

As Ações e Métodos Russos contra os EUA e a OTAN



Maj Collins Devon Cockrell, Exército dos EUA

A Rússia tem tentado derrubar a ordem europeia pós-Guerra Fria com uma agressiva campanha de guerra de informação nos últimos anos — a ponto de o documento *European Command Posture Statement* (“Relatório de Situação do Comando dos EUA para a Europa”, em tradução livre) de 2017 identificar a Rússia como principal ameaça, afirmando que ela “busca enfraquecer o sistema internacional e desacreditar aqueles que o criaram no Ocidente”¹. Em janeiro de 2017, o Alte Esq (Reserva) James Mattis, então nomeado como Secretário de Defesa, declarou que a Rússia era a ameaça número um aos Estados Unidos da América (EUA) e estava empenhada em um contínuo esforço para “romper a aliança do Atlântico Norte”². Em seu discurso em Munique, em 2007, o Presidente Vladimir Putin declarou que a Rússia ia executar uma política externa que não reconheceria mais um sistema unipolar liderado pelos EUA³. Putin afirmou, publicamente, que o Ocidente, especificamente os EUA, estava tentando transformar a Rússia em um fraco Estado “vassalo” e impedindo que ela reivindicasse seu lugar de herdeira do papel de contrapeso da União Soviética no mundo⁴. Pode-se resumir a visão de mundo hiperbólica e agressiva da elite governante russa com os comentários, segundo noticiados, de Andrey Krutskikh, assessor sênior do Presidente Putin, em uma conferência em Moscou, em fevereiro de 2017:

Vocês acham que estamos vivendo em 2016. Não, nós estamos vivendo em 1948. E sabem por quê? Porque, em 1949, a União Soviética conduziu seu primeiro teste com a bomba atômica. E se, até aquele momento, a União Soviética estava tentando

chegar a um acordo com o [Presidente Harry] Truman para proibir as armas nucleares e os norte-americanos não estavam nos levando a sério, em 1949, tudo mudou e eles começaram a falar conosco em pé de igualdade⁵.

Como reflexo direto disso, a Rússia vem intervindo em sistemas políticos por toda a Europa a fim de desestabilizar tanto os Estados democráticos mais recentes quanto os já consolidados. O objetivo declarado de Putin é a restauração da “Grande Rússia”⁶. Este artigo apresenta uma breve visão geral das doutrinas de Operações de Informação (Op Info) dos EUA e da Organização do Tratado do Atlântico Norte (OTAN), comparando-as com uma análise atual dos conceitos russos de guerra de informação⁷. Essa visão geral visa a esclarecer o leitor acerca de importantes diferenças

O Maj Collins Devon Cockrell, do Exército dos EUA, é o Oficial de Operações do 7º Grupo de Operações Psicológicas, em Mountain View, na Califórnia. Possui os títulos de mestrado em Ciência Política pela University of Arkansas e mestrado em Arte e Ciência Militar pelo U.S. Army Command and General Staff College, em Fort Leavenworth, no Kansas. Serviu, anteriormente, como coordenador de curso e instrutor do Curso de Qualificação para Oficiais de Operações Psicológicas no John F. Kennedy Special Warfare Center and School, em Fort Bragg, na Carolina do Norte; em missões na Coreia; e em missões no Iraque, como engenheiro, em 2004, e como comandante de destacamento de operações psicológicas, em 2009.

em doutrina, capacidade e propósito, de modo que os atores ocidentais tenham um sólido entendimento, como base para a tomada de decisões.

A doutrina dos EUA define Operações de Informação como “o emprego integrado, durante as operações militares, das capacidades relacionadas à informação [CRI], em conjunto com outras linhas de operações, para influenciar, abalar, corromper ou usurpar o processo decisório dos adversários e potenciais adversários, ao mesmo tempo protegendo o nosso”⁸. Essas CRI incluem as Operações de Apoio à Informação (Op Ap Info) [military information support operations — MISO], Operações Cibernéticas, Guerra Eletrônica (GE), Dissimulação Militar, Operações Civil-Militares e Comunicação Social⁹. Como uma função de coordenação no campo de disseminar e moldar informações, a Op Info é uma parte essencial de todas as operações ofensivas, defensivas e de estabilização. Na doutrina norte-americana, o esforço principal de influenciar os públicos-alvo estrangeiros fica a cargo das forças de Operações Psicológicas (Op Psc) que desempenham as Op Ap Info. Segundo a doutrina, as forças de Op Psc ficam incumbidas de:

elaborar e transmitir mensagens e conceber ações para influenciar grupos estrangeiros específicos e promover temas para mudar as posturas e comportamentos desses grupos. As Op Ap Info também podem degradar o poder de combate do inimigo, reduzir a interferência civil, minimizar os danos colaterais e aumentar o apoio da população às operações¹⁰.

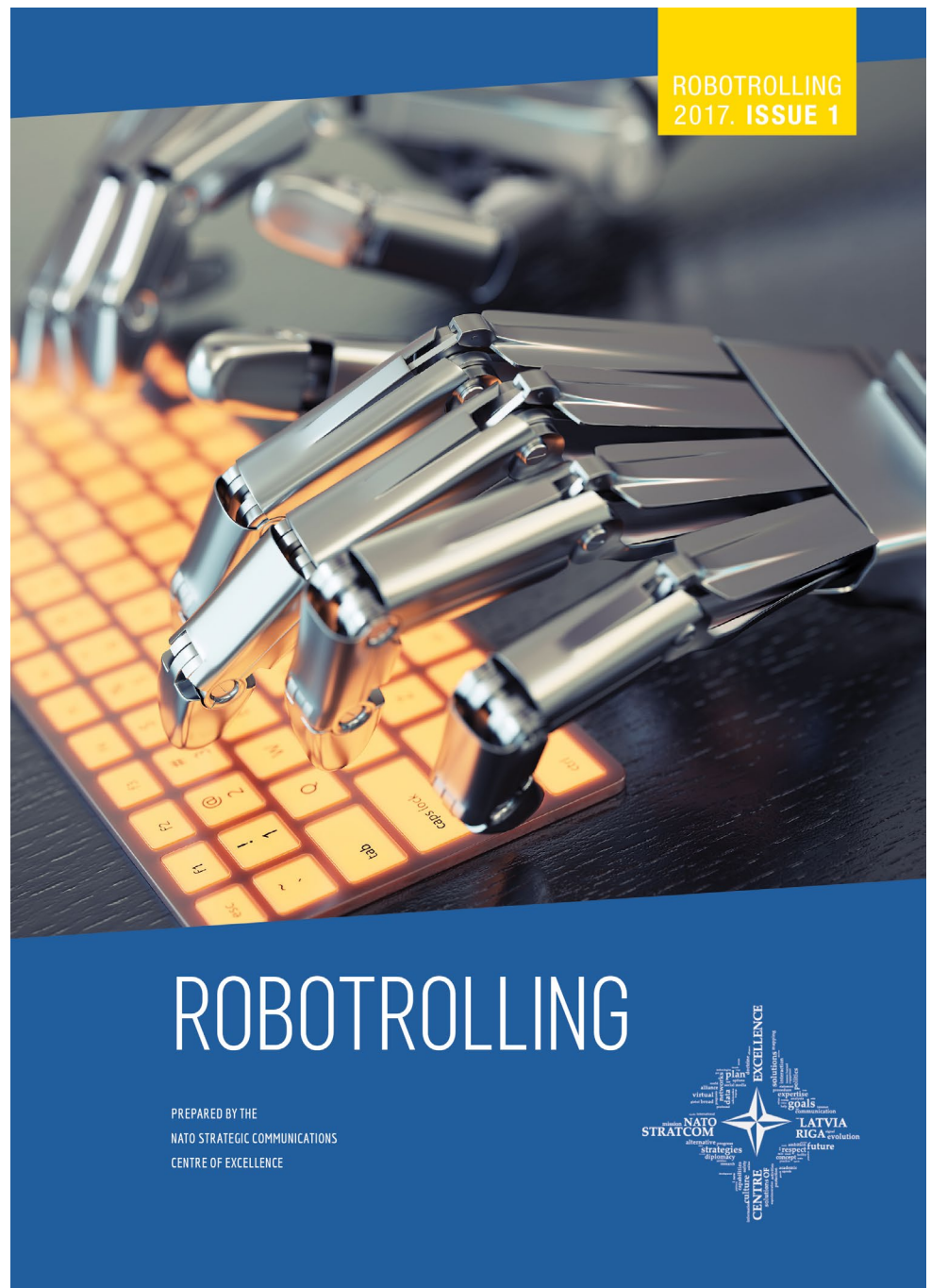
As ações e programas de Op Info dos EUA e do Ocidente para responder às ações russas têm aumentado desde a anexação da Crimeia, tomada da Ucrânia. Os Estados-membros da OTAN reconheceram a crescente ameaça dos esforços russos para influenciar questões políticas internas e exacerbar divisões. Contudo, esses programas ocidentais são de uma ordem inferior à atividade russa, devido ao poder da influência corruptora da Rússia. Uma parte central da estratégia dos EUA e da OTAN consiste no apoio e desenvolvimento de organizações que analisam ameaças na dimensão informacional e fazem recomendações aos governos, forças armadas e coalizões ocidentais. Por exemplo, em 2014, a OTAN aprovou o estabelecimento do Centro de Excelência de Comunicações Estratégicas da OTAN (StratCoE) em

Riga, na Letônia¹¹. Essa organização está encarregada de combater o extremismo violento e a influência hostil, especialmente na área dos Estados Bálticos. Ela produziu uma grande quantidade de análises das atividades russas em todo o continente. Embora não seja uma parte formal da estrutura de comando da OTAN, o StratCoE serve como um tipo de instituição de pesquisa sobre influência para a organização, incumbido de “contribuir para o processo de comunicação da Aliança por meio do fornecimento de análises detalhadas, assessoramento oportuno e apoio prático [...]”¹². Tem como foco entender o extremismo e as influências hostis, assim como apoiar o plano de comunicações estratégicas do Comitê Militar da OTAN e a doutrina da Aliança. Um dos mais notáveis pesquisadores trabalhando para organismos da OTAN, Keir Giles também elaborou análises oficiais da organização, incluindo o documento “Handbook of Russian Information Warfare” (“Guia sobre a Guerra de Informação Russa”, em tradução livre), de 2016¹³. O StratCoE é um efetivo apoio aos membros da OTAN com respeito a questões relacionadas ao extremismo e a ações russas contra a Europa.

A doutrina da OTAN sobre Op Psc se enquadra na doutrina de Op Ap Info dos EUA. Emprega termos semelhantes para conceitos-chave, como *target audience analysis*, ou “análise do público-alvo”, o processo analítico pelo qual se identifica a população ou grupo mais útil para se obter uma mudança comportamental em apoio aos requisitos da missão e contribuir aos objetivos do comandante¹⁴. As limitações à capacidade da OTAN para responder às ações russas não representam uma deficiência doutrinária, e sim o problema de 29 Estados-membros terem de coordenar uma única e oportuna resposta em um ambiente informacional extremamente mutável. Salvo em caso de uma declaração de hostilidades contra membros da OTAN, os processos para ações de Estados-membros por meio dos comitês militares que coordenam as atividades não têm como se equiparar à ação unificada da ditadura russa. Os Estados-membros da OTAN reconheceram a crescente ameaça dos esforços russos para influenciar suas questões políticas internas e exacerbar divisões. Em seu depoimento perante a Comissão de Inteligência do Senado dos EUA, em junho de 2017, Constanze Stelzenmüller, da entidade Brookings Institution, afirmou que o objetivo da guerra de informação russa

é “desestabilizar o projeto europeu de dentro para fora: dismantlar décadas de progresso rumo à construção de uma Europa democrática completa, livre e pacífica”¹⁵. Em abril de 2017, nove Estados-membros da União Europeia e da OTAN concordaram em criar uma organização combinada para a cooperação ativa no “combate à guerra híbrida”, com sede em Helsinque¹⁶. A atual lei National Defense Authorization Act (“Lei de Autorização da Defesa Nacional”, em tradução livre) autoriza um “Fundo de Combate à Influência Russa” de US\$ 80 milhões, para apoiar “organizações da sociedade civil e outras entidades”¹⁷. Houve uma controvérsia após essa ação do Congresso de exigir uma iniciativa específica do governo dos EUA, porque o Departamento de Estado se recusou, até agosto de 2017, a fornecer um plano para empregar as verbas por meio de seu Global Engagement Center¹⁸.

Dessa e de outras formas, os Estados aliados europeus e da OTAN vêm coordenando suas respostas a esse conflito em curso com a Rússia na dimensão informacional. Contudo, as estratégias de coalizões são bem mais difíceis de executar que as de um ator unificado e autoritário como a Rússia. Além disso, o elemento essencial da doutrina de influência e Op Psc dos EUA e da OTAN está centrado na exigência de que as mensagens persuasivas a serem disseminadas se baseiem em informações verdadeiras



A foto da capa da primeira edição da revista *Robotrolling* 2017, do Strategic Communications Centre of Excellence, da OTAN, representa, visualmente, a ascensão da automação nas mídias sociais. O Strategic Communications Centre of Excellence é uma de dezenas de instituições dedicadas à busca e análise de informações para assistir os membros da OTAN em seu complexo processo decisório. (Imagem de *Robotrolling* 1 [2017], acesso em 8 set. 2017, <http://www.stratcomcoe.org/robotrolling-20171>.)

para influenciar o público-alvo. Como afirma o manual da OTAN, as “Op Psc devem se basear em informações verdadeiras. A utilização de informações falsas é

contraproducente para a credibilidade e sucesso de longo prazo das Op Psc¹⁹. Isso representa tanto um ponto forte quanto uma limitação. O ponto forte é a credibilidade e o poder que isso transmite, mas a limitação é que a Rússia não tem essas restrições às suas campanhas de influência.

A visão da Rússia sobre esse tipo de guerra é de que ela pode começar antes que hostilidades tenham início. Conforme citado por Keir Giles em sua monografia para o NATO Defense College, “Handbook of Russian Information Warfare”:

Os russos utilizam informações desde um estágio oculto, passando por seis fases de guerra, até o restabelecimento da vitória. O confronto informacional é conduzido em todas as fases, incluindo secretamente, na paz e na guerra. Nossas doutrinas não nos permitem fazer muitas dessas coisas até que o combate, basicamente, comece²⁰.

O Presidente Putin e seus estrategistas militares baseiam suas ações no que, na Rússia, é denominado “guerra de nova geração”. No documento *Doutrina Militar da Federação Russa*, publicado pela primeira vez em 2000, os “russos reconheceram a necessidade de que suas forças armadas operassem no ‘espaço informacional’ e a existência de ‘ameaças informacionais’ diante do Exército russo”²¹. Para os EUA e a OTAN, “guerra híbrida”, assim como “guerra de informação”, é o termo mais comumente empregado por analistas militares e civis para descrever as atividades russas. A doutrina dos EUA afirma que “uma *ameaça híbrida* é a combinação diversificada e dinâmica de força regulares, forças irregulares e/ou elementos criminosos: todos unificados para obter efeitos mutuamente benéficos”²². Essa definição condiz com a concepção russa de guerra de nova geração. Cabe notar que a visão russa sobre esse tipo de guerra diverge da noção de guerra assimétrica como ferramenta de um oponente intrinsecamente fraco contra um mais forte. A Rússia vira o conceito de ponta-cabeça em relação aos antigos Estados soviéticos. Emprega esses métodos híbridos contra Estados mais fracos ou de poder de combate equivalente para alcançar objetivos da política externa ou militares. Tem como objetivo obter resultados políticos decisivos com pouco ou nenhum poder militar, mas está pronta para empregar a força militar sobrepujante, se necessário²³. Dessa forma, uma Aliança

como a OTAN está em desvantagem, não só porque consiste em uma estrutura de coalizão, mas porque esses métodos híbridos ou assimétricos são mais difíceis de classificar como tendo cruzado o limiar de um verdadeiro “ataque” contra um Estado-membro.

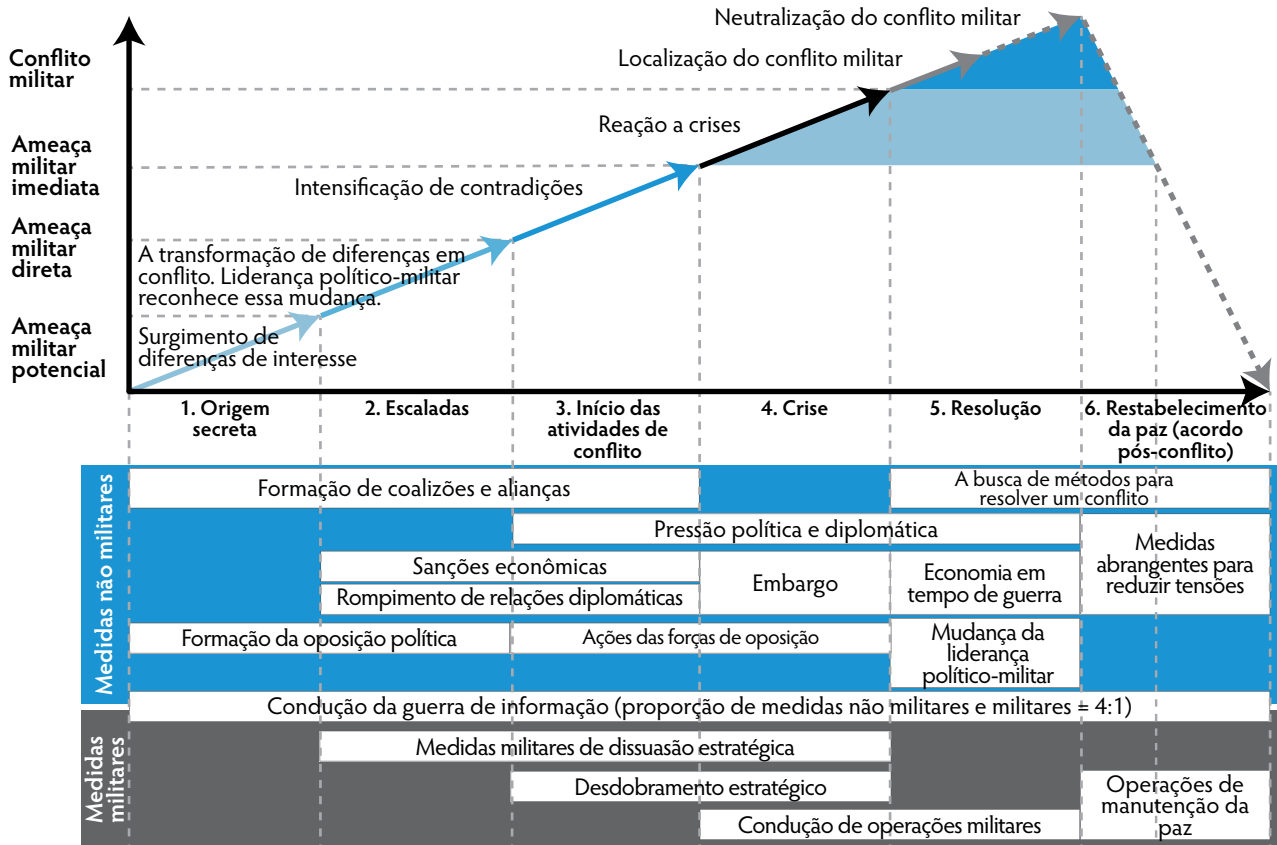
Desde 2012, a estratégia militar da Rússia está centrada na “Doutrina de Gerasimov”, extraída de uma série de discursos e declarações do General Valery Gerasimov, Comandante do Exército Russo. As ideias do General Gerasimov são sua síntese de um tipo de guerra não convencional ou guerra assimétrica. Esse método visa a criar uma “oposição interna” viável dentro de um Estado²⁴. Esse processo faseado da guerra irregular russa, descrito na figura 1, é descrito de modo convincente por Charles K. Bartles, no artigo “Getting Gerasimov Right”, de 2016²⁵. [A versão em português, intitulada “Para Entender Gerasimov”, consta da edição brasileira de março-abril de 2016 da *Military Review* — N. do T.] Também foi citado no documento “*Little Green Men: A Primer on Modern Russian Unconventional Warfare*” (“Homenzinhos Verdes”: Fundamentos da Guerra Não Convencional Russa Moderna”, em tradução livre), do Comando de Operações Especiais dos EUA, publicado em 2016²⁶.

Como afirmou Gerasimov:

As próprias “regras da guerra” mudaram. O papel de meios não militares para a consecução de objetivos políticos e estratégicos cresceu, tendo, em muitos casos, ultrapassado o poder da força das armas em termos de sua eficácia²⁷.

A abordagem de Gerasimov quanto à coordenação de ações econômicas, diplomáticas e políticas, aliadas à força militar, assemelha-se ao antigo termo “guerra política” para defini-las. É um termo que surgiu durante a Segunda Guerra Mundial, mas está sendo usado novamente pela comunidade de operações especiais dos EUA²⁸. A estratégia militar russa prevê ações dirigidas contra países estáveis, que podem ser, então, rapidamente desestabilizados com o emprego de ações não militares²⁹. Os métodos russos se concentram em identificar as fraquezas e divisões internas do Estado visado e em explorá-las para enfraquecer sua sociedade. Essas ações podem incluir o “envolvimento do potencial de protesto da população, Forças de Operações Especiais e medidas secretas militares e de guerra de informação”³⁰.

Principais Fases (Estágios) do Desenvolvimento do Conflito



(Imagem do National Security Analysis Department, "Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014, Assessing Revolutionary and Insurgent Strategies Study [unclassified working draft, Fort Bragg, NC: U.S. Army Special Operations Command], p. 18.)

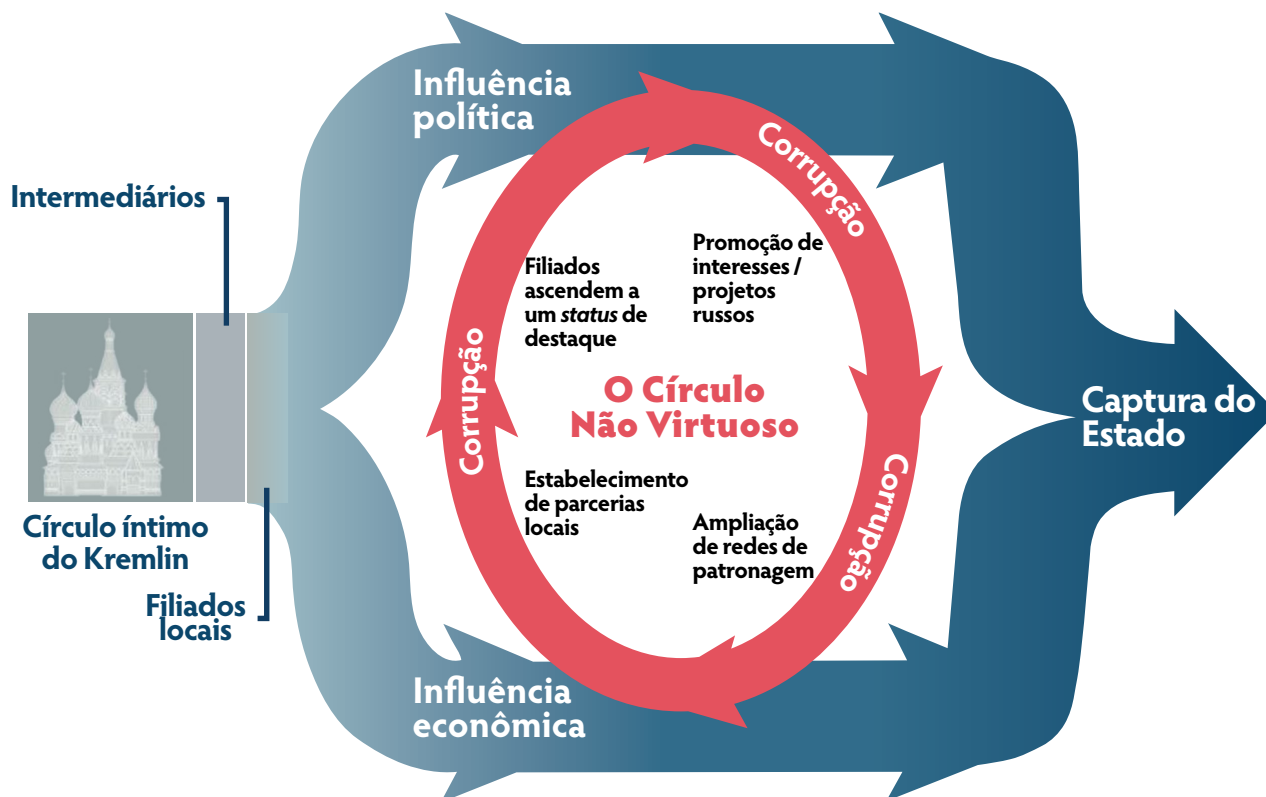
Figura 1 - O Papel de Métodos Não Militares na Resolução de Conflitos entre Estados

Conforme claramente descrito na obra *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* ("O Manual do Kremlin: Entendendo a Influência Russa na Europa Central e no Leste Europeu", em tradução livre), a influência russa, coordenada por meio de redes criminosas de etnia russa, pode ser usada para aumentar a corrupção de uma sociedade, gerando um efeito semelhante a uma doença incapacitante, em que "a nociva influência russa pode ser comparada a um vírus que ataca as democracias"³¹. A Rússia emprega o poder econômico, canalizado, especificamente, através de vias de corrupção, para influenciar decisores e instituições políticas e econômicas em toda a Europa. O objetivo dessa influência velada dirigida às autoridades eleitas, empresários, organizações da

mídia, partidos e movimentos políticos é "por meio da coação e da corrupção, fazer com que as políticas da região se afastem da integração europeia e se aproximem da Rússia"³². A figura 2, da obra *The Kremlin Playbook*, ilustra esse processo.

As atividades conduzidas pela Rússia em toda a Europa nos últimos cinco anos não são algo novo, mas o emprego inovador de meios tecnológicos para disseminar suas mensagens tornou essas atividades bem mais eficazes do que antes. Os métodos e doutrina de influência russos remontam a antes e durante a Segunda Guerra Mundial:

A teoria russa moderna sobre guerra de informação advém diretamente da *spetspropaganda*, lecionada, pela primeira vez, como uma disciplina do Instituto Militar



(Imagem de Heather Conley, James Mina, Rusland Stefanov e Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* [Washington, DC: Center for Strategic & International Studies, 2016], p. 3, acesso em 18 jul. 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf).

Figura 2 - Canais de Influência Russa

Russo de Idiomas Estrangeiros em 1942, mas com origens profundamente arraigadas na ideologia marxista-leninista³³.

A atual guerra de informação russa é uma atualização bem executada desses métodos mais antigos. Essas táticas mais antigas estão centradas em dois elementos principais: *medidas ativas* e *controle reflexivo*. As medidas ativas incluem esforços para influenciar, enfraquecer, abalar e desacreditar os países visados, suas instituições e organizações não governamentais³⁴. O controle reflexivo se assemelha às descrições do Departamento de Defesa dos EUA para a dissimulação militar e operações psicológicas. Contudo, essa atividade opera sem a exigência de se utilizarem informações verdadeiras. Em *Russian Military Strategy*, o analista de assuntos russos Timothy Thomas cita V. L. Makhnin ao descrever que o controle reflexivo busca manipular e confundir o decisor da organização visada para paralisar a “atividade (criativa) inteligente dos (decisores) do adversário”³⁵. Segundo o “Handbook of Information Warfare” da OTAN, o

controle reflexivo visa a manipular o processo decisório da organização visada “alterando fatores essenciais na percepção que o adversário tem do mundo [...] levando-o a escolher as ações mais vantajosas para os objetivos russos”³⁶. A doutrina russa, conforme expressa pelo Estado-Maior Geral da Rússia, afirma o seguinte:

As guerras serão resolvidas por uma hábil combinação de medidas militares, medidas não militares e medidas especiais não violentas, que serão realizadas por meio de uma variedade de formas e métodos e uma mistura de medidas políticas, econômicas, informacionais, tecnológicas e ambientais, principalmente tirando-se vantagem da superioridade de informações³⁷.

Jolanta Darczewksa, partindo da ótica polonesa, também sustenta que a guerra de informação russa é um retorno às práticas soviéticas:

As premissas doutrinárias sobre a guerra de informação demonstram não tanto uma mudança na teoria sobre sua condução

(as mudanças se referem, principalmente, à forma de sua descrição, e não ao seu conteúdo), e sim um apego a velhos métodos (sabotagem, táticas diversionárias, desinformação, terrorismo estatal, manipulação, propaganda agressiva, exploração do potencial para protesto entre a população local)³⁸.

Os métodos russos da atualidade são bem mais avançados do que os empregados contra a Geórgia em 2008, especialmente envolvendo o emprego seletivo das mídias sociais. Em *Social Media as a Tool of Hybrid Warfare* (“Mídias Sociais como uma Ferramenta de Guerra Híbrida”, em tradução livre), o Centro de Comunicações Estratégicas da OTAN identificou “*trolls* híbridos” que operam “no contexto de um programa político ou militar particular”³⁹. O governo russo utiliza *sites* falsos que parecem ser fontes independentes de informação. Esses *sites* “fantoques” que atuam como agregadores de notícias têm sido especialmente eficazes ao influenciarem públicos fora da Rússia durante operações como as conduzidas na Crimeia. Igor Panarin é um influente teórico sobre a guerra de informação russa e o nacionalismo russo extremo. Em 2014, conforme observado por Darczewska, o Professor Panarin, então docente da Academia Diplomática do Ministério de Relações Exteriores da Federação Russa, descreveu as ações conduzidas contra a Ucrânia durante a anexação da Crimeia como uma “guerra de informação defensiva”, executada como uma campanha planejada e coordenada, aprovada e dirigida pessoalmente por Putin⁴⁰.

Constituindo uma parte importante do movimento nacionalista e um útil recurso para a influência russa, os russos que vivem fora da Rússia propriamente dita têm sido identificados e recrutados como agentes de influência, na qualidade de “compatriotas residentes no exterior”. Considerados pela Rússia como estando legalmente conectados à nação materna, o *status* de compatriota fornece direitos, com exceção da cidadania, aos que se identificam como russos⁴¹. A Rússia usa essa rede de russos étnicos e simpatizantes como uma forma de exercer pressão e influência sobre os Estados visados. Compatriotas criminosos e não criminosos são frequentemente empregados como “grupos representantes” atuando em prol dos interesses russos. Esses indivíduos podem ser usados para dar a impressão de que haja apoio local para as ações russas. Podem servir como testemunhas diretas dos acontecimentos e apoiar

a narrativa de que haja uma ameaça existencial aos russos étnicos nos Estados Bálticos, Ucrânia e Geórgia. Esses grupos “representantes” incluem redes criminosas, organizações fraternas voltadas ao idioma russo, associações da Igreja Ortodoxa Russa e paramilitares como o clube de motoqueiros “Lobos da Noite”⁴².

Em outubro de 2016, a Rússia organizou um violento golpe em Montenegro para impedir a votação da proposta de solicitar entrada na OTAN⁴³. Nos países bálticos, as forças russas empregaram, cuidadosamente, a intimidação e encenaram ações de violência contra a população russa, simultaneamente retratando as tropas desdobradas da OTAN na mídia como estupradores e agitadores. Além disso, as mídias sociais das tropas da OTAN na área de operações foram visadas, com agentes russos ameaçando suas famílias em seu país de origem⁴⁴.

Recentemente, a Rússia empregou ataques contra soldados ucranianos individualmente, com o envio de mensagens de celular durante combates contra a insurgência apoiada pela Rússia nas Províncias do leste da Ucrânia⁴⁵. A eleição presidencial na França, em maio de 2017 assistiu a uma enorme iniciativa russa em prol da candidata da extrema direita, Marine Le Pen, incluindo o apoio financeiro direto na forma de empréstimos de vários milhões de euros ao seu partido, Frente Nacional⁴⁶. A ação nas mídias sociais empregou “*Twitter bots*” russos, ou “amplificadores ativos”, que foram extremamente dinâmicos, disseminando mensagens contra Macron e a favor de Le Pen. Esses *bots* controlados pelos russos redirecionaram seus esforços para as eleições de setembro de 2017, para atacar a Chanceler Angela Merkel e apoiar candidatos alemães de extrema direita, conforme detalhado na pesquisa on-line realizada pelo Digital Forensic Research Lab, do instituto Atlantic Council⁴⁷. Conforme observado também por Stelzenmüller, o equivalente alemão do FBI declarou que os “serviços de Inteligência russos também estão ‘tentando influenciar os decisores e a opinião pública da Alemanha’”⁴⁸. Os métodos russos incluem partidos políticos de extrema direita influenciados pela Rússia, o emprego de russos étnicos na Alemanha como “representantes” e o apoio de amplificadores automáticos de mensagens em múltiplas plataformas midiáticas. Como se pode observar com esse e outros acontecimentos, as técnicas de guerra de informação russas são sofisticadas e multifacetadas⁴⁹.

Este artigo constitui apenas uma breve discussão sobre a doutrina e métodos informacionais russos e ocidentais. Busca introduzir o leitor a um crescente volume de pesquisas de fontes ostensivas que analisam a significativa ameaça de ações russas contra os aliados dos EUA e as partes do tratado. Está claro que as ações e a agressão russa contra os EUA e seus aliados não vão diminuir. As ações russas foram

redirecionadas, com o objetivo de influenciar as eleições alemãs e os membros centro-europeus da OTAN. A Rússia continua a conduzir suas ações sincronizadas por toda a Europa. Instituições mais fortes, campanhas mais agressivas de resposta e melhores ações unificadas em prol dos interesses dos EUA serão essenciais para combater essa agressão russa. ■

Referências

1. "U.S. European Command Posture 2017: Posture Statement of General Curtis M. Scaparroti, Commander, U.S. European Command February 25, 2017", U.S. European Command website, 23 Mar. 2017, acesso em 18 ago. 2017, <http://www.eucom.mil/mission/eucom-2017-posture-statement>.
2. Missy Ryan e Dan Lamothe, "Placing Russia First among Threats, Defense Nominee Warns of Kremlin Attempts to 'Break' NATO", *Washington Post* online, 12 Jan. 2017, acesso em 14 jul. 2017, https://www.washingtonpost.com/world/national-security/senate-set-to-question-trumps-pentagon-pick-veteran-marie-n-gen-james-mattis/2017/01/11/b3c6946a-d816-11e6-9a36-1d296534b31e_story.html?utm_term=.824924803d00.
3. Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington, DC: Institute for the Study of War, September 2015), p. 9.
4. Katri Pynnöniemi, "The Metanarratives of Russian Strategic Deception", in *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, FIIA [Finnish Institute of International Affairs] Report 45, eds. Katri Pynnöniemi and András Rác (Helsinki: FIIA, 2016), p. 97.
5. David Ignatius, "Russia's Radical New Strategy for Information Warfare", *Washington Post* online, 18 Jan. 2017, acesso em 13 set. 2017, https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.492f34e18be9.
6. NATO Strategic Communications (StratCom) Centre of Excellence, *Analysis of Russia's Information Campaign against Ukraine: Examining Non-Military Aspects of the Crisis in Ukraine from a Strategic Communications Perspectives* (Riga, Latvia: NATO StratCom Centre of Excellence, 2015), p. 15, acesso em 20 jul. 2017, <http://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine>.
7. Este artigo foi adaptado de parte da dissertação do autor para o Mestrado em Arte e Ciência Militar do U.S. Command and General Staff College. Collins D. Cockrell, "Gray Zone Warfare: German and Russian Political Warfare 1935-1939 and 2014" (thesis, Fort Leavenworth, KS: Command and General Staff College, 2017).
8. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 2014), p. ix.
9. Ibid., II-4. As capacidades relacionadas à informação "são as ferramentas, técnicas ou atividades que afetam qualquer uma das três dimensões do ambiente informacional. Afetam a capacidade do público-alvo para buscar, processar ou disseminar informações antes e após decisões serem feitas. O público-alvo consiste no indivíduo ou grupo selecionado para ser sujeito à influência".
10. JP 3-13.2, *Military Information Support Operations* (Washington, DC: U.S. GPO, 21 Nov. 2014), p. vii. A JP 3-13.2 estava sendo revisada quando da publicação deste artigo.
11. Para obter mais informações sobre o StratCom Centre of Excellence, da OTAN, acesse <http://www.stratcomcoe.org/about-us>.
12. Ibid.
13. Keir Giles, "Handbook of Russian Information Warfare" (NATO Defense College Fellowship Monograph Series 9, Rome, Italy: NATO Defense College, Nov. 2016).
14. Allied Joint Publication 3.10.1, *Allied Joint Doctrine for Psychological Operations* (Brussels: NATO Standardization Office, Sept. 2014), p. 1-3.
15. Constanze Stelzenmüller, "The Impact of Russian Interference on Germany's 2017 Elections", 28 Jun. 2017, acesso em 5 set. 2017, <https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/>.
16. "NATO Welcomes Opening of European Centre for Countering Hybrid Threats", NATO website, 11 Apr. 2017, acesso em 14 jul. 2017, http://www.nato.int/cps/en/natohq/news_143143.htm?utm_source=twitter&utm_medium=press&utm_campaign=20170411-hybrid.
17. "In Massive Spending Bill, U.S. Lawmakers Back Several Measures Targeting Russia" Radio Free Europe/Radio Liberty, 4 May 2017, acesso em 16 ago. 2017, <https://www.rferl.org/a/us-spending-bill-government-running-senate-trump/28468643.html>.
18. Nahal Toosi, "Tillerson Moves toward Accepting Funding for Fighting Russian Propaganda", *Politico* online, 31 Aug. 2017, acesso em 5 set. 2017, <http://www.politico.com/story/2017/08/31/rex-tillerson-funding-russian-propaganda-242224>.
19. Allied Joint Publication 3.10.1, *Allied Joint Doctrine for Psychological Operations* (Brussels: NATO Standardization Office, Sept. 2014), p. 1-6.
20. Giles, "Handbook of Russian Information Warfare", p. 11.
21. Jolanta Darczewska, "Russia's Armed Forces on the Information War Front: Strategic Documents", OSW [Centre for Eastern Studies] Studies no. 57 (Warsaw, Poland: OSW, June 2016), p. 8. Para conferir a versão em inglês da atual doutrina russa, veja "The Military Doctrine of the Russian Federation Approved by Russian Federation Presidential Edict on 5

February 2010", School of Russian and Asian Studies website, 20 Feb. 2010, acesso em 17 jul. 2017, http://www.sras.org/military_doctrine_russian_federation_2010.

22. Training Circular 7-100, *Hybrid Threat* (Washington, DC: U.S. GPO, November 2010), V.

23. Diego A. Ruiz Palmer, "Back to the Future? Russia's Hybrid Warfare, Revolutions in Military Affairs, and Cold War Comparisons", (Research Paper No. 120, Rome, Italy: NATO Defense College, October 2015), p. 2.

24. National Security Analysis Department, "Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014, Assessing Revolutionary and Insurgent Strategies Study (unclassified working draft, Fort Bragg, NC: U.S. Army Special Operations Command), p. 27. Veja também "SOF Support to Political Warfare White Paper" (Fort Bragg, NC: U.S. Army Special Operations Command, 10 March 2015), p. 201, acesso em 18 jul. 2017, [http://www.soc.mil/swcs/ProjectGray/Support%20to%20Political%20Warfare%20White%20Paper%20v2.3-RMT%20\(10MAR2015\)%20%20%20.pdf](http://www.soc.mil/swcs/ProjectGray/Support%20to%20Political%20Warfare%20White%20Paper%20v2.3-RMT%20(10MAR2015)%20%20%20.pdf).

25. Charles K. Bartles, "Getting Gerasimov Right", *Military Review* 96, no. 1 (January-February 2016), p. 35. [A versão em português, intitulada "Para Entender Gerasimov", consta da edição brasileira de março-abril de 2016 da *Military Review* — N. do T.]

26. National Security Analysis Department, "Little Green Men", p. 27.

27. Valery Gerasimov, "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", *Military Review* 96, no. 1 (January-February 2016): p. 24. O artigo de Gerasimov foi publicado originalmente em *Military-Industrial Kurier*, 27 fev. 2013. [A versão em português, intitulada "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* — N. do T.]

28. "SOF Support to Political Warfare White Paper".

29. Jolanta Darczewska, "The Devil is in The Details: Information Warfare in the Light of Russia's Military Doctrine" OSW Point of View no. 50 (Warsaw, Poland: OSW, May 2015), p. 12.

30. Timothy L. Thomas, *Russian Military Strategy: Impacting 21st Century Reform and Geopolitics* (Fort Leavenworth, KS: Foreign Military Studies Office, 2015), p. 238-39.

31. Heather Conley, James Mina, Rusland Stefanov e Martin Vladimov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, DC: Center for Strategic and International Studies, 2016), p. 26.

32. Alina Polyakova, Marlene Laruelle, Stefan Meister e Neil Barnett, *The Kremlin's Trojan Horses*, 3rd ed. (Washington, DC: Dinu Patriciu Eurasia Center, Atlantic Council, November 2016), 4, accessed 17 July 2017, http://www.atlanticcouncil.org/images/publications/The_Kremlins_Trojan_Horses_web_0228_third_edition.pdf.

33. Edward Lucas e Peter Pomeranzen, *Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in*

Central and Eastern Europe (Washington, DC: Center for European Policy Analysis, August 2016), p. 6.

34. Katri Pynnöniemi, "The Conceptual and Historical Roots of Deception", in *Fog of Falsehood*, p. 38.

35. V. L. Makhnin, "Reflexive Processes in Military Art: The Historico-Gnoseological Aspect", *Voennaya Mysl' (Military Thought)*, No. 1 2013, p. 40, apud Thomas, *Russian Military Strategy*, p. 120.

36. Giles, "Handbook of Russian Information Warfare," 19.

37. Sergey Checkinov e Sergei Bogdanov, "Forecasting the Nature and Content of Wars of the Future: Problems and Assessments", *Voennaya Mysl' (Military Thought)*, no. 10 (2015): p. 44-45, apud Giles, "Handbook of Russian Information Warfare", p. 6.

38. Darczewska, "The Devil is in the Details", p. 12.

39. NATO StratCom Centre of Excellence, *Social Media as a Tool of Hybrid Warfare* (Riga, Latvia: NATO StratCom Centre of Excellence, May 2016), p. 27, acesso em 20 jul. 2017, <http://www.stratcomcoe.org/social-media-tool-hybrid-warfare>.

40. Jolanta Darczewska, "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study", OSW Point of View no. 42 (Warsaw, Poland: OSW, May 2014), p. 24.

41. Vera Zakem, Paul Sanders e Daniel Antoun, *Mobilizing Compatriots: Russia's Strategy, Tactics, and Influence in the Former Soviet Union*, CNA [Center for Naval Analyses] Occasional Paper (Arlington, VA: CNA, November 2015), p. 14.

42. Orysia Lutsevych, "Agents of the Russian World: Proxy Groups in the Contested Neighbourhood" (research paper, London: Chatham House, The Royal Institute of International Affairs, April 2016), p. 19.

43. Milena Veselinovic e Darran Simon, "Montenegro: Russia Involved in Attempted Coup", CNN, 21 Feb. 2017, acesso em 17 jul. 2017, <http://www.cnn.com/2017/02/21/europe/montenegro-attempted-coup-accusation/index.html>.

44. Tom Porter, "British Soldiers' Latvia Brawl 'Was Set Up As Part Of Russian Propaganda Sting'", *International Business Times*, 2 Nov. 2016, acesso em 14 jul. 2017, <https://sg.news.yahoo.com/british-soldiers-latvia-brawl-set-104233445.html>.

45. Raphael Satter e Dmytro Vlasov, "Ukrainian Soldiers Bombarded By 'Pinpoint Propaganda' Texts", ABC News, 11 May 2017, acesso em 14 jul. 2017, <http://abcnews.go.com/Technology/wireStory/sinister-text-messages-reveal-high-tech-front-ukraine-47341695>.

46. Gabriel Gatehouse, "Marine Le Pen: Who's Funding France's Far Right?", BBC News, 3 April 2017, acesso em 14 jul. 2017, <http://www.bbc.com/news/world-europe-39478066>.

47. @DFRLab, "The Kremlin's Audience in France: Breaking Down the Amplifiers of Sputnik and RT in French", Atlantic Council's Digital Forensic Research Lab, medium.com, 14 April 2017, acesso em 14 jul. 2017, <https://medium.com/dfrlab/the-kremlins-audience-in-france-884a80515f8b>.

48. Stelzenmüller, "The Impact of Russian Influence on Germany's 2017 Elections".

49. Snegovaya, *Putin's Information Warfare in Ukraine*, p. 20.