Oficial de operações cibernéticas observa integrantes do 175º Grupo de Operações Cibernéticas analisando arquivos e fornecendo uma atualização de ameaças cibernéticas, na Base Aérea da Guarda Nacional Warfield, Middle River, Maryland, 03 Jun 17. (Foto por J. M. Eddins Jr., Força Aérea dos EUA)

Segurança Cibernética Social

Um Requisito Emergente de Segurança Nacional

Ten Cel David M. Beskow, Exército dos EUA
Kathleen M. Carley, Ph.D.

A segurança cibernética social é um subdomínio emergente da segurança nacional que afetará todos os níveis da guerra do futuro, tanto convencional quanto não convencional, com claras implicações estratégicas. A segurança cibernética social "é uma área científica emergente, focada na ciência para caracterizar, entender e prever mudanças intermediadas pela cibernética no comportamento humano e seus resultados sociais, culturais e políticos. Destina-se também à construção da infraestrutura cibernética necessária para a sociedade manter seu caráter essencial em um ambiente informacional afetado por condições variáveis e ameaças cibernéticas sociais reais ou iminentes"[1]. Nos dias de hoje, a tecnologia capacita tanto atores estatais quanto não estatais a manipularem o "mercado global de crenças e ideias" à velocidade de algoritmos, e isso está transformando o campo de batalha em todos os níveis da guerra.

Recentemente analisada pela ótica da "guerra híbrida", a guerra da informação está se tornando um fim em si mesma. Dmitry Kiselev, o coordenador da agência estatal russa de notícias internacionais, observa que "as guerras de informação são [...] o principal tipo de guerra"[2]. A informação é usada para fortalecer a narrativa de quem a manipula, enquanto ataca, interrompe, distorce e divide a sociedade, a cultura e os valores de outros Estados e organizações antagônicas. Ao enfraquecer a confiança nas instituições nacionais, no consenso sobre os valores nacionais e na dedicação a esses valores por toda a comunidade internacional, um determinado ator pode vencer a próxima guerra antes mesmo de sua deflagração. De fato, refletindo uma mudança de conflito episódico para a competição contínua, oficiais do mais alto escalão do Estado-Maior russo já afirmaram que "As guerras não são declaradas, mas já se iniciaram"[3].

O papel da informação dentro dos elementos do poder nacional está se tornando cada vez mais importante. A estratégia se apoia nos quatro elementos do poder nacional: diplomático, informacional, militar e econômico (DIME). Atualmente, a tecnologia permite que atores estatais e não estatais estendam seu poder no domínio informacional em uma escala e complexidade até então consideradas impossíveis. Se não nos atentarmos para tal fato, uma "*blitzkrieg* informacional" terá efeitos estratégicos semelhantes à *blitzkrieg* física desencadeada pelos alemães no início da Segunda Guerra Mundial.

Embora seja uma atividade técnica por natureza, a segurança cibernética social se diferencia da segurança cibernética usual. A forma tradicional está associada a pessoas que usam a tecnologia para "hackear" tecnologia. Os sistemas de informações são o alvo. A segurança cibernética social envolve humanos que usam a tecnologia para "hackear" outros humanos. Ou seja, os alvos são pessoas e a sociedade da qual fazem parte. Essa distorção do paradigma cibernético tradicional, às vezes, é chamada de "hacking cognitivo". Enquanto se vale do meio cibernético para a difusão em massa, essa guerra de informação emergente explora os avanços em marketing direcionado (ou micromarketing); os recursos da psicologia e da persuasão; as lacunas políticas existentes entre instituições privadas e governamentais; e o entendimento das ciências sociais para empregar operações de informação coordenadas visando a alcançar efeitos estratégicos.

A segurança cibernética social é uma ciência social computacional multidisciplinar. "As teorias emergentes se fundem à ciência política, sociologia, ciência

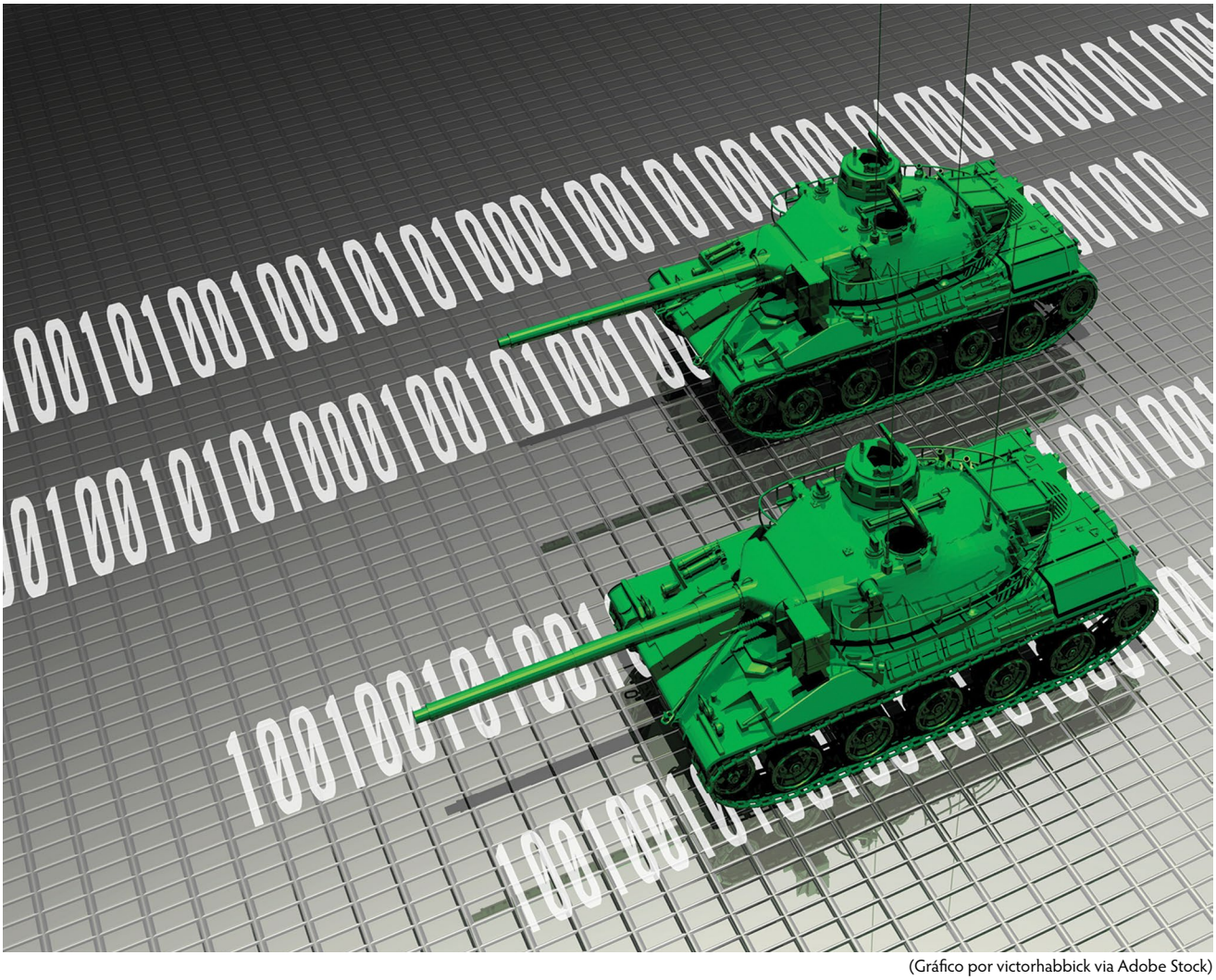
O Ten Cel David Beskow, do Exército dos EUA, é doutorando pela School of Computer Science na Carnegie Mellon University. É bacharel em Engenharia Civil pela Academia Militar dos Estados Unidos, em West Point, e mestrado em Investigação Operacional pela Naval Postgraduate School. Durante sua carreira, serviu como comandante de tropa na 82ª Divisão Aeroterrestre e na 4ª Divisão de Infantaria. Como analista de sistemas de pesquisa operacional (ORSA, na sigla em inglês), serviu como professor assistente em West Point e no Comando de Inteligência e Segurança do Exército dos EUA. Sua pesquisa atual desenvolve algoritmos de aprendizado de máquina para detectar e caracterizar *bots on-line* e as campanhas de desinformação habitadas por eles.

Kathleen M. Carley, Ph.D., é professora de computação social na School of Computer Science da Carnegie Mellon University. É bolsista IEEE, diretora do Center for Computational Analysis of Social and Organizational Systems (CASOS), e CEO da companhia Netanomics. Foi vencedora do Simmel Award da International Network for Social Network Analysis (2011) e vencedora do National Geospatial-Intelligence Agency Academic Award da GEOINT (Inteligência geoespacial – 2018).

da comunicação, ciência organizacional, marketing, linguística, antropologia, investigação forense, ciência da decisão e psicologia social"[4]. Muitos pesquisadores desse novo campo aproveitam as ferramentas das ciências sociais computacionais, como análise de redes, análise espacial, análise semântica e aprendizado de máquina. Esses recursos são empregados em múltiplos níveis, do indivíduo à sua comunidade.

Para o Departamento de Defesa "prover a segurança do nosso país e manter a influência norte-americana no exterior", faz-se necessário que os líderes militares dos Estados Unidos entendam essa disciplina emergente denominada segurança cibernética social e como ela impacta nossa força, nossa nação e nossos valores[5]. O presente artigo irá discorrer sobre essa nova disciplina, discutindo de forma sucinta seu histórico e as mudanças sociotecnológicas que a capacitam. Por fim, abordaremos as "formas de manobra" atuais e futuras da segurança cibernética social. Ao longo de todo o texto, procuraremos destacar as semelhanças e diferenças entre a segurança cibernética social e as operações cibernéticas tradicionais.

> Uma "*blitzkrieg* informacional" terá efeitos estratégicos semelhantes à *blitzkrieg* física desencadeada pelos alemães no início da Segunda Guerra Mundial.



(Gráfico por victorhabbick via Adobe Stock)

Antecedentes: A *Blitzkrieg* Informacional Russa

A Rússia está travando a mais incrível blitzkrieg *informacional que já vimos na história da guerra de informação.*

—Ten Brig Ar Philip Breedlove, reunião de cúpula da OTAN no País de Gales em 2014[6]

O sistema de propaganda russo, por muito tempo direcionado para sua própria sociedade e para os Estados satélites da antiga União Soviética, visa atualmente a alcançar alvos no exterior. No ano de 2013, em seu famoso artigo "O Valor da Ciência Está na Previsão", o Gen Valery Gerasimov definiu a guerra da informação como um componente importante da estratégia russa daqui para frente[7]. Embora o Ocidente tenha interpretado o texto de forma retrospectiva, associando-o ao conflito na Ucrânia, e atribuindo-lhe erroneamente a responsabilidade pelo advento da guerra híbrida no âmbito do exército russo, o artigo do Gen Gerasimov era, na realidade, sua perspectiva pessoal acerca da Primavera Árabe, bem como das operações dos EUA na Iugoslávia, Iraque e Afeganistão[8]. De acordo com seu ponto de vista, a Primavera Árabe e as coalizões lideradas pelos EUA no Oriente Médio dependeram sobremaneira de recursos que extrapolavam as capacidades disponíveis nas forças militares convencionais para moldar eventos, referindo-se especialmente às operações de informação. As forças militares foram introduzidas no último momento, apenas, como um golpe de misericórdia.

Após estudar esses conflitos, Gerasimov buscou acelerar as iniciativas referentes à guerra da informação que já estavam em curso, declarando: "A guerra da informação abre amplas possibilidades assimétricas para reduzir o potencial de combate do inimigo"[9]. Essas atividades estavam alinhadas com as tradicionais operações russas da KGB (Comitê de Segurança do Estado), conhecidas como "medidas ativas". O Gen Bda Oleg Kalugin as descreveu como "medidas ativas para enfraquecer o Ocidente, abrindo brechas de todos os tipos nas alianças existentes na comunidade ocidental, particularmente na OTAN, semeando discórdia entre os aliados; enfraquecendo os Estados Unidos aos olhos dos povos da Europa, Ásia, África e América Latina; e, assim, criando condições favoráveis no caso de uma eventual guerra"[10]. A citação de Kalugin ressalta um dos papéis críticos da teoria da *blitzkrieg* informacional russa, que é abrir "brechas" em todas as fissuras possíveis, fraturando uma nação ou uma coalizão. Isso inclui a exploração de cismas entre partidos políticos, raças, religiões, sociedades, forças armadas e alianças internacionais. Uma nação fraturada é, inerentemente, um país menos apto a se defender de uma agressão externa.

As tendências emergentes nas operações de informação russas são construídas a partir de uma longa história de operações de propaganda legada da era soviética. Em 1951, o então professor de direito Harold Lasswell resumiu a essência da máquina de propaganda soviética, da qual o sistema de segurança da Federação Russa de hoje é herdeiro:

> O principal objetivo estratégico [da propaganda soviética] é economizar os recursos materiais necessários para proteger e expandir o poder da elite russa dentro e fora do país. A propaganda se torna, assim, sob o ponto de vista soviético, uma disputa pela mente das pessoas, pois não passa de uma disputa pelo controle dos meios materiais pelos quais, se acredita, as mentes das massas são moldadas. Portanto, o propósito da propaganda russa não é a persuasão pacífica da maioria do povo de um dado país, como prelúdio de uma assunção do poder. Em vez disso, a propaganda é concebida como instrumento de uma minoria que precisa sobreviver ideologicamente até que consiga acumular os meios materiais necessários para obter um consenso [...] os propagandistas soviéticos e seus agentes podem mentir e distorcer os fatos sem nenhum tipo de comedimento interno, porque são imunes em sua maioria às alegações de violação da dignidade humana em qualquer outro sentido, exceto a dignidade de [...] contribuir para o poder presente e futuro da elite do Kremlin[11].

Essa abordagem geral perdura até os dias de hoje, construindo um pequeno núcleo de poder russo, enquanto divide todas as organizações e instituições que lhe são antagônicas por meio do uso contínuo da desinformação. Porém, atualmente, a tecnologia permite que isso aconteça em uma escala e alcance inimagináveis para os padrões de 1951.

O Estado russo aborda isso de forma empírica. Desde 2003, a Academia de Ciências Russa tem conduzido pesquisas básicas para desenvolver modelos matemáticos sofisticados acerca da guerra da informação e sua aplicabilidade na sociedade. Seus pesquisadores combinam as ciências sociais e a

Alexander Malkevich, 03 Mar 12. (A. Khmeleva via Wikimedia Commons)

modelagem matemática para produzir estudos como "Mathematical Modeling of Rumors and Information Propagation in Society" ("A Modelagem Matemática de Rumores e da Propagação de Informação na Sociedade", em tradução livre). Embora esses artigos aleguem uma conotação defensiva, presume-se que possam ser empregados também nas operações ofensivas.

Tais operações são sincronizadas por um quadro, cada vez maior, de tecnólogos políticos. Ou seja, líderes, tanto dentro quanto fora do governo, que entendem a natureza interdependente dos domínios humano, político, militar e tecnológico. Valendo-se desse entendimento dos "múltiplos domínios", eles desenvolvem e coordenam as ações para moldar o ambiente, explorando os domínios cibernético e tecnológico para afetar os domínios social, político e militar. Por exemplo, Alexander Malkevich, um tecnólogo residente em Moscou, criou o website www.USAreally.com, antes das eleições estaduais de 2018 nos EUA[12]. Sua missão era disseminar uma narrativa distorcida, promovendo agitação e discordância entre o povo dos EUA, por meio das principais agências de notícias norte-americanas ou fontes complementares aos veículos convencionais. A *descrição* pessoal que consta de sua conta no Twitter declara: "Jornalista. Homem de mídia. Uma pessoa interessada na vida, que não teme trabalhar nas regiões da Rússia e em nome da Rússia"[13]. Malkevich pode ser considerado um tecnólogo político.

Mudança no Centro de Gravidade Estratégico

O início do Século XX testemunhou as guerras mais simétricas e cinéticas de toda a história da humanidade. O Século XXI, por sua vez, começou com vários conflitos assimétricos e não cinéticos, decorrentes de décadas de competição durante a Guerra Fria. No decurso da Primeira Guerra Mundial, por exemplo, as nações sacrificaram centenas de milhares de vidas por alguns poucos metros de terreno físico. Hoje, muitos atores desenvolvem planos complexos para conquistar lentamente "metros" no domínio humano com ramificações no domínio físico.

A geografia ainda exerce grande importância na atualidade. Os dois maiores eixos de segurança dos Estados Unidos continuam sendo os oceanos Pacífico e Atlântico[14]. A Crimeia foi anexada pela Rússia, sobretudo, em face da relevância estratégica do porto de Sebastopol no Mar Negro (bem como por suas implicações energéticas)[15]. A instabilidade no Afeganistão continuará sendo, em parte, alimentada por sua localização geográfica[16]. Ou seja, a geografia é, e sempre será, importante. No entanto, pode-se afirmar que vários fatores, incluindo a tecnologia, já inclinaram o pêndulo para as dimensões humana e informacional.

Essa mudança para o domínio humano e informacional foi profundamente debatida no âmbito das Forças Armadas dos EUA durante a Guerra Contra o Terror. Após anos de debate, parece que a maioria dos

profissionais concordou com a afirmação de um artigo, de 2009, publicado pelo *Small Wars Journal*: "Uma das mudanças mais significativas que as Forças Armadas dos EUA precisam fazer para se tornarem eficazes nas operações de contrainsurgência é retirar os centros de gravidade estratégicos dos aspectos físicos e colocá-los nos aspectos humanos da guerra"[17]. Embora essa assertiva seja aceita em contextos de contrainsurgência, ainda não sabemos como essa mudança para o domínio humano afeta as operações de combate em larga escala.

A ideia do povo como centro de gravidade assumiu um novo significado após a Primavera Árabe, na medida em que movimentos populares descentralizados, capacitados pela tecnologia da informação, se organizaram e derrubaram regimes autocráticos em diferentes países do mundo Árabe. Esses eventos abalaram o Norte da África e o Oriente Médio e têm sido estudados por líderes tanto no Leste quanto no Ocidente. A onda de distúrbios internos colocou em evidência o valor da dimensão humana, bem como o poder das mídias sociais, para mobilizar as massas. Muitos artigos publicados em revistas especializadas já analisaram esses movimentos, com foco específico nas mídias sociais que os tornaram viáveis. Até mesmo o artigo, de 2013, do General Gerasimov no *Military-Industrial Courier* da Rússia, estudado no Ocidente como a gênese da *guerra híbrida* ou do *conflito na zona cinza*, nada mais é do que sua reflexão pessoal acerca da Primavera Árabe (bem como dos conflitos no Iraque, Afeganistão e Iugoslávia). Ao contrário do que muitos sugerem, não foi uma tentativa do General russo de criar um novo tipo de guerra[18].

Múltiplos atores estatais e não estatais observaram as mudanças em curso e começaram a explorar a ideia de manipulação desses movimentos no espaço cibernético. Muitos Estados e atores não estatais já têm experiência com a manipulação do seu próprio povo ou organização por meio de operações de informação, e agora buscam estender essa experiência a fim de atingir outras populações e sociedades[19]. Ataques direitos contra o tecido social, o verdadeiro centro de gravidade de uma nação, produzem efeitos massivos sobre os níveis tático e estratégico da guerra, e constituem a gênese desse domínio emergente denominado segurança cibernética social.

Capacitando Mudanças

Duas mudanças na comunicação humana e no fluxo de informações na sociedade já proporcionaram o surgimento de ameaças cibernéticas à estrutura social de uma nação. Primeiro, a tecnologia da informação tornou dispensável o requisito da proximidade física para influenciar a sociedade, e a descentralização dos fluxos de informação tem reduzido os custos de entrada. De acordo com Fabio Rugge, do Italian Institute for International Political Studies, "O ciberespaço é um poderoso multiplicador dos efeitos desestabilizadores da informação manipulada porque permite alta conectividade, baixa latência (rápida transmissão), baixo custo de entrada, múltiplos pontos de distribuição sem intermediários e quase total indiferença quanto a distâncias físicas e fronteiras nacionais. Mais importante ainda, o anonimato e a incapacidade de atribuir corretamente a responsabilidade por um ataque fazem com que o espaço cibernético seja o domínio da ambiguidade"[20].

Descentralização. Ao longo dos últimos 30 anos, observamos como os fluxos de informação rapidamente se descentralizaram. Historicamente, governos, grandes organizações e alguns canais de notícias controlavam a maioria da cobertura midiática formal por meio de radiodifusão, imprensa escrita e televisão. Essas organizações eram responsáveis pelo fluxo de informações e, em geral, o distribuíam uniformemente por toda a sociedade. Hoje, com o surgimento de blogs, microblogs e redes sociais, a maioria das pessoas obtém informação de uma maneira desuniforme nas mídias sociais[21]. Atualmente, é possível veicular, com relativa facilidade, informações a baixo custo de entrada, incentivo financeiro para criar conteúdo viral e anonimato. Essa descentralização, por si só, já é capaz de proporcionar o ingresso de atores externos com pouquíssimos requisitos.

O controle de qualidade relativo ao fluxo de informação é hoje descentralizado. Atualmente, a veracidade dos fatos é realizada no nível do próprio usuário em detrimento do crivo jornalístico. Os usuários, muitos dos quais cresceram em uma época na qual as notícias eram em sua maioria confiáveis, atualmente não estão preparados para "filtrar" as notícias que misturam verdade e mentira, especialmente, se as distorções da realidade são previamente planejadas para validar as parcialidades embutidas na notícia.

O modelo de negócios do jornalismo tradicional requer a verdade. Jornalistas perdem seu emprego e as agências de notícias perdem clientes se estão continuamente erradas. O modelo de negócios das mídias sociais, prioritariamente centrado na publicidade e no fluxo geral de dados, não depende tanto da verificação dos fatos. No entanto, isso

está mudando aos poucos, como observado no declínio do preço das ações do Twitter e do Facebook em agosto de 2018. A queda dos valores foi atribuída, em grande medida, ao lento crescimento enquanto retiravam de suas plataformas contas que propagavam notícias falsas.

Embora legisladores em todo o mundo tentem descobrir uma forma de normatizar e centralizar o controle, isso envolve algum tipo de censura e ameaça à liberdade de expressão. Em alguns casos, pode resultar em caos absoluto, especialmente se as empresas de mídias sociais são requeridas a fornecer uma função na própria plataforma que permita aos usuários apontar informações falsas ou maliciosas. Se um usuário qualquer pode acessar esse tipo de função por uma interface de programação de aplicação (API, na sigla em inglês) ou por uma interface *on-line*/móvel, então os mesmos *bots* [uma conta de mídia social que usa um computador para automatizar as tarefas do aplicativo — N. do T.] responsáveis pelas notícias falsas podem marcar todos os tipos de conteúdo verdadeiro como falso à velocidade de algoritmos, causando exponencialmente danos ainda maiores.

Presença física desnecessária. Durante a maior parte da história, influência requeria presença física ou, pelo menos, proximidade física. Para influenciar um debate no Fórum Romano, centro nervoso daquela sociedade, por exemplo, um ator ou representante qualquer tinha que estar dentro do fórum, ou pelo menos, em Roma, claramente identificado e ativo nas negociações. Existiam operações clandestinas, mas até elas exigiam a presença física. Esse requisito durou até a primeira metade do Século XX, ocasião em que as operações de radiodifusão e panfletagem surgiram,

Tabela. O Modelo BEND para Descrever as Formas de Manobra da Segurança Cibernética Social

	Manobra de Informação		Manobra de Rede	
	Manipulação das redes de conhecimento		Manipulação das redes sociais	
	Coisas que se pode fazer para afetar o que está sendo discutido		Coisas que se pode fazer para afetar quem fala e quem escuta	
Positivo	**Engajar**	Discussão que traz à tona um assunto relacionado relevante	**Respaldar**	Ações que aumentam a importância do líder ou formador de opinião
	Explicar	Discussão que fornece maiores detalhes ou aprofunda o assunto	**Construir**	Ações que criam um grupo ou a aparência de um grupo
	Excitar	Discussão que traz alegria/felicidade/ânimo/entusiasmo ao grupo	**Transpor**	Ações que conectam dois ou mais grupos
	Aprimorar	Discussão que incentiva o grupo a continuar com o assunto	**Aumentar**	Ações que ampliam o tamanho do grupo ou o fazem parecer maior
Negativo	**Dispensar**	Discussão sobre a irrelevância do assunto	**Neutralizar**	Ações que limitam a eficácia do líder de opinião, reduzindo o número de pessoas que o acompanham, replicam ou participam de suas redes sociais
	Distorcer	Discussão que altera a mensagem principal do assunto	**Implodir**	Ações que levam ao desmantelamento do grupo
	Desmotivar	Discussão sobre um assunto que trará preocupação/tristeza/raiva ao grupo	**Isolar**	Ações que levam à separação do grupo de outros grupos
	Distrair	Discussão sobre um tema totalmente diferente e irrelevante	**Degradar**	Ações que reduzem o tamanho do grupo ou o fazem parecer menor do que ele realmente é

(Tabela pelos autores)

não exigindo a presença física direta, mas, não obstante, requerendo algum nível de proximidade. Mesmo as poderosas operações de propaganda russas se restringiam ao Leste Europeu e à Ásia, devido a limitações geográficas. Porém, a internet eliminou essa exigência. Afinal, a maioria das sociedades interage em ambientes *on-line* livres com acesso irrestrito, permitindo que atores se engajem no domínio cibernético a partir dos recantos mais longínquos do planeta, ignorando as fronteiras nacionais.

Nações que valorizam a liberdade de expressão e possuem mercados abertos para opiniões e ideias são mais vulneráveis a esse tipo de ameaça[22]. Isso se torna bem evidente no caso da Coreia do Norte, indiscutivelmente a nação mais fechada do mundo. O país é, em grande parte, imune à manipulação social pela internet. A presença física ou a proximidade, ainda são necessários para influenciar diretamente a sociedade norte-coreana.

A vulnerabilidade das sociedades abertas diante da manipulação social pela tecnologia é exacerbada pelo fato de que a maioria das campanhas de informação estratégica pode ser lançada nas plataformas globais de mídias sociais que são privadas e, portanto, se encontram fora da supervisão direta dos governos (embora existam normas e regulamentos). Ainda que todas as empresas de mídia social censurem o conteúdo em sua plataforma, o propósito se restringe geralmente em proporcionar melhor serviço para o maior número de usuários ao redor do planeta, sem qualquer fim de segurança nacional em nenhum país. Tomar partido em qualquer assunto, quase sempre, é ruim para os negócios porque aliena uma parte da clientela. Presume-se que a censura governamental de conteúdo não seja imparcial e infrinja a liberdade de expressão defendida por esses mesmos governos. Existem esforços promovidos por entidades externas a fim de censurar conteúdo, mas até hoje, essas iniciativas têm tido um enfoque restrito e são facilmente contornadas. O "Social Science One" ("Ciência Social Um", em tradução livre), por exemplo, é uma parceria inovadora entre pesquisadores acadêmicos, indústria privada e financiamento proveniente de todo o espectro político, destinada a facilitar a pesquisa feita por entidades externas sobre os dados disponíveis nas mídias sociais, enquanto mantém a privacidade individual. Porém, esforços como esse ainda são incipientes.

Formas de Manobra Sociocibernética

Assim como os domínios físico e cibernético tradicional, o domínio sociocibernético oferece múltiplas "formas de manobra". Nesse domínio, um adversário pode manipular a *informação* bem como a *rede*. Essas redes podem ser redes sociais (Sarah e Peter são *amigos*), redes de conversa (Sarah *replica* a Peter) ou redes informacionais (ambos Sarah e Peter compartilham o hashtag #OTAN).

As formas de manobra BEND. O estado final desejado para as operações de informação varia. As operações de informação tradicionais visam a aumentar o apoio para a narrativa que nos interessa e reduzir o apoio à contranarrativa. Outras operações simplesmente têm por propósito aumentar a agitação e reduzir a confiança interna, independentemente da narrativa. Essa agitação se destina a criar fissuras em uma sociedade. Sejam quais forem, esses estados finais desejados se enquadram no modelo "BEND" de manobra informacional (como visto na Tabela)[23].

As formas de manobra BEND descrevem como um ator pode manipular o mercado de crenças, ideias e informação. As formas de manobra são construídas a partir das "ações táticas" dispensar, distorcer, desanimar e distrair introduzidas por Ben Nimmo no Atlantic Councils Digital Forensic Research Lab[24]. O modelo BEND caracteriza as formas de manobra por polaridade, identificando se o alvo é a *informação* ou a *rede*.

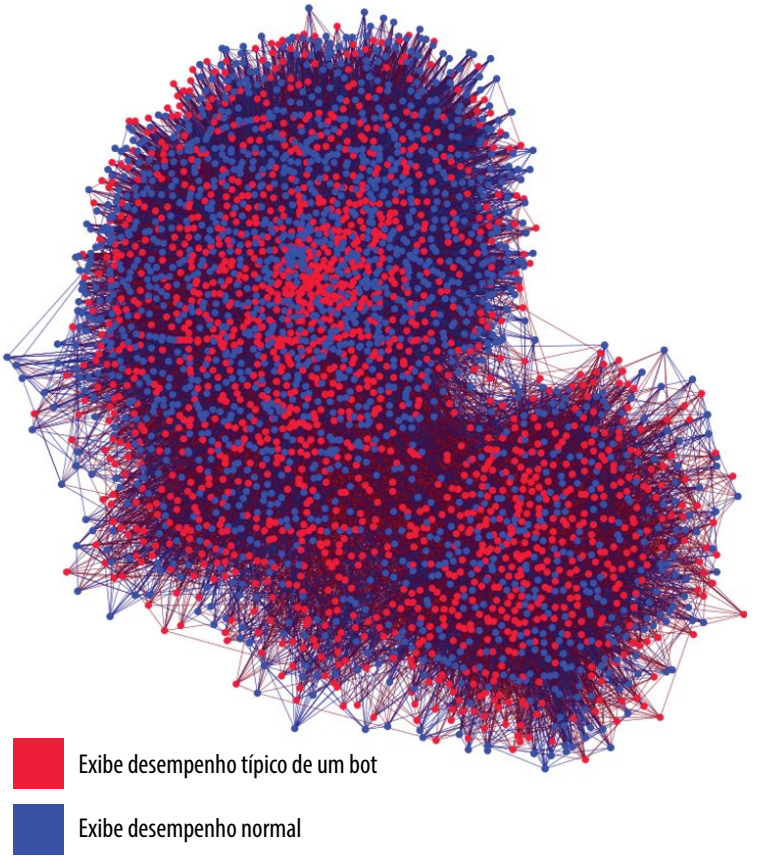
Manobra de informação. A manobra de informação é a manipulação da informação, bem como o fluxo ou a relevância da informação no ciberespaço. Exemplos da manobra de informação incluem:

- Desorientação. Introdução de assuntos polêmicos não relacionados a um tópico de discussão, afim de desviar o foco da conversa.
- *Hashtag latching*. Vinculação de conteúdo e narrativas não relacionados a determinados assuntos e hashtags.
- Cortina de fumaça. Disseminação de conteúdo (tanto forma semântica quanto geográfica) para dissimular outras operações.
- *Thread jacking*. Interromper agressivamente ou cooptar uma conversa *on-line* produtiva.

Manobra de rede. A manobra de rede é a manipulação da própria rede. Nessas manobras, um adversário ataca uma rede social (uma rede social *on-line*

é a projeção de ligações sociais e de debates na dimensão cibernética). Exemplos da manobra de rede inclui o seguinte:

- Cooptação de um líder ou formador de opinião. Obter acesso e reconhecimento de um líder de opinião *on-line* e valer-se de sua influência para disseminar uma narrativa específica.
- Construção de comunidade. Criar uma comunidade em torno de um tópico, ideia ou *hobby* e depois inserir uma narrativa no grupo. Esse recurso foi empregado na Ucrânia ao construir comunidades de jovens do sexo masculino em torno de contas de compartilhamento de conteúdo próprio para adultos, para em seguida inserir retórica antiucraniana e pró-russa nessas redes.
- Transposição de comunidades. A contaminação de ideias de um grupo para outro. Nesse caso, duas comunidades são identificadas, "A e B". O adversário tem por objetivo inserir determinadas ideias no grupo A, por meio do grupo B. Infiltra-se no grupo B e, depois, lentamente acrescenta-se tuites ou compartilha ideias com o grupo A, trazendo, aos poucos, as ideias do grupo B para o grupo A.
- Noção falsa generalizada. Cria-se a falsa noção de que uma determinada ideia ou crença representa o consenso das massas e, portanto, deve ser aceitada por todos.



(Figura dos autores)

Figura. Envolvimento de *Bots* na Discussão Política Principal no Twitter em Relação à Recente Eleição na Suécia

Bots como Multiplicadores de Força

Dentro do contexto das operações de informação, *bots* são empregados cada vez mais como multiplicadores do poder de combate. Eles aproveitam o aprendizado de máquina e a inteligência artificial para conduzir as trocas de informações visadas com oportunidade e em grande escala, enquanto deixam o diálogo crítico mais sutil para operadores humanos. Nesse contexto, os atores humanos são frequentemente chamados de "trolls", para diferenciá-los dos recursos computacionais que fazem isso automaticamente (i.e., "*bots*").

Um *bot* pode ser definido como uma conta de mídia social que usa um computador para automatizar as tarefas do aplicativo. Por exemplo, no ambiente do Twitter, uma conta *bot* pode automaticamente enviar tuites, repassar tuites, acompanhar, adicionar amigos, replicar, citar e "gostar". O usuário de um *bot* pode recorrer a meios criativos para gerar conteúdo, juntando fragmentos de outras fontes disponíveis na internet e resumi-los automaticamente; repassando tuites de conteúdo existente; manipulando o conteúdo de outros usuários ou criando seu próprio conteúdo por meio da combinação de contribuições humanas e de inteligência artificial. Ao produzir seu próprio conteúdo, o criador do *bot* pode manipular o momento de sincronização do tuite para parecer obra de um ser humano. Se isso não for importante, ele pode conduzir milhares de ações todos os dias. Finalmente, esses *bots* são distribuídos em redes de *bots* (às vezes chamadas "exércitos" de *bots* ou *bots* "coordenadores") onde adicionam amigos, seguem uns aos outros e se promovem mutuamente para parecerem mais populares do que realmente são.

Os *bots* são usados para uma enorme variedade de propósitos, criando efeitos que podem ser positivos, inconvenientes ou maliciosos. Alguns exemplos do bom uso de *bots* incluem assistentes pessoais e contas que notificam o público sobre desastres naturais. Os *bots* inconvenientes disseminam spam com assuntos que variam desde publicidade comercial a conteúdo para adultos. Os *bots* maliciosos são aqueles tipicamente utilizados com fins de propaganda, supressão de dissidência, intimidação e infiltração e/ou manipulação de redes[25].

Embora frequentemente tentemos distinguir o uso de uma conta por um *bot* ou um humano, podem existir diversos recursos automatizados associados a uma única conta. Muitas delas não são totalmente automatizadas, isto é, as ações não são controladas integralmente por computador. Pessoas podem contribuir para um "diálogo sutil" enquanto a máquina executa tarefas automatizadas em grande escala. Porém, quando os *bots* são combinados com inteligência artificial, eles realizam um grande volume de sofisticadas operações à velocidade de algoritmos (veja a Figura).

Conclusão

Uma guerra de nova geração será dominada pela guerra psicológica e informacional, que buscará obter um controle superior ao das tropas e das armas, minando, moral e psicologicamente, os exércitos inimigos e seu povo. Na contínua revolução das tecnologias da informação, as guerras psicológica e informacional prepararão, em grande medida, o caminho para a vitória.

—*Military Thought* russo, 2013[26]

Pode-se argumentar que a maior fraqueza estratégica de qualquer país é interna, não externa. Os líderes precisam entender melhor o conceito de segurança cibernética social, a fim de evitar que as vulnerabilidades internas sejam manipuladas por forças externas. Nós, como líderes militares, precisamos entender que uma das linhas de esforço de uma *blitzkrieg* informacional será abrir uma brecha de desconfiança entre nós e a sociedade que protegemos, bem como entre a liderança civil que nos lidera. Uma instituição sem credibilidade não receberá investimentos adequados, será subutilizada e terá um desempenho insatisfatório.

Se uma das nossas missões principais é "manter a influência norte-americana no exterior", então precisamos descobrir nosso papel em promover os valores dos EUA nesse mercado internacional de crenças e ideias, como parte de um esforço interagências coordenado. Esse esforço vai desde a interação *on-line* a um simples aperto de mão de um comandante de pelotão desdobrado no exterior.

Os líderes militares precisam adotar políticas e estratégias que proporcionem liberdade de manobra em ambientes informacionais relevantes. Um recente relatório de operações de informação da RAND Corporation concluiu que o Departamento de Defesa precisa mudar suas políticas para permitir a manobra ética dentro do domínio informacional em sua plenitude[27]. A maioria dos adeptos da segurança cibernética social (tanto os criadores quanto os defensores dos *bot*) usa as API e tecnologia de fonte aberta para acessar e manobrar no ambiente virtual de dados. Em outras palavras, as API são a porta de entrada tanto para as operações cibernéticas sociais ofensivas quanto as defensivas. Nas Forças Armadas, as normas e as autoridades que regulam o acesso às API são severamente restritas para algumas organizações enquanto não são bem definidas para outras. Precisamos de políticas ágeis que fomentem a iniciativa em um ambiente informacional dinâmico enquanto protegem a privacidade de indivíduos bem intencionados e permaneçam dentro dos limites da autoridade que compete ao Departamento de Defesa.

Em resumo, precisamos educar diretamente nossa Força e informar indiretamente nossa sociedade sobre a natureza descentralizada do moderno ambiente informacional e os riscos que nele existem. Precisamos, também, difundir os métodos e os meios para filtrar individualmente fatos e opiniões que assimilamos e que inadvertidamente permitimos que moldem nossas crenças e atitudes. Precisamos desenvolver uma abordagem multidisciplinar para a segurança cibernética social. Necessitamos elaborar normas relevantes que instrumentalizem a segurança cibernética social. Precisamos buscar remover qualquer brecha de desconfiança artificialmente criada entre as Forças Armadas e a sociedade que defendemos. Temos que definir o papel do Departamento de Defesa no esforço interagências para se contrapor à *blitzkrieg* informacional que enfrentamos hoje. A segurança cibernética social é uma disciplina imprescindível para o futuro próximo. ■

Este trabalho foi apoiado, em parte, pelo Office of Naval Research (ONR) Multidisciplinary University Research Initiative Award N000141812108, Office of Naval Research Minerva Awards N00014-13-1-0835/N00014-16-1-2324, e pelo Center for Computational Analysis of Social and Organization Systems (CASOS). As opiniões e conclusões expressas neste artigo são de inteira responsabilidade dos autores e não correspondem necessariamente às posições oficiais do ONR ou do governo dos EUA.

Referências

1. Kathleen M. Carley et al., "Social Cyber-Security", in *Social, Cultural, and Behavioral Modeling: 11th International Conference, SBP-BRiMS 2018*, Washington, DC, USA, July 10–13, 2018, *Proceedings*, ed. Halil Bisgin et al. (New York: Springer, 2018), p. 389–94.

2. Joshua Yaffa, "Dmitry Kiselev Is Redefining the Art of Russian Propaganda", *The New Republic* (website), 1 Jul. 2014, acesso em: 14 nov. 2018, https://newrepublic.com/article/118438/dmitry-kiselev-putins-favorite-tv-host-russias-top-propogandist.

3. Stephen Townsend, "Accelerating Multi-Domain Operations: Evolution of an Idea", Modern War Institute at West Point, 23 Jul. 2018, acesso em: 14 nov. 2018, https://mwi.usma.edu/accelerating-multi-domain-operations-evolution-idea/; 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. 23–29.

4. Carley et al., "Social Cyber-Security".

5. "Legacy Homepage", U.S. Department of Defense, acesso em: 16 nov. 2018, https://dod.defense.gov/.

6. Peter Pomerantsev, "Russia and the Menace of Unreality: How Vladimir Putin is Revolutionizing Information Warfare", *The Atlantic* (website), 9 Sep. 2014, acesso em: 14 nov. 2018, https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

7. Gerasimov, "The Value of Science is in the Foresight".

8. Charles K. Bartles, "Getting Gerasimov Right", *Military Review* 96, no. 1 (January-February 2016): p. 30–38.

9. Ibid.

10. Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia", *Connections: The Quarterly Journal* 15, no. 1 (2016): p. 5–31.

11. Harold D Lasswell, "The Strategy of Soviet Propaganda", *Proceedings of the Academy of Political Science* 24, no. 2 (1951): p. 66–78.

12. Tim Johnson, "Exclusive: 'Little Russian Media Project' Tries to Turn America against Itself", McClatchy, última atualização 10 Jun. 2018, acesso em: 21 dez. 2018, https://www.mcclatchydc.com/news/nation-world/national/national-security/article213403299.html.

13. Alexander Malkevich (@McCevich), "Jornalista. Homem de mídia. Uma pessoa interessada na vida. E ele não tem medo de trabalhar nas regiões da Rússia. E em nome da Rússia [em russo]", Twitter, acesso em: 21 dez. 2018, https://twitter.com/McCevich.

14. Peter Zeihan, *The Accidental Superpower: The Next Generation of American Preeminence and the Coming Global Disorder* (New York: Twelve, 2014).

15. John Biersack e Shannon O'Lear, "The Geopolitics of Russia's Annexation of Crimea: Narratives, Identity, Silences, and Energy", *Eurasian Geography and Economics* 55, no. 3 (2014): p. 247–69.

16. Robert D. Kaplan, "The Revenge of Geography", *Foreign Policy*, no. 172 (2009): p. 96–105.

17. James A. Gavrilis, "A Model for Population-Centered Warfare: A Conceptual Framework for Analyzing and Understanding the Theory and Practice of Insurgency and Counterinsurgency", *Small Wars Journal*, 10 May 2009, acesso em: 14 nov. 2018, https://smallwarsjournal.com/blog/journal/docs-temp/241-gavrilis.pdf.

18. Bartles, "Getting Gerasimov Right".

19. Lasswell, "The Strategy of Soviet Propaganda".

20. Fabio Rugge, "'Mind Hacking': Information Warfare in the Cyber Age", Analysis No. 319, Italian Institute for International Political Studies, 11 Jan. 2018, acesso em: 14 nov. 2018, https://www.ispionline.it/en/pubblicazione/mind-hacking-information-warfare-cyber-age-19414.

21. Elisa Shearer e Jeffrey Gottfried, "News Use Across Social Media Platforms 2017", Pew Research Center, 7 Sep. 2017, acesso em: 14 nov. 2018, https://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

22. Robert F. Baumann, "A Central Asian Perspective on Russian Soft Power: The View from Tashkent", *Military Review* 98, no. 4 (July-August 2018): p. 50–63.

23. O acrônimo "BEND" (em inglês) se deriva das 16 formas de manobra apresentadas na Tabela: quatro começam com a letra "B", quatro com "E", quatro com "N" e quatro com "D".

24. Ben Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It", *Central European Policy Institute* 15 (2015).

25. Cristian Lumezanu, Nick Feamster e Hans Klein, "#bias: Measuring the Tweeting Behavior of Propagandists", *Proceedings of the Sixth International Conference on Weblogs and Social Media* (Palo Alto, CA: The AAAI Press, 2012), p. 210–17; John-Paul Verkamp e Minaxi Gupta, "Five Incidents, One Theme: Twitter Spam as a Weapon to Drown Voices of Protest" (apresentação de estudo, 3rd USENIX Workshop on Free and Open Communication on the Internet, Washington, DC, 13 Aug. 2013), p. 1–7; Rosie Alfatlawi, "Thousands of Twitter Bots Are Attempting to Silence Reporting on Yemen", *Al Bawaba: The Loop*, 22 Nov. 2017, acesso em: 16 nov. 2018, https://www.albawaba.com/loop/original-saudi-bots-yemen-suffering-1051564; Matthew Benigni e Kathleen M. Carley, "From Tweets to Intelligence: Understanding the Islamic Jihad Supporting Community on Twitter", in *Social, Cultural, and Behavioral Modeling: 9th International Conference, SBP-BRiMS 2016*, Washington, DC, USA, June 28–July 1, 2016, *Proceedings*, ed. Kevin S. Xu et al. (New York: Springer, 2016), p. 346–55.

26. Sergey G. Chekinov e Sergey A. Bogdanov, "The Nature and Content of a NewGeneration War", *Military Thought* 4 (2013): p. 12–23.

27. William Marcellino et al., "Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations" (Santa Monica, CA: RAND Corporation, 2017).