revista Fronteiras – estudos midiáticos
22(1):11-20 janeiro/abril 2020
Unisinos – doi: 10.4013/fem.2020.221.02

Comunicação militarizada: a internet e os novos formatos da guerra

Militarized communication: the internet and the new formats of war

Sérgio Amadeu da Silveira[1]
sergio.amadeu@ufabc.edu.br

João Francisco Cassino[1]
cassino@gmail.com

RESUMO

O presente artigo tem por objetivo abordar os principais conflitos digitais que ocorrem no âmbito de uma Internet militarizada. Debate como os atores não-estatais ganharam força e desequilibraram o poder dos Estados Nacionais usando do meio digital. Detalha as diferenças entre as Guerras Convencionais e outras formas de guerra que combinam tipos de ações indiretas para destruir o inimigo. Mostra como surge o conceito de Guerra Híbrida e a falta de consenso sobre o que isso significa com exatidão. Esclarece as distinções entre *Netwar* (Guerra em Rede) e *Cyberwar* (Ciberguerra). Examina como as técnicas de captura, armazenamento em massa e processamento de gigantescas bases (*Big Data*) contribuem para a espionagem e para a vigilância generalizada em nossa sociedade conectada. Por fim, questiona se é possível, na atual realidade, ter perspectivas de uma desmilitarização da Internet.

Palavras-chave: Militarização. Ciberespaço. Vigilância.

ABSTRACT

This article aims to address the main digital conflicts that occur within the framework of a militarized Internet. Discuss how non-state actors gained strength and unbalanced the power of national states using the digital environment. Details the differences between conventional wars and other forms of war that combine types of indirect actions to destroy the enemy. Shows how the concept of Hybrid Warfare arises and the lack of consensus on what it means exactly. Clarifies the distinctions between Netwar and Cyberwar. It examines how techniques of capture, mass storage and processing of gigantic bases (big data) contribute to espionage and widespread surveillance in our connected society. Finally, questions whether it is possible, in the present reality, to have prospects of a demilitarization of the Internet.

Keywords: Militarization. Cyberspace. Surveillance.

[1] Universidade Federal do ABC (UFABC). Av. dos Estados, 5001 – Bangú, Santo André (SP).

Introdução

A Internet é infraestrutura elemental para o desenvolvimento do capitalismo contemporâneo. Por ela trafegam os fluxos de capitais em alta velocidade. Os sistemas de comunicação oferecem efetividade e agilidade jamais vistas na história da humanidade. Mas as tecnologias digitais também são armas de guerra nas disputas travadas em quase todas as sociedades. Seja pelo exercício democrático da cidadania, seja pela competição eleitoral ou pelo conflito bélico, independentemente do terreno de luta, os combatentes usarão a Internet para derrotar adversários ou destruir inimigos.

Há várias formas de utilizar a Internet como arma. Para cada forma, cria-se um conceito que tenta descrever como se dão estratégias, táticas e operações. Porém, há muita confusão na hora de usar tais conceitos. Neste artigo, esclareceremos alguns dos termos mais comuns: *guerra na rede* (*netwar*), *guerras centradas em redes sociais*, *guerra cibernética* (*cyberwar*), *guerra híbrida, revoluções coloridas*, *guerras não convencionais* e *guerras de nova geração*. Também mostraremos como operam a vigilância, a espionagem e a coleta de dados em massa em um cenário de Internet militarizada. Registre-se que esta abordagem é apenas uma visão das muitas possíveis e para alguns termos não há consenso estabelecido. Este texto não tem a pretensão de esgotar o tema, mas busca esclarecer nomenclaturas com base em referencial teórico.

Primeiramente, relembremos a origem da Internet. Surge no cenário de Guerra Fria, dentro da *Advanced Research Projects Agency* (ARPA), organizada pelo Departamento de Defesa dos Estados Unidos da América, no final dos anos 1960 e início dos anos 1970. A missão era criar uma rede de arquitetura distribuída, que pudesse resistir a um ataque nuclear, pois uma rede centralizada, com pontos centrais de interconexão, seria alvo fácil. O engenheiro Paul Baran, que integrou o time da ARPA, escreveu que a agência queria mobilizar recursos de pesquisa para superar em tecnologia militar a União das Repúblicas Socialistas Soviéticas (URSS), que, em 1957, lançara o primeiro satélite artificial na órbita do planeta Terra (BARAN, 1964). Apesar da forma como nasceu, os militares não foram decisivos para a expansão da Internet e não controlaram as tecnologias que levaram a rede a se estruturar mundialmente. As aplicações militares acabaram por ser secundárias ao projeto (CASTELLS, 2003, p.20). Porém, isso não significa que a Internet não seja um espaço militarizado.

Foi no período dos presidentes norte-americanos Dwight D. Eisenhower (1953-1961), John F. Kennedy (1961-1963) e Lyndon B. Johnson (1963-1969) que o termo *militarização do espaço* passou a ser utilizado corriqueiramente quando se tratava de ações aeroespaciais, principalmente entre os anos 1946 e 1967, conforme demonstrou pesquisa de Sean N. Kalic. Como *militarização*, incluía-se o uso de sistemas baseados no espaço para coletar, reunir e disseminar inteligência fotográfica, dados de comunicações, meteorológicos, inteligência de sinais e reconhecimento estratégico (KALIC, 2012, p.5-6). A militarização das redes não se refere necessariamente à destruição de dados sensíveis ou à invasão de sistemas computacionais. Também não se limita a operações estritamente de combate, como seu nome pode sugerir. A expressão *militarização* engloba práticas aplicadas para garantir a segurança nacional ou projetar poder político-econômico. Ao final da segunda década do Século XXI, o fluxo de dados que percorre a Internet passou a ser constantemente vigiado pelos principais serviços de inteligência do mundo e pelas forças armadas de quase todos os países.

Quando os atentados de 11 de setembro de 2001 derrubaram as Torres Gêmeas em Nova Iorque, surgia uma novo *regime de verdade*[2], no sentido utilizado por Michel Foucault. Ampliar a militarização da Internet era necessário para enfrentar o terrorismo internacional e outras ameaças globais. As Tecnologias de Informação e Comunicação (TICs), que na época se popularizavam pelo planeta, estavam alterando o equilíbrio de poder entre as nações. Universidades e *Think Tanks* intensificaram os estudos de possíveis cenários de conflitos na era digital. John Arquila e David Ronfeldt, consultores da RAND Corporation[3], já haviam escrito, quase dez anos antes, que a revolução informacional mudaria a forma como as sociedades entrariam em conflito e como suas forças armadas entrariam em guerra . Eles advertiram que novos atores surgiriam no cenário global: movimentos sociais, ativistas, organizações não-governamentais, grupos criminosos

[2] Para Foucault, as sociedades possuem seus regimes de verdade, "tipos de discurso que elas acolhem e fazem funcionar como verdadeiros". Uma das características dessa economia política da verdade "é centrada na forma do discurso científico e nas instituições que o produzem"… "é objeto de debate político e de confronto social (as lutas 'ideológicas')". (FOUCAULT, 1979, p. 12-13)
[3] A Rand Corporation é um dos principais think tanks norte-americanos.

e agrupamentos terroristas. Eles atuariam no ciberespaço e dificultariam a manutenção do equilíbrio de poder dos grandes Estados. Arquilla e Ronfeldt usaram a imagem de Atena – a deusa grega da sabedoria – para descrever o novo cenário. Atena substituiria Ares, o deus da guerra. Na era da informação, o conhecimento superaria a força bruta. Aceitar Atena como patrona desse novo tempo ajudaria na prevenção e na preparação para conflitos vindouros. As poderosas nações poderiam ser derrotadas por meio das redes (ARQUILLA, RONFELDT, 1997, p. 25-27, 30).

Joseph S. Nye Jr., teório das relações internacionais, de modo similar, alertou para a importância dos atores não-estatais no contexto do poder global. Nye trabalhou com a metáfora de um tabuleiro de xadrez tridimensional. No tabuleiro superior, o poder seria unipolar, controlado pelos Estados Unidos da América e por sua força militar. O tabuleiro intermediário seria multipolar e nele está o poder econômico, assim como outras nações relevantes como China, Japão e países da Europa. Por fim, no tabuleiro inferior estão as forças que escapam dos controles governamentais, os agentes não-estatais, desde banqueiros (que transferem eletronicamente valores que superam orçamentos de nações) até terroristas e *crackers*[4] que atuam para sabotar e prejudicar operações na Internet. Nesta última camada, segundo Nye, as palavras unipolaridade, multipolaridade ou hegemonia não fazem sentido. Ele afirma que ali os governos perderam parte do controle sobre a informação em suas próprias sociedades e que é muito mais difícil controlar a Internet do que foi controlar as tecnologias da segunda revolução da informação (NYE, 2002, p.80, 95-100). Oito anos mais tarde, Nye publica o livro *Cyberpower* (2010), no qual confirmou seus temores diante das redes digitais. Defendeu que mesmo que não substitua o espaço geográfico, mesmo que não encerre a soberania estatal, o ciberespaço altera profundamente a difusão do poder e de seu exercício. Os EUA exercem poder nos céus, nos mares e nas terras do planeta, mas têm mais dificuldade de praticar esse domínio no ciberespaço. Apesar de continuar assimétrico, o poder dos pequenos atores não-estatais cresceu com a Internet (NYE, 2010, p.19).

O diplomata britânico Nicholas Westcott, em *Digital Diplomacy: The Impact of the Internet on International Relations*[5], tem outra perspectiva. Considerou que a Internet trouxe três impactos importantes nas relações internacionais: o primeiro multiplicou e amplificou as vozes e os interesses na formulação de políticas e na tomada de decisões para assuntos exteriores, terreno antes reservado aos Estados nacionais; o segundo foi acelerar a disseminação de informações sobre os acontecimentos, reais e fictícios[6]; e o terceiro permitiu que os serviços diplomáticos tradicionais fossem prestados mais rapidamente, de modo mais eficaz e com custos bem menores (WESTCOTT, 2008, p.2). Arquila, Ronfeldt, Nye e Westcott concordam, portanto, com a fragilização dos Estados em um mundo de redes digitais distribuídas globalmente. E nesse contexto é que se dão as *guerras na rede* (*netwars*), as *guerras cibernéticas* (*cyberwars*) e as *guerras híbridas*.

Guerras na Rede

Segundo a formulação de Arquilla e Ronfeldt, as *guerras na rede* (*netwars*) estão relacionadas a conflitos entre nações ou sociedades. Ocorre quando se tenta atrapalhar, danificar ou modificar o que uma população-alvo pensa sobre o mundo ao seu redor (ARQUILLA, RONFELDT, 1997, p. 28). São claros exemplos de *guerras na rede*: a campanha que levou o Reino Unido a deixar a União Europeia (Brexit), em junho de 2016; a batalha política que Donald Trump travou contra Hillary Clinton nas eleições norte-americanas, também em 2016; e nas candidaturas vitoriosas da extrema direita brasileira nas eleições de 2018, tanto em governos estaduais, quanto no poder central ou nos parlamentos. Nas ilhas britânicas e na América do Norte, a democracia foi afetada por operações em larga escala envolvendo *Big Data* e Inteligência Artificial, como demonstrou-se ao eclodir o escândalo *Facebook–Cambridge Analytica*, no início de 2018. No Brasil, a jornalista Patrícia Campos Mello, da Folha de S.Paulo, ganhou destaque ao publicar reportagem sobre como funcionava a gigantesca rede de produção de notícias (muitas delas falsas) e de envio de mensagens via o aplicativo WhatsApp (MELLO, 2018), o que influenciaria de maneira determinante a vitória de um desprestigiado candidato à Presidência da República, que, poucos meses antes, só havia conseguido se candidatar por meio de

[4] *Crackers são hackers* criminosos.
[5] *Diplomacia Digital: o impacto da Internet nas Relações Internacionais* (WESTCOTT, 2008), tradução nossa.
[6] As disputas entre nações são também disputas discursivas. A diplomacia se baseia nelas. A ideia chamada de pós-verdade pode ser compreendida como distorções e invenções de relatos sobre fatos tão comuns nas relações internacionais.

um partido nanico e, nas vésperas da inscrição do pleito, coligou-se somente com outra legenda igualmente insignificante, apesar de aparecer sempre em primeiro ou em segundo lugar nas pesquisas de intenção de votos. Não há como fazer uma análise simplista e afirmar categoricamente que o aplicativo de mensagens eletrônicas foi a única ou principal causa do resultado brasileiro, mas é um elemento que não pode ser desprezado em nenhuma avaliação política. O que se pode dizer é que Brexit, Trump e Bolsonaro são casos bem-sucedidos de *netwar*. Com as *guerras na rede*, o conflito acontece na camada da informação, do convencimento da opinião popular.

Muito parecida com as *guerras na rede*, a *guerra centrada em rede social* (termo usado por Andreew Korybko) se organizaria de forma dispersa, em pequenos grupos e indivíduos, que se comunicam e coordenam campanhas conectadas na Internet, geralmente sem um comando central preciso. O Facebook tem um papel importante por reunir perfis psicológicos criados voluntariamente, conteúdos de interesse (baseados em *curtidas*) e redes de amigos e de grupos *online*, o que facilita a *publicidade dirigida* preparada para potencializar os mecanismos de projeção (uso de tecnologias de *Big Data*). O objetivo de uma inteligência estrangeira que faz uso desse tipo de recurso seria se infiltrar nas redes sociais e criar uma *mente de colmeia* para que seus membros formem um *enxame* contra um determinado inimigo (geralmente um governo) e, de maneira aparentemente caótica, o levem ao colapso. A partir daí, insurgem as massas contra centros simbólicos e contra centros administrativos das autoridades até que o regime caia pela lei aglomeração (KORYBKO, 2015, p. 45). Francisco Carlos Teixeira, professor visitante da Universidade de Berlim, mostra em seu artigo *O Faraó, Camelos e o Facebook* (2011) como Egito e Tunísia, cujos governos estavam há décadas no poder, foram derrubados por movimentos iniciados no ambiente virtual das redes sociais. (TEIXEIRA, 2011). As *guerras na rede* se diferem das *guerras centradas em rede social* por utilizarem recursos, *softwares* e aplicativos de maneira mais abrangente.

Ciberguerras

Já as *ciberguerras* (*cyberwars*) ocorrem, segundo definição de Arquilla e Ronfeldt, quando as redes e os sistemas digitais são utilizados militarmente para interromper e/ou destruir sistemas de informação e comunicação inimigos. Podem ser travadas com o objetivo de se conhecer melhor o rival. Saber onde ele está, do que é capaz, quais suas motivações, quais ameaças devem ser contidas. Trata-se de fazer pender a balança de informação e conhecimento (ARQUILLA, RONFELDT, 1997, p. 30).

Um exemplo claro de *cyberwar* foi o ataque às centrífugas de enriquecimento de urânio da República Islâmica do Irã utilizando o Stuxnet, um *worm* (verme) de computador projetado para reprogramar e danificar sistemas industriais. Revelado em 2010 por uma empresa da Bielorrússia, que desenvolve o antivírus VirusBlokAda, o Stuxnet foi criado para atacar o *Sistema de Supervisão e Aquisição de Dados – SCADA*[7], um software produzido pela Siemens, que controlava as centrífugas iranianas. Motivada pelo episódio, a imprensa mundial passou a debater os perigos e o potencial de destruição desse tipo de ação de guerra. Dentre os especialistas de segurança e de defesa, o Stuxnet alimentou a produção de pesquisas e discussões. Quem poderia ter lançado Stuxnet? O *worm* realmente destruiu os sistemas de controle nuclear? O que mais ele danificou? Por que ninguém assume sua autoria? Teria sido desenvolvido pelos EUA ou Israel, grandes inimigos dos iranianos? Se sim, por qual razão o Stuxnet seria encontrado em máquinas na Ásia e na América do Norte? Para o pesquisador francês Daniel Ventre, o caso Stuxnet confirma o que já se sabia: ataques virtuais invisíveis, totalmente anônimos, são possíveis, inclusive os de bandeira falsa. Para Ventre, a mentira é uma arma por direito próprio no jogo entre os atores de poder nas relações internacionais. A *cyberwar* pode ser efetuada sem que seja necessário assumir os ataques, ou seja, pode ser empregada mesmo que um governo desminta sua participação em uma ação cibernética destrutiva (VENTRE, 2011, p. 215, 231-233). A *cyberwar* difere da guerra tradicional, a começar pela possibilidade de ser desfechada sem uma declaração formal.

Por outro lado, em sua argumentação, Ventre afirma que não seria correto elevar demasiadamente o peso das assimetrias no ciberespaço, uma vez que todos – exércitos regulares, grupos criminosos e *hackerativistas* – têm acesso às mesmas armas e aos mesmos recursos, o que geraria capacidades equivalentes (VENTRE, 2011, p. 221). Ventre parece desconsiderar as diferenças brutais de capacidade de poder de processamento computacional e de infraestrutura, algo bastante ressaltado por Joseph

[7] *Supervisory Control and Data Acquisition* – SCADA.

Nye. Não há como comparar um ou dois servidores mal armazenados debaixo de uma mesa de um *hacker* contra um parque de milhares de computadores das grandes empresas de tecnologia ou mesmo de agências estatais.

O fato é que tanto as *guerras na rede* quanto as *guerras cibernéticas* são travadas por meio da comunicação e da informação. Giram em torno dos conhecimentos, da capacidade de coletar dados, processá-los e analisá-los. Trata-se de um tipo específico de poder: o poder de análise, entendido como uma capacidade cada vez mais importante de extrair da manipulação de dados a ampliação do conhecimento que se têm sobre os elementos que se pretende controlar e dominar. Das sangrentas campanhas de Genghis Khan aos conselhos de Maquiavel ao Príncipe, o conhecimento sempre foi fundamental para o sucesso na guerra. As tecnologias cibernéticas trouxeram uma nova qualidade para o tratamento de informações e sua transformação em bens, em produtos imateriais e na multiplicação do conhecimento.

Guerras Híbridas

Guerra Híbrida tem sido um termo bastante popular nos últimos anos e é usado com frequência pela mídia e por analistas políticos, notadamente após a eclosão da Guerra Civil no Leste da Ucrânia, iniciada em março de 2014. O problema é que há centenas de reportagens e de artigos que usam essa nomenclatura sem definir seu significado. Não é raro ver esse conceito aplicado de maneira incorreta. Vulgarmente, o termo *Guerra Híbrida* tem sido utilizado para definir qualquer combinação de mecanismos – militares ou civis – para se destruir um inimigo e derrubar governos. Cabem nessa definição quase tudo: golpes armados, judicialização da política, criminalização de líderes populares, destruição de reputações pela mídia, processos eleitorais fraudulentos, milícias virtuais, *fake news*, envio de mensagens em massa via ferramentas de comunicação digital (como WhatsApp), dentre outras.

Em nossa opinião, uma guerra – para ser híbrida – precisa combinar os elementos de informação com componentes militares tradicionais de fato, com o uso de armamento bélico real ou, no mínimo, ameaça explícita de usá-los. É verdade que mesmo no meio militar, o termo *guerra híbrida* não goza de unanimidade absoluta. Artigo do Coronel brasileiro Paulo César Leal para a publicação *Doutrina Militar Terrestre em Revista,* publicada em 2016, mostra que, apesar de existir a consciência das *ameaças híbridas*, não há consenso para o uso dessa expressão e nem de seu exato significado. Cada país trata do mesmo problema com escopo diferenciado. Os Estados Unidos não incorporaram o termo *guerra híbrida* em sua *Estratégia Nacional Militar* (2015), mas descrevem o aumento da complexidade dos conflitos e a necessidade de resiliência e da capacidade de adaptação das forças armadas frente a característica do inimigo a ser enfrentado. O Brasil, em seu *Manual de Fundamentos EB20-MF-10.103 OPERAÇÕES* (2014), limita-se a estabelecer que o Exército Brasileiro deve preparar a Força Terrestre para contemplar *todo o espectro dos conflitos* (Guerra e Não Guerra). Já o Reino Unido conta com a *77ª Brigada contra Guerra Híbrida*, que mistura múltiplas ferramentas de guerra convencional e não convencional (forças regulares, irregulares e especiais, apoio à manifestações locais, guerra de informação, diplomacia, ataques cibernéticos e guerra econômica). Os russos, como veremos adiante, também têm outro entendimento. Em síntese, as definições, apesar de próximas e de tratar mais ou menos do mesmo assunto, não são iguais, o que gera problemas para quem quer avaliar um fato político com precisão. O termo *guerra híbrida* ainda está em formação. Ressalte-se que nos casos citados pelo Coronel Leal sempre há a coordenação central de um Estado Nacional interessado no conflito, mesmo que inclua em seu método a participação de atores não-estatais.

Em 2015, Andrew Korybko publicou o livro *Hybrid Wars: The Indirect Adaptive Approach To Regime Change*[8]. Seu objeto de pesquisa é a estratégia norte-americana com nova abordagem padronizada para trocas de regimes. Ele parte do princípio de que o domínio da Eurásia é a chave para o domínio global. E que os EUA estão decididos a quebrar a influência da Rússia, principalmente nos Bálcãs, no Oriente Médio, no Cáucaso e na Ásia Central. Como uma guerra convencional – exército contra exército – é inviável, já que há sérios riscos de um conflito nuclear aniquilador, os Estados Unidos passaram a utilizar, na visão de Korybko, formas indiretas: a combinação de *Revoluções Coloridas* e de *Guerra Não-convencional*.

Revoluções Coloridas

Por *Revoluções Coloridas* entende-se operações psicológicas para conquistar demografias-alvo específi-

[8] *Guerras Híbridas: a abordagem adaptativa indireta com vistas à troca de regime* (KORYBKO, 2015), tradução nossa.

cas. Forma-se um movimento de pessoas grande o bastante para confrontar o Estado e tentar derrubá-lo. As mídias sociais e a Internet passaram a oferecer a oportunidade de penetrar nas mentes das populações, disseminando informações para *fabricar consenso*. Para tanto, usa notícias criadas artificialmente com fins de publicidade. O nome *revoluções coloridas* vem dos movimentos que sacudiram algumas repúblicas da ex-União Soviética, como a *Revolução Rosa* na Geórgia (2003), a *Revolução Laranja* na Ucrânia (2004) e a *Revolução das Tulipas* no Quirguistão (2005). Em todos os três casos, foram levantes que questionaram resultados eleitorais naqueles países. O grande problema da visão de Korybko é que ela não aborda levantes similares que são contrários aos interesses dos EUA, como os protestos sociais no Chile contra a política neoliberal do Presidente Piñera, que se iniciaram no final de 2019.

Guerras Não Convencionais

A *Guerra Não Convencional*, por sua vez, consiste em apoiar movimentos de resistência ou de insurgência, abalando ou derrubando um governo com uma força clandestina e guerrilheira. Tratam-se de ataques reais, que envolvem conflito armado, insurreição urbana, sabotagem e terrorismo. Um exemplo é a Guerra da Síria, iniciada em 2011, que tem por combatentes a República Árabe da Síria (o governo oficial, que conta com suporte russo e iraniano), a oposição síria (que tem apoio de EUA e Israel) e a organização terrorista Estado Islâmico. Outro exemplo seria as ações contra a República Bolivariana da Venezuela, que sofre com ameaças explícitas de invasão militar do presidente norte-americano Donald Trump, além de sanções econômicas e tentativas de ganhar a adesão do povo venezuelano ao autodeclarado presidente interino Juan Guaidó, reconhecido por EUA, Colômbia e pelo Brasil de Jair Bolsonaro. Em fevereiro de 2019, houve grande tensão quando o recém-empossado governo brasileiro apoiou uma operação supostamente humanitária por terra e mar para tentar entrar na Venezuela.

Na opinião de Korybko, temos uma Guerra Híbrida quando se somam as táticas de *Revolução Colorida* e de *Guerra Não Convencional* (KORYBKO, 2015, p. 28). Com isso, os EUA teriam uma *Dominação de Espectro Total*, somando forças armadas convencionais, armas nucleares, retórica de direitos humanos e dos meios de comunicação e informação, inclusive as *guerras na rede* e as *ciberguerras*. Porém, até novembro de 2019, mesmo após anos de esforços, nem Bashar al-Assad ou Nicolás Maduro haviam sido derrubados do comando de suas nações. Mesmo na Primavera Árabe, alguns episódios agradaram aos EUA, como o caso da Líbia. Porém, a queda do ditador egípicio Hosni Mubarak representou a saída de um aliado do Ocidente e vitória eleitoral da opositora Irmandade Muçulmana. Em maio de 2011, a Espanha viu uma série de protestos espontâneos, inicialmente organizados pelas redes sociais digitais, que contestavam fortemente os atuais modelos democrático e econômico. Em setembro de 2011, o Zuccotti Park, na cidade de Nova Iorque, foi palco do movimento *Occupy Wall Street*, contra a desigualdade econômico-social, contra a ganância e contra a influência das corporações no governo.

Guerras de Nova Geração

No mesmo ano da publicação do livro de Andrew Korybko, um pesquisador do Instituto Finlandês de Relações Internacionais, András Rácz, lança *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*[9], com o qual detalha como a Federação Russa pratica a *guerra híbrida* contra a Ucrânia. Aqui há uma contradição fundamental: se aceitarmos a opinião de Rácz, automaticamente negamos a teoria de Korybko de que a Guerra Híbrida é um método de guerra indireta perpetrado pelos EUA. Rácz explica que a assimetria na guerra esteve presente desde sempre, já que um dos exércitos invariavelmente é mais forte do que o outro. Afirma que o termo *guerra híbrida foi* criado pelo Major William J. Nemeth, dos EUA, em 2002, em uma tese sobre o conflito da Chechênia. O termo nasceu com um significado completamente diferente de como é utilizado por Korybko: tratava de um conflito entre um Estado contemporâneo (Rússia) contra uma sociedade pré-moderna, de clãs e laços familiares (Chechênia). A sofisticada e moderna tecnologia de uma potência militar enfrentaria guerrilhas, que tinham nas suas táticas e na fluidez de suas operações os principais recursos combater um grande exército regular (RÁCZ, 2015, p. 29). Rácz também afirma que o que chamamos nos dias de hoje de *Guerra Híbrida* no Ocidente é denominado como *Guerra de Nova Geração* na Rússia. Seriam dois nomes para o mesmo fenômeno. As

[9] *Guerra Híbrida da Rússia na Ucrânia: Destruindo a Habilidade do Inimigo Resistir* (RÁCZ, 2015), em tradução livre.

operações russas no conflito ucraniano faz uso combinado de diplomacia, economia, política e outros métodos não-militares em conjunto com a força militar direta, em vez de uma simples guerra aberta. Inclui-se nessa estratégia o uso de paramilitares, unidades civis insurgentes, destruição da infraestrutura do inimigo e até mesmo armas robóticas, como *drones*.

Vigilância e espionagem

Apresentada a tipologia de conflitos na Internet e/ou que fazem uso da rede, como analisá-los? As opiniões de Arquilla, Ronfeldt e Joseph Nye Jr. convergem para uma visão em que terrorismo, organizações criminosas, movimentos sociais e ativismos como possíveis ameaças ao poder dos Estados nacionais, já que a comunicação distribuída e o anonimato nas redes digitais permitiriam que pequenos coletivos adquirissem poder de disseminar informações, de articular ações públicas ou secretas em rede e realizar ataques a alvos conectados a computadores. Consequentemente, exige-se das forças estatais nova postura e novas ações para garantir a segurança de seus cidadãos.

O ponto central é a mudança de mentalidade que ocorre após o 11 de Setembro. A vigilância passa de *focalizada* para ser *em massa*. Antes, se alguém era suspeito, tornava-se alvo de investigação. Agora, dados de todos e todas são coletados pela Internet diariamente e armazenados. Todos são vigiados em tempo integral. Usar ou não usar as informações contra seus titulares é opção dos que controlam os bancos de dados. O que tornou essa prática possível foi a evolução tecnológica. A emergência do *big data,* do *data mining* e o surgimento de técnicas de cruzamento de dados permitiram que o poder computacional de países e empresas fosse utilizado para fazer operações como vasculhar o ciberespaço; capturar expressões e palavras consideradas suspeitas; observar as trocas de mensagens pessoais; vigiar os assuntos mais requisitados em ferramentas de buscas (como Google); e fazer correlações em velocidade antes inimaginável. A *National Security Agency* (NSA) se preparou para explorar falhas e quebrar códigos daquilo que é comunicado e considerado de interesse dos EUA e de seus aliados. Como explicou Greenwald, a NSA é um braço do Pentágono e a maior agência de inteligência do mundo. Dentre os anos de 2005 e 2014, ela cresceu de forma agressiva em tamanho e influência (GREENWALD, 2014, p.102).

Após o 11 de Setembro

Só há como compreender o desenvolvimento dos acontecimentos se revisitarmos os anos que se seguiram aos atentados de 2001 em Nova Iorque e em Washington. O 11 de Setembro seria prova contundente de que os serviços militares, policiais e de inteligência precisavam aumentar a segurança e reduzir as restrições às ações preventivas aos ataques terroristas. No primeiro capítulo do livro *Estado de Exceção*, Giorgio Agamben argumenta que o "*significado imediatamente biopolítico do estado de exceção como estrutura original em que o direito inclui em si o vivente por meio de sua própria suspensão"* (AGAMBEN, 2004, p.14). Um exemplo seria a *Ordem Militar de 13 de novembro de 2001*, assinada pelo Presidente George W. Bush, que estabelecia comissões militares para julgar indivíduos conectados com o terrorismo internacional. A lei autorizava a detenção indefinida dos acusados que nem eram *"prisioneiros nem acusados, mas apenas detidos"* (AGAMBEN, 2004, p.14). Passavam a ser objeto de uma dominação pura de fato, de uma medida fora da lei e do controle judiciário.

Após o 11 de Setembro produziu-se várias outras medidas de exceção, muitas delas inclusas no *USA Patriot Act*, promulgado pelo Senado, em 26 de outubro de 2001. Uma delas dizia respeito à capacidade das agências de segurança e inteligência de coletar todas as informações necessárias para combater uma ameaça terrorista. A seção 215 do *Patriot Act* alterava a *Lei de Vigilância de Informações Estrangeiras*[10], de 1978, concedendo ao FBI o poder de acessar e observar *qualquer coisa tangível*, incluindo consultas em livrarias e registros de leitura em bibliotecas, sem nenhuma ordem judicial, desde que a investigação fizesse parte de ações antiterroristas. Foram criados ainda vários outros dispositivos que ampliavam o poder da inteligência para perseguir o dinheiro de organizações terroristas e de investigar os dispositivos eletrônicos de pessoas suspeitas, sem limites territoriais. A Guerra ao Terror passou a ter prioridade máxima. Se constituiu um momento *hobbesiano*: a sociedade aceitava abrir mão de direitos em função do combate ao mal maior, o terrorista. Mas onde estaria a nova célula agressora? Como estariam escondidos? Qual seria seu novo plano de ataque?

[10] *Foreign Information Surveillance Act.*

O discurso oficial consolida a necessidade de utilizar as tecnologias de processamento de informações para prevenir e impedir novos ataques. Vasculhar as redes digitais e penetrar nos esconderijos onde os inimigos planejam ações torna-se uma atividade tecnicamente possível, doutrinariamente embasada e politicamente necessária. Os Estados Unidos contavam agora com um aparato legal que permitia utilizar suas empresas nesta tarefa. As grandes corporações de tecnologia da informação são principalmente norte-americanas e estão submetidas às suas leis. O governo brasileiro ou de um país europeu não consegue acessar o banco de dados de uma empresa como a Google, nem tem como saber quais assuntos, temas ou palavras estão sendo procurados pelas pessoas. Washington possui essa condição, já que as corporações colaboram com as agências de Estado. Em março de 2018, o jornal britânico *The Guardian* publicou matéria em que demonstrou como a inteligência artifical do Google está sendo usada pelo programa militar de *drones* do Departamento de Defesa dos EUA (GIBBS, 2018, *online*). Fatos como esse comprovam a colaboração entre Governo e corporações. Tal sinergia já acontecia mesmo antes da queda das duas torres. A *Communications Assistance for Law Enforcement Act* (CALEA), aprovada em 1994, na gestão de Bill Clinton, exigia que toda empresa norte-americana de equipamentos de telecomunicações inserisse em seus produtos dispositivos que asseguressem o acesso das agências de segurança e inteligência. O texto original excluía a Internet, mas a *Eletronic Frontier Foundation* (EFF) analisou minuciosamente a aplicação da lei e concluiu que a CALEA é utilizada para a interceptação do fluxo de informações de provedores de Internet, ao menos desde 2005. Alegando risco de *"ameaças à segurança nacional"*, o Presidente Donald Trump, em meio a sua guerra comercial com a República Popular da China, anunciou que iria banir as gigantes chinesas de telecomunicações Huawei e ZTE, em novembro de 2019. Para a administração Trump, a Huawei, empresa líder mundial de equipamentos 5G, é um "cavalo de Troia" do regime chinês para captura de informações (AFP, 2019, *online*).

A acusação de Trump contra a China é prática dos EUA há muitos anos. Edward Joseph Snowden, analista de sistemas que trabalhou para a *Central Intelligence Agency* (CIA) e para a NSA, denunciou, em 2013, a existência de um esquema global de espionagem massiva, que não é realizada diretamente pelo aparato de segurança militar e de inteligência do Estado, na maioria dos casos. A tarefa é realizada pelas corporações de tecnologia que tanto encantam as populações no planeta: Facebook, Google, Microsoft, Apple e Amazon penetram a intimidade dos usuários e nela encontram seu real produto. A comercialização de dados pessoais – tratados, qualificados e segmentados – para disseminar ideias ou impulsionar a venda de produtos e serviços próprios ou de terceiros. O que sustenta economicamente esses colossos corporativos do mundo informacional é justamente esse mercado de dados pessoais. Há uma relação direta entre militarização da Internet, sistemas de vigilância global e mercados dominados pela doutrina neoliberal.

É possível desmilitarizar a Internet?

Deleuze escreveu um pequeno e perturbador texto chamado *Post-scriptum sobre as sociedades de controle* em que afirmava ter realizado uma descoberta assombrosa – *as empresas tinham uma alma* (DELEUZE, 1992, p.224). Tal alma era o *marketing,* que passou a exigir mais e mais informações sobre os consumidores. Logo, tornou-se um poderoso instrumento de controle e de formação de subjetividades. As pessoas passaram a amar suas corporações. Encantaram-se e passaram a adorar entregar seus dados pessoais para melhorar suas experiências em produtos e serviços. A competitividade corporativa é também a disputa pelo afeto dos seus consumidores. Quem vigia seus clientes pode saber e prever gostos e comportamentos. As corporações contam com departamentos especializados em vigiar, em acompanhar e em compreender compradores – sejam existentes ou potenciais. A professora da Universidade Harvard, Shoshana Zuboff, chama esse sistema econômico de *capitalismo de vigilância.* Seria uma nova forma de poder em que contratos e o estado de direito são trocados por recompensas e punições de um novo tipo de *mão invisível* (ZUBOFF, 2015, p.82). Ela refere-se às dinâmicas de atração e de engajamento que as plataformas criam para manter seus usuários conectados o máximo possível, interagindo com as dinâmicas internas do próprio sistema.

A Microsoft, uma das grandes empresas dessa economia digital, viu seu presidente Brad Smith clamar por uma *Convenção Digital de Genebra*, em 2017, em uma conferência sobre segurança da informação (SMITH, 2017, *online*). Seu discurso deixa clara a militarização da Internet, as operações militares na rede e as projeções de poder das nações que ocorrem no ciberespaço. A voz do dirigente maior de uma das grandes corporações de tecnologia da informação corrobora e legitima as denúncias de coletivos *cyberpunks* e de organizações

independentes, como o Wikileaks. Em seu *blog* oficial, escreve que os conflitos já não se limitam ao solo, ao mar e ao ar. O ciberespaço é um campo de batalha potencial e global. Os governos tendem cada vez mais a explorar e a produzir *softwares* para atingir objetivos de segurança nacional. Brad Smith considera que o plano de batalha do ciberespaço difere dos anteriores, pois ele não existe de forma tangível no mundo físico. Também é produzido e protegido pelo setor privado. Apesar de os governos terem papel fundamental, a infraestrutura é o alvo principal neste tipo de guerra e é propriedade privada de civis. São passíveis de ataque cabos submarinos, *data centers*, servidores, *laptops* e *smartphones*.

Snowden já havia mostrado como o Gabinete da Presidência da República Federativa do Brasil, sob Dilma Rousseff, e a empresa petrolífera estatal brasileira Petrobras haviam sido alvo de espionagem dos EUA. Um fato tão relevante do ponto de vista diplomático que fez com que a Presidenta do Brasil falasse, na abertura da 68ª Assembleia Geral das Nações Unidas, em discurso para 193 representantes dos Estados-Membros, sobre o direito à privacidade e à soberania. Rousseff criticou os norte-americanos e disse que as tecnologias da informação e da comunicação não podem ser o novo campo de batalha estatal. Que era o momento de criar condições para evitar que o ciberespaço fosse usado como arma, para a espionagem, para a sabotagem (ROUSSEFF, 2013).

Infelizmente, já era tarde demais. Em 2010, um relatório do Departamento de Defesa dos EUA, intitulado *The Quadriennal Defense Review*, na edição de fevereiro, analisava os objetivos estratégicos e as potenciais ameaças militares. Eram explícitas as avaliações que cenários de conflitos com estados exigiam a melhoria de capacidades para lutar no ciberespaço (THE QUADRIENNAL, 2010, p.37). E mais: voltando ao discurso de Brad Smith, percebe-se que as corporações não querem o fim da espionagem ou da militarização, mas de regras e proibições para combater na Internet.

Países em desenvolvimento e com importância regional, como o Brasil, podem até criar suas próprias estruturas militares e de vigilância na rede, como o Centro de Defesa Cibernética do Exército (CDCiber). O órgão foi responsável pelas operações cibernéticas durante a Copa do Mundo de 2014 e as Olimpíadas de 2016. Podem criar também legislações, como fez o Congresso Nacional do Brasil ao aprovar a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que busca regular as atividades de tratamento de dados pessoais. A pergunta que não cala, porém, é como órgãos e legislações brasileiras poderão bloquear os interesses geopolíticos dos países do centro do capitalismo mundial?

Considerações finais

O presente artigo procurou esclarecer conceitos utilizados para abordar os conflitos que ocorrem na Internet e/ou que fazem uso dela como instrumento de combate. Explicou-se que a Internet nasceu dentro do meio militar, apesar das forças armadas não terem tido papel ativo na sua difusão e desenvolvimento. A Internet, no entanto, mantém-se militarizada, entendendo-a como um espaço vital para a garantia da segurança das nações e de projeção de poder. Somam-se as redes de atores não-estatais – inimigos ou colaboradores dos Estados – alterando a balança de equilíbrio de poder global. Surgem conflitos de novos tipos, seja a *netwar* (restrita à guerra de informação) ou a *cyberwar* (cujas ações cibernéticas visam destruir instalações e infraestrutura do inimigo). Aparece também o termo *Guerra Híbrida*, mais complexo que os anteriores, combinando recursos tradicionais e não tradicionais, sejam militares, civis ou digitais, não ocorrendo, portanto, no âmbito exclusivo do espaço virtual. Na Rússia, *Guerra Híbrida* é chamada por *Guerra de Nova Geração*. Para todos os casos, a vigilância e a espionagem são ações que coletam dados pessoais. O registro sistemático dos fluxos de navegação e dos rastros digitais da Internet tornaram-se a principal fonte de renda da economia informacional. Se as corporações realizam um tipo de vigilância privada com finalidade econômica, os Estados a realizam com finalidades política, estratégica e militar. Por fim, atualmente a guerra nem é a continuação da política por outros meios, nem a política é a continuação da guerra. Tornou-se, no contexto neoliberal, uma única realidade onipresente: a competitividade virou guerra, espionagem e controle se tornaram aceitáveis e considerados como inevitáveis. A vigilância massiva se realiza a partir da entrega de nossas informações para um conjunto de corporações de tecnologia e de entretenimento, cada vez mais vinculadas aos Estados que as beneficiam e as projetam. Será possível banir operações militares, sabotagem política e vigilância do ciberespaço? As evidências atuais indicam que não.

Referências

AFP. *Huawei anuncia segunda ação judicial contra a administração de Donald Trump*. In: Universo

Online (UOL), 05/12/2019. Disponível em: https://noticias.uol.com.br/ultimas-noticias/afp/2019/12/05/huawei-anuncia-segunda-acao-judicial-contra-a-administracao-de-donald-trump.htm. Acesso em: 12/12/2019.

AGAMBEN, Giorgio. *Estado de Exceção*. São Paulo: Boitempo, 2004.

ARQUILLA, John; RONFELDT, David. *In Athena's camp: preparing for conflict in the information age*. Rand corporation, 1997.

BARAN, Paul. *On distributed communications*. Prepared for United States Air Force Project RAND. The RAND Corporation: Santa Monica, Califórnia, 1964. Disponível em: http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf. Acesso em12/12/2019.

CASTELLS, Manuel. *A galáxia internet*: refelexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003.

DELEUZE, Gilles. Post-scriptum sobre as Sociedades de Controle. In: *Conversações*. São Paulo: Editora 34, 1992.

GIBBS, Samuel. *Google's AI is being used by US military drone programme*. In: The Guardian, 7 mar 2018. Disp.: https://www.theguardian.com/technology/2018/mar/07/google-ai-us-department-of-defense-military-drone-project-maven-tensorflow. Acesso em: 12/12/2019.

GREENWALD, Glenn. *Sem lugar para se esconder*. Rio de Janeiro: Sextante, 2014.

KALIC, Sean N. *US Presidents and the Militarization of Space, 1946-1967*. Texas A&M University Press, 2012.

KORYBKO, Andrew. *Hybrid Wars: the indirect adaptive approach ton regime chance*. Institute for Strategic Studies and Predictions – RPFU. Moscow, 2015. Disponível em: http://orientalreview.org/wp-content/uploads/2015/08/AK-Hybrid-Wars-updated.pdf. Acesso em 12/12/2019.

LEAL, Paulo Cesar. *A Guerra Híbrida: reflexos para o sistema de defesa do Brasil*. Doutrina Militar Terrestre em Revista – volume 4 número 9, p. 7 a 16, 2016. Disponível em: http://ebrevistas.eb.mil.br/index.php/DMT/article/view/722/775. Acesso em11/04/2019.

MELLO, Patrícia Campos. *Empresários bancam campanha contra o PT pelo WhatsApp*. Folha de S.Paulo, 18 de outubro de 2018. Disponível em: https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml. Acesso em12/12/2019.

NYE, Joseph S. *O paradoxo do poder americano*. Por que a superpotência do mundo não pode prosseguir isolada. São Paulo: Editora UNESP, 2002.

NYE, Joseph S. *Cyberpower*. Harvard Univ Cambridge MA Belfer Center for Science and International Affairs, 2010. Disponível em: http://belfercenter.hks.harvard.edu/files/cyber-power.pdf. Acesso em12/12/2019.

QUADRIENNAL Defense Review Report. Washington, DC: Department of Defense. Feb. 2010.

RÁCZ, András. *Russia's Hybrid War in Ukraine Breaking the Enemy's Ability to Resist*. The Finnish Institute of International Affairs, 2015. Disponível em: https://www.stratcomcoe.org/andras-racz-russias-hybrid-war-ukraine-breaking-enemys-ability-resist. Acesso em11/04/2019.

ROUSSEFF, Dilma. *Discurso da Presidenta da República do Brasil*, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas – Nova Iorque/EUA. 24/09/2013. Disponível em: http://www.itamaraty.gov.br/pt-BR/discursos-artigos-e-entrevistas-categoria/presidente-da-republica-federativa-do-brasil-discursos/5898-discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68-assembleia-geral-das-nacoes-unidas-nova-iorque-estados-unidos-24-de-setembro-de-2013. Acesso em12/12/2019.

SMITH, Brad. *The need for a Digital Geneva Convention*. Feb 14, 2017. Disponível em: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention. Acesso em 11/04/2019.

TEIXEIRA, Francisco Carlos. *O Faraó, camelos e o Facebook*. In: Carta Maior, 15 de fevereiro de 2011. Disponível em: https://www.cartamaior.com.br/?/Coluna/O-Farao-camelos-e-o-Facebook/19367. Acesso em: 12/12/2019.

VENTRE, Daniel. Cyberconflict: Stakes of Power. In: *Cyberwar and information warfare* / edited by Daniel Ventre. London, UK; Hoboken, USA: ISTE Ltd and John Wiley & Sons, Inc., 2011.

WESTCOTT, Nicholas. *Digital diplomacy: the impact of the internet on international relations (July 1, 2008). OII Working Paper* Nº. 16. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1326476. Acesso em12/12/2019.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, v. 30, n. 1, p. 75-89, 2015.