequência, a Rússia conseguiu manipular as percepções ucranianas, prevenir uma resposta militar, influenciar seu processo decisório, fomentar a desconfiança no governo e limitar seu comportamento estratégico, minimizando, ao mesmo tempo, o emprego de força letal.

Desafios

O Exército dos EUA se deu conta, tardiamente, do desafio representado pela guerra de próxima geração e está reorganizando seu Comando Cibernético (*Army Cyber Command*) com o objetivo de sincronizar as capacidades da Força para "mudar a forma pela qual conduzimos a Guerra de Informação".[14] Isso será realizado por meio da "integração e emprego de capacidades de inteligência, de operações de informação, cibernéticas, de guerra eletrônica e espaciais para oferecer aos comandantes de comandos geográficos conjuntos opções para competir abaixo do nível do conflito armado".[15] Embora esses sejam objetivos importantes, existem muitos desafios para implementar essa diretriz no nível tático. Com base em observações realizadas no Centro de Prontidão Multinacional Conjunto (*Joint Multinational Readiness Center*, JMRC) em Hohenfels, na Alemanha, os desafios incluem a falta de entendimento do ambiente informacional; não integração desse ambiente no processo operacional; incapacidade de integrar multiplicadores de força; coordenação ineficaz com parceiros civis; relutância em reconhecer que as ações físicas têm efeitos informacionais; e inexistência de doutrina, instrução e treinamento que permitam que as formações mitiguem ações inimigas a fim de recuperar a iniciativa tática e operacional.

Falta de entendimento do ambiente informacional. Embora sejam hábeis em identificar ameaças letais, as formações têm um entendimento limitado de ameaças não letais, que podem ter um impacto ainda maior sobre a manobra. Os futuros conflitos ocorrerão em meio a uma população conectada, em um complexo ambiente informacional. Caso não se melhore a consciência situacional, o poder de combate será degradado. Embora os comandantes precisem compreender e influenciar o ambiente informacional, a seção de estado-maior encarregada de entender o ambiente operacional (inteligência) se concentra em grupos e ações inimigas que possam ter consequências letais. Em consequência, o ambiente informacional é negligenciado. Os comandantes não estabelecem necessidades de inteligência prioritárias nem usam modelos padronizados para entender o ambiente informacional. Eles justificam isso simplificando o espaço de combate e empregando uma visão limitada da pior hipótese possível, em que forças inimigas excedem suas formações. Infelizmente, o conflito moderno não é um simples questão de 'ou isso ou aquilo'. As formações que não entendem o ambiente informacional ficam 'cegas' quanto ao modo como são vistas pela população e retratadas pelo inimigo. Essa cegueira limita a capacidade da formação para obter informações sobre forças e posições inimigas e identificar apoiadores ou forças de operações especiais do inimigo atrás do

"Homenzinhos verdes" da Rússia facilitaram a anexação da península ucraniana da Crimeia, em fevereiro de 2014. Munidos com modernas armas portáteis e equipamentos russos, esses efetivos eram uma mistura de forças especiais e outras unidades de elite russas, que vestiam fardas verdes sem identificação. A Rússia alegou, inicialmente, que os "homenzinhos verdes" eram milícias patrióticas ucranianas locais, favoráveis às reivindicações russas em relação à Crimeia. Eles tomaram e ocuparam o parlamento em Simferopol e várias bases militares na Crimeia, além de bloquear o Aeroporto Internacional de Simferopol para impedir a chegada de forças do governo ucraniano. Simultaneamente, a Rússia conduziu uma ampla campanha global de guerra híbrida, utilizando uma grande variedade de instrumentos, incluindo diplomacia, guerra econômica, guerra eletrônica, ataques cibernéticos, propaganda e violência concentrada, para alcançar seus objetivos. As contramedidas e respostas ocidentais têm sido, de modo geral, ineficazes contra o "fato consumado" russo. (Captura de tela de Hromadske.tv)

espaço onde as tropas terrestres operam. A título de ilustração, para proteger suas comunicações durante um exercício recente no JMRC, uma unidade em rodízio (*rotational unit*, RTU) decidiu usar a rede sigilosa (*Secret Internet Protocol Router Network,* SIPRNet) como seu principal meio de comunicação. Como resultado, embora pudesse se comunicar com segurança internamente, ela não tinha nenhum entendimento do ambiente local, porque os sistemas de informação não classificados haviam sido negligenciados. Essa falta de entendimento resultou em manifestações locais, que obstruíram as estradas principais de suprimento da unidade, e em pessoas deslocadas internamente, que interferiram em sua manobra. Além disso, fez com que se abrisse mão de uma riqueza de informações aproveitáveis colhidas por pessoas deslocadas internamente, à medida que fugiam do inimigo. Essa falta de visibilidade e entendimento do ambiente informacional afetou diretamente o poder de combate da RTU.

Não integração do ambiente informacional no processo operacional. O objetivo do processo operacional, conforme indicado na Publicação Doutrinária do Exército 5-0, *O Processo de Operações* (ADP 5-0, *The Operations Process*), é entender, visualizar e descrever o ambiente operacional; tomar e apresentar decisões; e direcionar, liderar e avaliar operações militares.[16] As observações extraídas de

exercícios no JMRC continuam mostrando que as formações táticas não conseguem integrar um entendimento do ambiente informacional nas operações. Isso resulta do fato de os comandantes não entenderem o ambiente informacional ou de enxergarem suas ações somente por um prisma físico.[17] Essa falta de entendimento é agravada por uma estrutura de estado-maior centrada em plataformas, letalidade e sistemas de armas inimigos. Por exemplo, um estado-maior pode, facilmente, visar uma formação de carros de combate do inimigo, mas tem dificuldade em fazer o mesmo com uma página de rede social do inimigo que esteja incitando manifestações nas estradas principais de suprimento. Em consequência, as formações não conseguem identificar ou apoiar capacidades relacionadas à informação (CRI) de forças amigas, identificar e atacar CRI inimigas ou integrar essas informações nas operações e planos. Isso faz parte de um desafio institucional maior: a ideia de que a "vitória" só pode ser alcançada com operações de combate letais.

Incapacidade de integrar multiplicadores de força. A doutrina do Exército dos EUA enfatiza a responsabilidade dos comandantes por operar em todos os domínios, incluindo o ambiente informacional. No entanto, as formações táticas carecem de muitas CRI orgânicas. Quando desdobradas, as formações táticas recebem multiplicadores de força, como elementos de assuntos civis (As Civ) e de operações psicológicas (Op Psc). No entanto, esses e outros multiplicadores de força (oficiais de comunicação social [Com Soc], oficiais de guerra eletrônica, etc.) são, muitas vezes, incapazes de influenciar o ambiente informacional. Existem várias razões para essa situação, mas duas se destacam:

1. Os multiplicadores de força não operam junto às formações táticas até o momento de um exercício ou desdobramento. Por não serem elementos orgânicos para o estado-maior e terem tido poucas interações com ele, é um desafio para eles integrar seu conhecimento do ambiente operacional nas operações. Isso resulta, em parte, do fato de que as áreas de adestramento das sedes não reproduzem o ambiente informacional multifacetado e dinâmico dos conflitos modernos. Normalmente, os comandantes criam suas próprias forças oponentes, que não têm as capacidades de guerra de informação do inimigo. Assim, eles não entendem como os multiplicadores de força podem facilitar suas operações. A consequência: unidades que vivem, comem e respiram letalidade na sede são imersas em ambientes realistas radicalmente diferentes durante os exercícios ou desdobramentos. No entanto, elas têm pouco ou nenhum treinamento para vencer nesses ambientes.
2. Os multiplicadores de força não geram produtos ligados à intenção do comandante e aos objetivos operacionais. Muitas vezes, os produtos dos multiplicadores de força estão vinculados à sua especialização operacional específica, em vez de estarem ligados aos estados finais de um comandante.[18] Por exemplo, o anexo de assuntos civis que deveria, segundo a doutrina, "descrever como as operações de assuntos civis, em coordenação com outras organizações militares e civis, apoiam o conceito da operação descrito no plano básico ou ordem" muitas vezes apenas relaciona as considerações civis (área, estruturas, capacidades, organizações, população e eventos).[19] Como os comandantes não veem como esses aspectos estão ligados à sua intenção, os multiplicadores de força frequentemente recebem outras atribuições, como, por exemplo, proteger o centro de operações táticas ou instalar obstáculos. Um desafio relacionado é a incapacidade dos multiplicadores de força para saírem de seus 'compartimentos de excelência'. No JMRC, observamos, com frequência, que, por definirem suas missões de uma forma restrita, as CRI (As Civ, Com Soc, Op Psc, etc.) não sincronizam suas atividades, limitando seus efeitos. Em comparação, a 77ª Brigada do Reino Unido combina essas capacidades em equipes de informação, atividade e difusão que "apoiam os objetivos militares dos comandantes [...] utilizando engajamentos não letais e instrumentos não militares legítimos como meio de adaptar comportamentos das forças oponentes e adversários".[20]

Coordenação ineficaz com parceiros civis. A guerra de informação russa está centrada em deslegitimar as estruturas militares e políticas dos adversários. No entanto, devido aos prazos operacionais, competência técnica limitada e falta de autoridade legal, as formações táticas estadunidenses

são incapazes, muitas vezes, de mitigar os efeitos de guerra de informação do inimigo. Para minimizar essas limitações, faz-se necessária uma abordagem do 'governo como um todo' (*whole-of-government*). Entidades internacionais, organizações não governamentais, governos locais, meios de comunicação e agências de marketing podem apoiar e/ou executar atividades de informação táticas. A incapacidade das formações táticas para identificar parceiros civis e integrar os conhecimentos e experiência deles nas operações limita a capacidade para manobrar e consolidar ganhos. Embora existam inúmeras razões para essa situação, os principais fatores incluem a não identificação de parceiros civis no ambiente operacional e a falta de entendimento de suas capacidades.

Relutância em reconhecer que a guerra de informação afeta a manobra. Houve uma mudança drástica nas operações militares contemporâneas em decorrência da globalização, difusão de tecnologias militares e revolução da informação. Apesar disso, a ênfase atual em LSCO tem levado os comandantes a se concentrar nos aspectos de manobra das operações ofensivas e defensivas. Embora a manipulação de informações possa gerar efeitos de negação de área e represente, segundo a doutrina, uma forma de fogos, os comandantes não têm aplicado os necessários recursos de estado-maior e ênfase da liderança ao aspecto cognitivo das operações.[21] Essa falta de recursos aplicados pode ter inúmeras consequências, que limitam a capacidade de conduzir operações em múltiplos domínios. Isso inclui permitir que o inimigo estabeleça as condições, neutralizar a superioridade militar, limitar a capacidade de empregar a força e gerar uma imagem negativa perante públicos amigos e inimigos.

Falta de instrução e treinamento contra guerra de nova geração. Os programas de instrução e treinamento tradicionais e contemporâneos do Exército dos EUA se concentram em operações de combate de grande porte contra forças armadas de um Estado com poder de combate equiparado ou quase equiparado. Não obstante, apesar da falta de êxito no Vietnã, Afeganistão, Iraque, Líbia, Mindanao (Filipinas), Síria e região do Sahel, ainda persiste a crença de que, se o Exército dos EUA puder executar LSCO eficazmente, ele poderá vencer qualquer conflito. Há três falhas significativas nesse modo de pensar. Em primeiro lugar, como esses conflitos demonstraram, aplicar a instrução e o treinamento sobre LSCO a operações de outra natureza sempre requer uma extensa e dispendiosa adaptação, pondo em risco o sucesso da missão. Em segundo lugar, existe a suposição comum de que o próximo confronto será um conflito convencional entre grandes potências. Conforme o ex-Secretário de Defesa James Mattis gostava de ressaltar, o inimigo também é um fator de influência. Cientes de que suas forças armadas não têm condições de vencer em um combate convencional contra os EUA, adversários como China, Irã e Rússia vêm investindo fortemente em recursos assimétricos para explorar as vulnerabilidades estadunidenses. Em terceiro lugar, o desejo do Exército dos EUA de se concentrar em ameaças tradicionais não muda o fato de que vários atores não estatais continuam a fomentar distúrbios por todo o mundo, prejudicando a estabilidade regional e ameaçando os interesses estadunidenses. Os dados mostram que os atuais conflitos armados são, em sua maioria, conflitos civis ou subestatais internacionalizados, em lugar de guerras interestatais convencionais.[22]

Para vencer os futuros conflitos, o Exército dos EUA deve rever seus programas de instrução e treinamento. Embora alguns centros de treinamento de combate tenham criado e integrado um ambiente informacional complexo e dinâmico em seus exercícios, ele é frequentemente ignorado, ou seu valor é minimizado, para que ele não "interfira em outros objetivos de treinamento". Em consequência, as RTUs não têm tido uma experiência realista de treinamento. Uma boa regra básica para medir o progresso seria analisar se uma unidade está investindo uma quantidade igual ou maior de recursos em operações de ambiente informacional em comparação com suas operações físicas. Embora fosse ser uma medida de desempenho em lugar de uma medida de efeito, isso pelo menos forçaria os comandantes a tentar integrar as operações de ambiente informacional no planejamento.[23]

Outro desafio é a falta de instrução sobre medidas contra guerra de nova geração, para treinar comandantes a obter o êxito contra operações em múltiplos domínios como a anexação da Crimeia pela Rússia. Além de um curso criado no JMRC, o autor não tem conhecimento de nenhum outro nos EUA ou na OTAN que treine formações táticas a neutralizar táticas de guerra de nova geração.

Especialistas em operações cibernéticas do Destacamento de Apoio Cibernético Expedicionário do 782º Batalhão de Inteligência Militar (Cibernético) conduzem operações cibernéticas ofensivas como parte do programa de atividades de apoio cibernético/eletromagnético nos escalões corpo de exército e abaixo, em 18 de janeiro de 2018, durante o rodízio da 1ª Brigada de Combate Stryker, 4ª Divisão de Infantaria, Rodízio 18-03 do Centro Nacional de Treinamento, em Fort Irwin, Califórnia. (Foto: Steven Stover, Com Soc, 780ª Brigada de Inteligência Militar)

Entender e influenciar o ambiente informacional

Embora muitos desses desafios sejam fruto de decisões e políticas formuladas em escalões mais elevados, as formações táticas terão de lidar com suas ramificações. Assim, o que poderão fazer para vencer no atual ambiente informacional? Muito pode ser feito em relação a isso, incluindo a instrução na sede, integração de multiplicadores de força no Programa de Treinamento de Liderança, análise do ambiente informacional pré-desdobramento, modificação da organização por tarefas, integração de parceiros civis nos processos de estado-maior, colocação de um oficial mais antigo a cargo da integração de multiplicadores de força e parceiros civis e envolvimento do comandante.

Instrução na sede. Percebendo que as RTUs não contam com treinamento contra guerra de nova geração, o JMRC criou um programa de instrução de três dias e uma equipe móvel de treinamento para apresentá-lo nas sedes. Infelizmente, a maioria recusou a oportunidade, o que significa que elas têm pouca ou nenhuma experiência em entender o ambiente operacional ou em sobrepujar ameaças não letais antes do desdobramento para centros de treinamento ou missões no mundo real. As formações que não treinam para contingências realistas se colocam em uma posição de enorme desvantagem. Como na situação durante as guerras no Afeganistão e no Iraque (quando uma equipe móvel de treinamento em operações contrainsurgência foi enviada para toda brigada a ser desdobrada), uma simples solução seria exigir que cada RTU realizasse o treinamento contra guerra de nova geração ou um curso regional equivalente antes de prosseguir para um centro de treinamento de combate. Isso é especialmente importante, uma vez que a guerra de nova geração se baseia em um estado de conflito permanente.

Alunos da disciplina eletiva presencial A350, Aplicação Tática da Ação Decisiva, planejam operações de combate em larga escala em um exercício de sala de aula, 14 de maio de 2019, no Command and General Staff College (CGSC), em Fort Leavenworth, Kansas. Persiste a crença de que o Exército poderá vencer qualquer conflito se puder executar operações de combate em larga escala com eficácia. (Foto: M. Shane Perkins, instrutor do CGSC)

Integração de capacitadores[NT] no Programa de Treinamento de Liderança. Como muitos dos multiplicadores de força fazem parte da reserva, eles frequentemente não são incluídos nos Programas de Treinamento de Liderança das RTUs. Portanto, eles só começam a atuar junto à unidade apoiada ao serem desdobrados. Isso faz com que seja difícil para eles sincronizar suas atividades com os estados-maiores de brigada e demonstrar seu valor para comandantes focados em ameaças letais. Para mitigar esse desafio, o 353º Comando de Assuntos Civis determinou que (1) todas as suas formações realizassem o curso contra guerra de nova geração do JMRC antes do desdobramento para o teatro de operações do Comando Europeu e que (2) representantes do batalhão sendo desdobrado participassem de conferências de planejamento do rodízio e do Programa de Treinamento de Liderança. Isso lhes permite começar a operar junto à unidade apoiada mais cedo e demonstrar seu valor à equipe.

Análise do ambiente informacional pré-desdobramento. Da mesma forma que devem identificar formações inimigas no ambiente operacional antes do desdobramento, as unidades também devem identificar operações de informação do inimigo que tenham influenciado esse ambiente antes de chegarem. No mínimo, essa análise deve incluir as principais CRI das forças aliadas e inimigas, informações sobre como o inimigo está influenciando o ambiente operacional, possíveis linhas de ação para neutralizar atividades inimigas que possam afetar as operações de combate e medidas de efeito que mostrem o êxito de operações de contrainformação.

Modificação da organização por tarefas. Como o ambiente informacional é global e em constante evolução, compreendê-lo é um desafio mais complexo que entender o ambiente físico. Assim, é preciso dedicar mais recursos de estado-maior para entender o ambiente informacional. Concentrar-se no "efeito" a ser obtido (por exemplo, degradar o poder de combate do inimigo, promover a liberdade de manobra e enfatizar as necessidades de inteligência prioritárias relacionadas à informação) facilitará a mudança. Durante uma análise pós-ação do ambiente operacional, o comandante da RTU que

[NT: Cabe observar que, por vezes, os capacitadores podem ser entendidos como "multiplicadores do poder de combate", por vezes, como "elementos em reforço". Meios associados à Inteligência, Operações Psicológicas, Assuntos Civis, Operações Especiais, Guerra Eletrônica, Guerra Cibernética, dentre outros, são, frequentemente, citados como capacitadores, segundo uma perspectiva mais ortodoxa das operações de combate em larga escala.]

usou a SIPRNet como seu meio de comunicação percebeu que isso teve inúmeras consequências imprevistas que limitaram seu poder de combate. Para mitigar esse problema, o comandante criou uma "célula de engajamento", incluindo não apenas os elementos habituais (oficiais de Com Soc, As Civ, GE, Op Psc), mas também oficiais de inteligência e operações. A célula de engajamento incluiu integrantes do estado-maior para garantir que as informações dos demais elementos fossem incorporadas no planejamento e seleção de alvos. Para promover a integração e melhorar a capacidade de visar ameaças não letais, o comandante também fez com que a equipe móvel de treinamento do JMRC desse o curso sobre medidas contra guerra de nova geração à célula.

Integração de parceiros civis nos processos de estado-maior. Por já estarem atuando nas áreas para onde a unidade será desdobrada, os parceiros civis terão contatos, conhecimentos especializados e capacidades locais para moldar ou se opor a tentativas de moldar o ambiente informacional. No entanto, essa oportunidade é frequentemente desperdiçada porque as formações não identificam ou integram os parceiros civis nas operações. Uma maneira simples de mitigar esse desafio é garantir que eles sejam incluídos nos processos de estado-maior. Por exemplo, segundo a doutrina, deve haver um Grupo de Trabalho de Operações de Informação (*Information Operations Working Group*, IOWG) na brigada. A integração no IOWG permitiria aos parceiros civis identificar a narrativa do inimigo e criar mensagens para neutralizá-la, bem como identificar objetivos não letais para o processo de seleção de alvos. O envolvimento de parceiros civis nas operações também pode ser facilitado por meio da estrutura de fogos existente. Quando os comandantes querem produzir efeitos letais, eles simplesmente informam ao coordenador de apoio de fogo o efeito que querem alcançar. O sistema já bem estabelecido executa, então, a tarefa. Se os comandantes fornecessem a mesma diretriz para efeitos não letais/informacionais — e considerando que as brigadas não dispõem de capacidades no espaço informacional —, o coordenador de apoio de fogo teria de usar os parceiros civis e multiplicadores de força para obter o efeito desejado.

Colocação de um comandante mais antigo a cargo de atividades não letais. As RTUs que tiveram mais êxito em operações em múltiplos domínios incumbiram um oficial de escalão mais elevado — geralmente o subcomandante ou oficial executivo da brigada — de supervisionar a integração das informações nas operações. Embora outros oficiais de estado-maior decerto sejam capazes, eles não têm o grau hierárquico para integrar multiplicadores de força e parceiros civis nas operações de brigada.

Envolvimento dos comandantes. O modo mais importante de vencer a guerra de informação é fazer com que comandantes em todos os escalões saibam que esse tipo de combate é de sua responsabilidade. Eles precisam entender como o ambiente informacional pode facilitar — ou limitar — sua capacidade de conduzir as operações em múltiplos domínios necessárias para alcançar os estados finais desejados. Um bom ponto de partida seria avaliar comandantes não apenas com base em suas pontuações em técnica de tiro, mas também quanto à sua capacidade para executar operações em múltiplos domínios no ambiente operacional contemporâneo.

Resumo

A dicotomia 'guerra e paz' já não é um conceito útil para se pensar sobre segurança nacional ou operações táticas. Estamos em um estado de competição e conflito que é contínuo e dinâmico. Conforme demonstrado por uma série de adversários, eles podem alcançar seus interesses nacionais abaixo do limiar de conflito por meio de operações não letais centradas na guerra de informação. Em um artigo publicado na revista militar russa *Military Thought*, I. Vorobyev e V. Kiselyov observaram: "A informação agora é um tipo de arma. Não apenas complementa ataques de fogos e manobras, mas os transforma e os une". Assim, "a informação vem se transformando em *uma luta armada por si só* [grifo no original]".[24] Para derrotar ameaças multidimensionais, as formações táticas dos EUA devem ser capazes de entender e influenciar o ambiente informacional. Apesar de ter se dado conta, tardiamente, da existência do espectro de competição/conflito informacional, o Exército dos EUA tem concentrado sua atenção e recursos em apoio às LSCO.[25] No entanto, a natureza das ameaças emergentes (por exemplo, fogos de precisão de longo alcance, sistemas de defesa antiaérea em múltiplas camadas, drones, guerra eletrônica, ataques cibernéticos, etc.) indica que as futuras operações militares serão conduzidas por unidades táticas. É por isso que, ao contrário da política estadunidense, a Rússia tem modificado sua estrutura de força, passando de divisões para formações de escalões mais baixos (brigadas e batalhões). A Rússia acredita que o êxito no atual ambiente operacional requer que as formações de escalões mais baixos tenham

certa autonomia e capacidade para executar várias missões, porque os fatores citados anteriormente limitarão seriamente a possibilidade de que os escalões superiores lhes apoiem. Isso inclui "subunidades de guerra psicológica e de confronto informacional."[26] Até que o Exército dos EUA reconheça que o espaço informacional não é apenas uma dimensão de conflito, mas também o centro de gravidade, enfrentaremos duas claras alternativas: tolerar desafios não convencionais ou escalar tais desafios até o nível de conflito armado. Isso deixa os EUA em uma posição de enorme desvantagem contra adversários que têm utilizado a informação como arma para influenciar e moldar interações em diferentes domínios em apoio à manobra tática integrada de armas combinadas. ■

Referências

Epígrafe. Valery Gerasimov, "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", *Voyenno-Promyshlennyy Kurier* (Military-industrial courier), 26 February 2013, acesso em 12 maio 2020, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf. [NT: O artigo traduzido, intitulado "O Valor da Ciência está na Previsão: Novos Desafios Exigem Repensar as Formas e Métodos de Conduzir as Operações de Combate", consta da edição brasileira de março-abril de 2016 da *Military Review*, https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese/MilitaryReview_20160430_art009POR.pdf.]

1. Russian Federation Ministry of Defence, *Military-Encyclopedic Dictionary* (2015), acesso em 28 maio 2020, http://encyclopedia.mi1.ru/encyclopedia/dictionaryIdetails_rvsn.htm?id=14206@morfDictionary, cited in K. Ven Bruusgaard, "Russian Strategic Deterrence", *Survival: Global Politics and Strategy* 58, no. 4 (2016). Veja também Okke Geurt Lucassen, "In Between War and Peace: The Conceptualization of Russian Strategic Deterrence", UPTAKE Working Paper No. 16/2018 (Tartu, Estonia: University of Tartu Press, 2018), p. 10, acesso em 28 maio 2020, http://www.uptake.ut.ee/wp-content/uploads/2019/03/Okke_Lucassen_WP2.pdf. A dissuasão estratégica "é o conjunto de instrumentos, que utilizam o poder de influência (*soft power*) e poder coercitivo (*hard power*), mediante o emprego de ferramentas de (des)informação, cibernéticas, econômicas, militares e políticas, tanto ofensiva quanto defensivamente, de modo contínuo, independentemente de ser tempo de paz ou guerra, em busca de prevenir conflitos violentos, reverter a escalada de conflitos militares (ou cessá-los no início) ou estabilizar situações político-militares em (potenciais) (coalizões de) Estados de interesse adversários, em condições favoráveis para a Federação Russa".

2. Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

3. Gerasimov, "The Value of Science Is in the Foresight". Gerasimov observa que as operações contemporâneas seguem uma proporção de aproximadamente 4:1 de medidas não militares para medidas militares, com a competição não militar sob o controle de formações militares, que utilizam operações de informação, organizações militares privadas, forças de operações especiais e potencial interno para protestos. Essa perspectiva tem duas ramificações significativas. Primeiro, o Ocidente considera as medidas não militares como formas de evitar a guerra, enquanto a Rússia as considera armas de guerra (veja Charles Bartles, "Getting Gerasimov Right", *Military Review* 96, no. 1 [2016]: p. 34). [NT: O artigo traduzido, intitulado "Para Entender Gerasimov", consta da edição brasileira de março-abril de 2016, https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese/MilitaryReview_20160430_art010POR.pdf.] Segundo, as formações táticas enfrentarão vários desafios não letais, que afetarão seu poder de combate e capacidade de manobra.

4. Veja Catherine Theohary, "Information Warfare: Issues for Congress", Congressional Research Service (CRS) Report No. R45142 (Washington, DC: CRS, 2018), acesso em 28 maio 2020, https://crsreports.congress.gov/product/pdf/R/R45142/5. Ao contrário das operações de informação, a guerra de informação não está definida na doutrina militar estadunidense. Este artigo utiliza 'guerra de informação' para descrever a execução de ações ofensivas e defensivas na dimensão informacional, destinadas a obrigar adversários a se submeter à vontade de um ator por meio do emprego de operações cibernéticas, operações psicológicas, guerra eletrônica, segurança de operações e dissimulação militar.

5. "Convention on International Information Security", Ministry of Foreign Affairs of the Russian Federation, 27 September 2011, acesso em 20 maio 2020, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666. Veja também *On Russia's Information War Concepts before the House Armed Services Subcommittee on Emerging Threats and Capabilities*, 115th Cong., 1st sess. (2017) (statement of Timothy Thomas), acesso em 20 maio 2020, https://docs.house.gov/meetings/AS/AS26/20170315/105689/HHRG-115-AS26-Wstate-ThomasT-20170315.pdf. Um documento sobre estratégia russo de 2011, "Convention on International Information Security" ("Convenção sobre Segurança de Informação Internacional", em tradução livre), define guerra de informação como um "conflito entre dois ou mais Estados no espaço informacional com o objetivo de causar danos a sistemas, processos e recursos de informação, bem como a estruturas de vital importância e de outra natureza; minar sistemas políticos, econômicos e sociais; realizar campanhas psicológicas em massa contra a população de um Estado para desestabilizar a sociedade e o governo; e forçar um Estado a tomar decisões no interesse de seus oponentes". No campo militar, o objetivo da guerra de informação é (1) alcançar objetivos políticos sem o emprego da força militar e (2) promover uma resposta internacional favorável ao desdobramento de suas forças militares ou de forças militares aliadas a Moscou. As "armas" informacionais são a tecnologia, meios e métodos utilizados na guerra de informação.

6. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: U.S. Government Printing Office, 2012, incorporating Change 1, 2014), p. ix. Segundo a doutrina, as operações de

informação são "o emprego integrado, durante operações militares, das capacidades relacionadas à informação [CRI], em conjunto com outras linhas de operações, para influenciar, desorganizar, corromper ou usurpar o processo decisório dos adversários e potenciais adversários, ao mesmo tempo protegendo o nosso". De acordo com essa definição, as operações de informação se concentram na coordenação e sincronização apenas durante operações militares, dependendo de outras capacidades para produzir efeitos. Monica Ruiz, "Impacts of Russian Information Operations: Technical and Psychological Aims", International Centre for Defence and Security, 24 October 2017, acesso em 13 maio 2020, https://icds.ee/impacts-of-russian-information-operations-technical-and-psychological-aims/. Em contrapartida, a abordagem holística da Rússia em relação à guerra de informação está dividida em dois componentes: "informacional técnico", que se alinha com a definição ocidental de guerra eletrônica e cibernética e se concentra em capacidades técnicas; e "informacional psicológico", que se assemelha ao conceito da OTAN de comunicações estratégicas e operações psicológicas, centrado nas operações de influência.

7. Keir Giles, "Delivery of Information Effects by Russian Special Forces and Intelligent Agencies" (versão preliminar).

8. Sergei Modestov, "Strategicheskoe sderzhivanie na teatre informatsionnogo protivoborstva", *Vestnik Akademii Voennykh Nauk*, no. 1 (2009): p. 26, cited in Dmitry (Dima) Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy", Proliferation Papers 54 (Paris: Institut français des relations internationales [ifri], November 2015), acesso em 13 maio 2020, https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf. Na perspectiva russa, a campanha de informação obscurece a linha entre guerra e paz, frente e retaguarda, níveis de guerra (tático, operacional, estratégico), formas de guerra (ofensiva e defensiva) e formas de coerção (dissuasão e compulsão).

9. Veja Adamsky, "Cross-Domain Coercion", p. 24; Gerasimov, "The Value of Science is in the Foresight"; Margarita Jaitner, "Russian Information Warfare: Lessons from the Ukraine", in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO Cyber Defence Centre of Excellence, 2015), p. 91, acesso em 13 maio 2020, https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf. Isso pode ser realizado com desinformação, notícias falsas, ataques cibernéticos, sabotagem digital, etc. A importância de obter a superioridade de informações na guerra pode ser vista com base no tempo e na quantidade de recursos que foram gastos na criação de fontes oficiais, semioficiais e não oficiais de informações relacionadas à guerra, incluindo canais dedicados no YouTube.

10. Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 2017), para. 2-113. Para obter informações adicionais, veja JP 3-13, *Information Operations*, p. ix-x.

11. Não está claro como ataques cibernéticos, guerra eletrônica, fogos de precisão de longo alcance, drones, etc., permitiriam que os escalões superiores se comunicassem, e muito menos executassem operações de guerra de informação taticamente relevantes.

12. Adaptado de "Weaponized Information: One Possible Vignette", *Mad Scientist Laboratory* (blog), U.S. Army Training and Doctrine Command, 7 November 2019, acesso em 13 maio 2020, https://madsciblog.tradoc.army.mil/190-weaponized-information-one-possible-vignette/.

13. Veja Vladimir Sazonov, Kristiina Müür, and Igor Kopõtin, "Methods and Tools of Russian Information Operations Used Against Ukrainian Armed Forces: The Assessment of Ukrainian Experts", ENDC Occasional Papers No. 6/2017 (Tartu, Estonia: Estonian National Defence College [ENDC], 2017): p. 59; Oscar Jonsson and Robert Seely, "Russian Full Spectrum Conflict: An Appraisal After Ukraine", *Journal of Slavic Military Studies* 28, no. 1 (2015): p. 15; Jaitner, "Russian Information Warfare: Lessons from the Ukraine", p. 91; Gleb Pakharenko, "Cyber Operations at Maidan: A First-Hand Account", in Geers, *Cyber War in Perspective*, p. 61; Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: RAND Corporation, 2017), p. 5-31, acesso em 13 maio 2020, https://www.rand.org/pubs/research_reports/RR1498.html.

14. Uma observação sobre definições. Ameaças contemporâneas emergentes e um tanto ambíguas, muitas das quais ficam aquém do limiar historicamente considerado como "guerra", têm sido denominadas como guerra híbrida (EUA e OTAN), guerra de nova geração (Rússia), guerra além dos limites (China) e competição na zona cinza (vários). A falta de uma definição comum permite que várias entidades escolham a que se encaixe em sua visão de mundo ou missão burocrática. Isso permite a justificação de noções preconcebidas e, o que é mais importante, limita nosso entendimento das ameaças reais. Na tentativa de mitigar esse desafio, este artigo utiliza as seguintes definições:

Ameaça híbrida. A Publicação Doutrinária do Exército 3-0, *Operações* (ADP 3-0, *Operations*), descreve ameaça híbrida como "uma combinação variada e dinâmica de forças regulares, forças irregulares, elementos criminosos ou uma combinação dessas forças e elementos, todos unificados para a obtenção de efeitos mutuamente benéficos". Cabe observar que essa perspectiva se concentra em ameaças militares, não em um tipo de guerra, e que ameaças híbridas podem ser derrotadas pelo emprego do poder militar. Army Doctrine Publication (ADP) 3-0, *Operations* (Washington, DC: U.S. GPO, 2019), 1-3.

Guerra de nova geração. A guerra de nova geração busca produzir resultados políticos ou militares sem recorrer abertamente a meios militares convencionais, embora estes últimos não estejam excluídos. Na guerra de nova geração, o principal espaço de combate é a mente. Como resultado, o conflito contemporâneo é dominado pela guerra de informação, com o objetivo de obter a superioridade por meio da desmoralização moral e psicológica dos efetivos militares e da população civil de um inimigo antes e, se necessário, durante as hostilidades. Isso reduz a necessidade de empregar o poder militar letal, fazendo com que as forças armadas e a população do adversário apoiem o atacante em detrimento de seu próprio governo. Em consequência, os russos colocaram a ideia de influência no cerne de seu planejamento operacional. Esse fato é relevante para se entender sua importância estratégica, uma vez que a operacionalização da guerra de nova geração não pode ser caracterizada como uma estratégia militar no sentido ocidental tradicional. Por exemplo, a guerra híbrida pode fazer parte da guerra de nova geração, mas não deve defini-la. Essa descrição se baseia em ações russas na Ucrânia, bem como discursos e trabalhos de líderes militares e pesquisadores russos. Veja Jānis Bērziņš, "Not 'Hybrid' but New Generation Warfare", in *Russia's Military Strategy and Doctrine*, ed. Glen E. Howard and Matthew Czekaj (Washington, DC: Jamestown Foundation, 2019), acesso em 13 maio 2020, https://jamestown.org/wp-content/uploads/2019/02/Russias-Military-Strategy-and-Doctrine-web.pdf?x30898&x87069; veja Gerasimov, "The Value of Science is in the Foresight"; S. G. Chekinov and S. A. Bogdanov, "On the Nature and Content of a New-Generation War", *Voennaia Mysl* [Military Thought], no. 10 (2013), acesso em 13 maio 2020, https://pdfs.semanticscholar.org/c887/4593b1860de12fa40dadcae8e96861de8ebd.pdf.

Guerra além dos limites. A "guerra além dos limites" se baseia na crença de que a globalização funciona como um multiplicador de força para métodos não militares menos tradicionais, como

guerra diplomática (estabelecimento de alianças), guerra econômica (sanções comerciais), guerra cibernética (ataques de hackers) ou guerra ambiental (desastres naturais provocados pelo homem). Assim, para alcançar objetivos estratégicos, a China deve ir além do espectro de poder da força puramente militar e operar em múltiplos domínios. Em 2003, a China publicou "Diretrizes de Trabalho Político do Exército de Libertação Popular". O documento descreve "três guerras", que devem ser empregadas em tempo de paz e em operações militares. A primeira, "guerra psicológica", é a aplicação de pressão militar, diplomática e econômica para enfraquecer a vontade dos adversários. A segunda, "guerra da opinião pública", concentra-se na manipulação aberta ou secreta de informações para influenciar os públicos internacional e nacional. A terceira, "guerra jurídica", refere-se à exploração das normas internacionais para alcançar os objetivos chineses. Veja Nan Li, "Unrestricted Warfare and Chinese Military Strategy" (Singapore: Institute of Defence and Strategic Studies, 2002), acesso em 28 maio 2020, https://www.rsis.edu.sg/wp-content/uploads/2014/07/CO02022.pdf; Sergio Miracola, "Chinese Hybrid Warfare", Italian International Institute for Political Studies, acesso em 13 maio 2020, https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853.

Competição na zona cinza. Esse conceito é definido como "atividades secretas ou ilegais de uma arte de governar não tradicional, que estão abaixo do limiar da violência organizada armada, incluindo a ruptura da ordem, subversão política de organizações governamentais ou não governamentais, operações psicológicas, abuso de processos legais e corrupção financeira como parte de um projeto integrado para obter a vantagem estratégica. Essa competição entre e dentro de atores estatais e não estatais se enquadra entre a dualidade tradicional de guerra e paz, caracterizando-se pela ambiguidade sobre a natureza do conflito, falta de transparência das partes envolvidas e incerteza sobre os arcabouços políticos e jurídicos relevantes". Observe-se que todas as três descrições incluem a competição de zona cinza. Veja Frank Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges", *Prism* 7, no. 4 (2018): p. 36; Philip Kapusta, "The Gray Zone", *Special Warfare* 28, no. 4 (October-December 2015): p. 18-25, acesso em 13 maio 2020, https://www.soc.mil/SWCS/SWmag/archive/SW2804/GrayZone.pdf.

Resumo. Ao contrário das descrições russas e chinesas da guerra contemporânea — que se baseiam em operações em múltiplos domínios facilitadas pela guerra de informação, que ocorre, simultaneamente, de forma aberta e secreta abaixo do tradicional limiar de guerra —, a visão dos EUA está centrada em ameaças militares visíveis, que possam ser derrotadas mediante o emprego do poder militar. Conforme observa Frank Hoffman, a adoção dessa limitada concepção convencional de conflito não prepara futuros líderes para a variedade de ameaças emergentes. Também não é propícia à formulação de doutrina e treinamento: "Um foco míope em ameaças convencionais obscurece a complexidade dos fenômenos e simplifica em excesso os desafios. Pode também ser uma forma de enfatizar uma missão preferida, ligada a um paradigma de guerra convencional de grande porte, que limita nossa compreensão cognitiva de conflito". Frank G. Hoffman, "Hybrid Warfare and Challenges", *Joint Force Quarterly*, no. 52 (2009, 1st Quarter): p. 34-59, acesso em 13 maio 2020, https://smallwarsjournal.com/documents/jfqhoffman.pdf.

15. Sydney Freedberg Jr., "The Golden 5 Minutes: The Need for Speed in Information War", Breaking Defense, 21 October 2019, acesso em 13 maio 2020, https://breakingdefense.com/2019/10/the-golden-five-minutes-the-need-for-speed-in-information-war/.

16. Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: U.S. GPO, 2019), p. v.

17. "Information Warfare Foundational Study (Working Draft)" (Fort Gordon, GA: U.S. Army Cyber Command, 10 July 2019), p. 8.

18. Jen Judson, "Army Learning How Cyber Support Plays Role in Tactical Operations", DefenseNews, 10 November 2015, acesso em 13 maio 2020, http://www.defensenews.com/story/defense/land/army/2015/11/10/army-learning-how-cyber-support-plays-role-in-tactical-operations/75545442/. Durante um exercício-piloto, em que se buscou incorporar o apoio cibernético em uma brigada de infantaria, um observador afirmou que "apesar de termos fornecido pessoas muito hábeis em questões técnicas, elas não foram capazes de se comunicar com o comandante e com o estado-maior da brigada em termos que eles pudessem compreender facilmente nem explicar quais recursos estávamos oferecendo e qual a melhor forma de integrar tais capacidades".

19. FM 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. Government Printing Office, 2014), Annex D.

20. "77th Brigade Influence and Outreach", British Army, acesso em 13 maio 2020, https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/. A 77ª Brigada, formada em 2015, conjuga elementos da ativa e reserva do Exército. Suas missões incluem a análise de público, atores e adversários, atividades e difusão de informação, medidas contra atividades de informações de adversários, apoio a parceiros civis, coleta de conteúdo de mídia, divulgação de mídia, monitoramento do ambiente informacional, avaliação do ambiente informacional, assessoramento e treinamento em segurança humana (enfatizando a segurança das pessoas e seu ambiente social e econômico, em lugar da segurança do Estado) e fornecimento de apoio às operações correntes.

21. *DOD Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense [DOD], 2020), acesso em 13 maio 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf. Ações tomadas no ciberespaço que criem efeitos de negação observáveis (ou seja, degradação, desorganização ou destruição) ou a manipulação que leve à negação na dimensão física são consideradas uma forma de fogos.

22. Alexandra Evans and Alexandra Stark, "Bad Idea: Assuming the Small Wars Era is Over", Defense 360, Center for Strategic and International Studies, 13 December 2019, acesso em 14 maio 2020, https://defense360.csis.org/bad-idea-assuming-the-small-wars-era-is-over/.

23. "Information Warfare Foundational Study", p. 35.

24. I. Vorobyov and V. Kiselyov, "Russian Military Theory: Past and Present", *Military Thought* 22, no. 1 (2013): p. 56.

25. Por exemplo, o Exército dos EUA planeja criar dois novos batalhões integrados de inteligência, informação, cibernética, guerra eletrônica e área espacial, para ajudar a moldar o ambiente operacional, monitorizar fluxos de informação e conduzir operações de informação ou missões cibernéticas.

26. "В Белоруссии начались учения 'Нерушимое братство-2016'" [In Belorussia begins the exercise Unbreakable Brotherhood 2016], RIA, 23 August 2016, acesso em 14 maio 2020, https://ria.ru/world/20160823/1475032583.html, cited in Giles, "Delivery of Information Effects by Russian Special Forces and Intelligent Agencies". Exercícios consecutivos em 2016 incluíram a utilização de "subunidades de guerra psicológica e confronto informacional".