Examinando a Guerra em Wi-Fi: Da Ciberguerra à Wikiguerra — Batalhas pelo Ciberespaço

Paul Rexton Kan

Esta resenha foi originalmente publicada na revista *Parameters* (*Autumn 2013*).

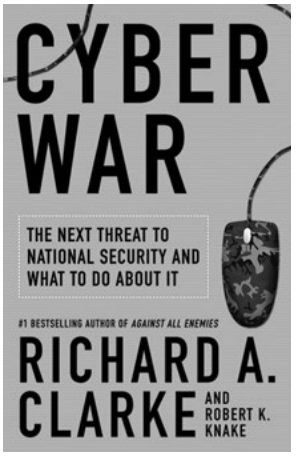
ALGUNS DIAS APÓS as explosões na Maratona de Boston, em abril de 2013, a agência de notícias Associated Press (AP) divulgou, pelo *site Twitter*: "Últimas Notícias: Duas explosões na Casa Branca e Barack Obama ficou ferido". O índice Dow Jones Industrial caiu quase 150 pontos, com uma perda súbita de US$ 136 bilhões em valor de mercado. A conta da AP no *site Twitter*, cujo *feed* havia sido incluído nos algoritmos de relatórios da Bolsa de Valores de Nova York alguns dias antes, foi atacada por *hackers* de um grupo autointitulado Exército Eletrônico da Síria, o que lhe possibilitou tuitar a mensagem falsa. Felizmente, a perda em riqueza nacional foi passageira, já que as ações recuperaram seu valor em três minutos.

Como estabelecer um contexto para o que aconteceu naqueles poucos minutos? Foi um ataque súbito em uma guerra cibernética iniciada pelo regime sírio ou uma brincadeira de algum grupo independente, por diversão? Não houve nenhuma perda permanente de capital e, fora os responsáveis pelo ocorrido, poucos teriam tido motivos para rir da situação. Contudo, ainda existe um sentido de seriedade com respeito ao incidente, o que revela os verdadeiros limites de nosso entendimento sobre o domínio cibernético na área de segurança nacional. Considerando o fato de o domínio digital ser algo novo, artificial e em constante mudança devido à ação das pessoas, não surpreende que os profissionais de segurança nacional busquem abordagens conhecidas e cômodas. Os ataques cibernéticos são um acontecimento diário — ou, mais precisamente, que ocorre a cada nanossegundo) —, que requer "segurança cibernética" (ou "cibersegurança"). A liderança nacional alerta sobre uma possível "guerra cibernética" (ou "ciberguerra") e "terrorismo cibernético", que podem levar a um "Pearl Harbor cibernético". A prevenção de um incidente desses requer uma "defesa cibernética" ou até mesmo algum tipo de "dissuasão cibernética". Alguns formuladores de políticas desejam que se estabeleça um "controle de armas cibernéticas" para limitar quais ataques dessa natureza podem ser conduzidos contra um outro país. Esses conceitos são uma adaptação dos que são utilizados no domínio físico para descrever atos violentos e reações a eles. Esses conceitos ajudam formuladores de políticas, profissionais de segurança nacional e acadêmicos a entender as ações de agressão conduzidas no ciberespaço?

Em seu livro *Cyber War: The Next Threat to National Security and What to Do About It* ("Guerra Cibernética: A Próxima Ameaça à Segurança Nacional e o que Fazer quanto a Isso",

Paul Rexton Kan é Professor Adjunto de Estudos de Segurança Nacional e Catedrático "Henry L. Stimson" de Estudos Militares no US Army War College. É o autor de Drugs and Contemporary Warfare *e de* Cartels at War: Understanding Mexico's Drug Fueled Violence and the Threat to US National Security. *Seu recente artigo, "Cyberwar in the Underworld", foi publicado no* Yale Journal of International Affairs.

em tradução livre), Richard Clarke afirma que esses conceitos são relevantes, mas frequentemente ignorados pelos formuladores de políticas. Para Clarke, a guerra cibernética se refere a "ações por um Estado-nação destinadas a penetrar nos computadores ou redes de outro país com o intuito de causar danos ou interrupções" (p. 6). No primeiro capítulo, o autor detalha "experiências" que constituem incidentes de guerra cibernética, executados, em particular, pelos russos, norte-coreanos e israelenses. Esses casos são bem conhecidos hoje em dia: o "controle" israelense sobre o sistema de defesa antiaérea da Síria em 2007; os ataques distribuídos de negação de serviço (*distributed denial of service — DDOS*) pela Rússia contra a Estônia em 2007 e seus ataques cibernéticos mais sofisticados contra a Geórgia em 2008; e o ataque de *botnet* da Coreia do Norte contra *sites* norte-americanos em 2009. Clarke extrai quatro máximas desses incidentes: a guerra cibernética é real; ocorre à velocidade da luz; é global; e já começou. Essas máximas constituem o cerne do livro, no qual ele apresenta mais relatos sobre "guerreiros cibernéticos" no "espaço de combate" e descreve como os Estados Unidos da América (EUA) devem preparar-se, defender-se e retaliar.



Clarke dedica a maior parte do livro a reiterar essas máximas, ilustrando-as com breves exemplos. Demonstra grande preocupação com a China, a qual, argumenta ele, vem "fazendo, sistematicamente, tudo o que um país faria, caso contemplasse obter uma capacidade ofensiva cibernética e considerasse poder ser, ele próprio, um alvo para ataques desse tipo" (p. 54). A principal preocupação de Clarke é que os EUA estejam ficando para trás em relação a países como a China. "De fato, devido à sua maior dependência de sistemas controlados ciberneticamente e à sua incapacidade, até o momento, para criar defesas cibernéticas nacionais, os EUA estão, atualmente, mais vulneráveis à guerra cibernética que a Rússia ou a China. Os EUA correm maior risco que Estados menores, como a Coreia do Norte" (p. 155).

Considerando a gravidade do parecer de Clarke e dos exemplos de terríveis consequências de ataques cibernéticos anteriores, seu livro merece especial atenção. A definição restrita de Clarke sobre o que constitui uma guerra cibernética é problemática. A infinidade de eventos que ele descreve realmente constituem uma "guerra"? Causar danos ou interrupções engloba uma gama bastante ampla de consequências: desde a desfiguração de um *site* até a incapacitação de uma rede elétrica. No mundo físico, uma ação pode ser interpretada como vandalismo, enquanto outra pode ser considerada uma destruição intencional de propriedade. Caso não haja uma intenção coercitiva de alcançar um objetivo político, os diversos ataques (cibernéticos ou não) seriam considerados um ato de guerra?

Nesse sentido, o livro *Cyber War Will Not Take Place* ("A Guerra Cibernética não Acontecerá", em tradução livre), de Thomas Rid, é especialmente útil para esclarecer boa parte da confusão conceitual em torno do tema. Ao contrário do livro de Clarke, o de Rid é uma obra mais acadêmica. Rid, palestrante do King's College, em Londres, defende que as ações nocivas cometidas pelo ciberespaço não constituem guerra ou combate nem são especialmente violentas. "Nenhuma ofensiva cibernética causou a perda de vidas humanas. Nenhuma ofensiva cibernética chegou a ferir pessoa alguma. Nenhuma ofensiva cibernética danificou, seriamente, prédio algum" (p. 166). Tomando como base a teoria da guerra de Clausewitz, Rid afirma que "se o emprego da força na guerra é violento, instrumental e político, então não há nenhuma ofensiva cibernética que satisfaça a todos os três critérios. Mais que isso, porém, há poucos ataques cibernéticos na história que cheguem a atender a apenas *um* desses critérios" (p. 4, ênfase no original). Para Rid, os eventos conduzidos pelo ciberespaço, relatados por inúmeros profissionais de segurança

nacional, como Clarke, enquadram-se em uma ou mais categorias de espionagem, sabotagem ou subversão. "Apesar das tendências, a 'guerra' em 'guerra cibernética' tem, em última análise, mais em comum com a guerra contra a obesidade do que com a Segunda Guerra Mundial — tem um valor mais metafórico que descritivo" (p. 9).

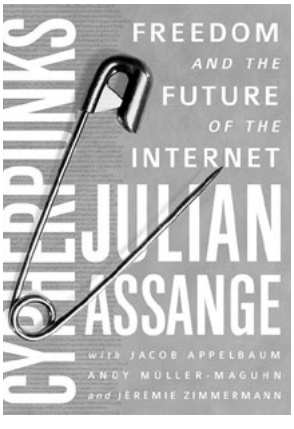
A observação de Rid sobre ter cuidado com metáforas e conceitos em um novo domínio é válida. O objetivo de seu livro é "tentar ajudar a consolidar a discussão, atenuar parte dos exageros e enfrentar, adequadamente, alguns dos desafios de segurança mais urgentes" (p. ix).

Muito já se ponderou sobre a mecânica de atos nocivos no ciberespaço, mas se dedicou relativamente pouco tempo a colocá-los em contexto. É essencial entender as motivações de grupos e indivíduos que agem no ciberespaço. O principal argumento de Rid e seus capítulos subsequentes sobre "Violência", "Sabotagem", "Espionagem" e "Subversão" são tônicos poderosos para algumas das obras mais alarmistas sobre a guerra cibernética. Sua conclusão é tão interessante quanto polêmica: os ataques cibernéticos são um ataque contra a própria violência. Já que atividades como a sabotagem, a espionagem e a subversão hoje podem ser realizadas no ciberespaço, são necessários menos efetivos para conduzi-las no mundo físico. Se, no passado, forças especiais teriam sido enviadas para destruir uma instalação, espiões teriam sido despachados para roubar segredos e multidões teriam sido organizadas para protestar contra as políticas do governo, hoje os ataques cibernéticos podem cumprir esses objetivos de maneira simples e secreta. Entretanto, essa conclusão precisa ser tratada com grande cautela. Evoca, vagamente, os primeiros teóricos sobre o poder aéreo, que previram que o avião tornaria as guerras menos violentas ao reduzir sua duração. Segundo, embora só possam causar destruição ou interrupções indiretamente no país visado, os ataques cibernéticos podem acarretar custos diretos no mundo físico. Ações digitais podem gerar represálias cinéticas. A sabotagem, a espionagem e a subversão podem não se encaixar na definição de guerra, mas serviram como justificativa para seu início no passado.

Embora ajude a esclarecer os parâmetros da discussão sobre a guerra cibernética ao concentrar-se em definições mais restritas, conceitos mais claros e metáforas mais adequadas, Rid não se aprofunda suficientemente nos ataques cibernéticos conduzidos por grupos não estatais. O capítulo sobre "Subversão" aborda apenas ligeiramente o tema de grupos não estatais, que utilizam o domínio digital para modificar o comportamento de Estados. Esses grupos não devem ser desconsiderados, porque uma outra questão em torno do tuíte falso da AP que levou à queda na bolsa de valores é quem, exatamente, é o Exército Eletrônico da Síria? É um grupo de *"hackers* patrióticos" apoiados pelo Estado, uma associação independente, um grupo flexível de simpatizantes do regime de Bashar al-Assad ou alguma combinação dessas opções? Com o anonimato proporcionado pelo ciberespaço, tanto Clarke quanto Rid concordam que o problema de atribuir responsabilidade é complicado. Se o Exército Eletrônico da Síria é um grupo independente de algum tipo, o debate sobre a guerra cibernética não capta a importância de suas atividades. A guerra cibernética entre países não ocupa todo o espaço do debate, da mesma forma que a guerra entre Estados não engloba todos os aspectos da guerra. Grupos dispersos de "hacktivistas" executam muitas das mesmas atividades cibernéticas danosas que os Estados-nação. Isso demonstra o caráter singular do domínio cibernético. Devido à facilidade de acesso ao ciberespaço, os hacktivistas cometem os mesmos tipos de ação *on-line* (como a desfiguração de *sites*, roubo de informações sigilosas, ataques distribuídos de negação de serviço e lançamento

de *botnets*) que integram o repertório de ataques cibernéticos conduzidos por países. Em consequência, os hacktivistas têm quase o mesmo poder no ciberespaço que os infames *hackers* chineses do Exército de Libertação Popular. Entretanto, ao contrário de países, que executam ataques cibernéticos por motivos políticos relacionados à política externa, os hacktivistas usam a internet para buscar objetivos políticos e sociais centrados na própria internet.

Grupos como Anonymous e WikiLeaks se consideram combatentes em uma guerra para alcançar o objetivo de liberdade na internet. Para eles, a libertação humana começa com a liberação das informações. No livro de Julian Assange, *Cypherpunks: Freedom and the Future of Internet* (publicado no Brasil com o título *Cypherpunks – Liberdade e o Futuro da Internet*), essa perspectiva é elucidada. O título do livro é uma referência ao movimento *cypherpunk* que surgiu no final dos anos 80, o qual defendia o uso disseminado e a disponibilidade da criptografia para proteger e promover a liberdade humana contra a invasiva vigilância estatal. O livro é uma coletânea de discussões de partidários do *slogan* dos *cypherpunks*: "privacidade para os fracos, transparência para os poderosos". Os debates foram realizados quando Assange, o criador do *WikiLeaks*, estava sob prisão domiciliar no Reino Unido, aguardando sua extradição para a Suécia, mas antes de seu pedido de asilo à Embaixada equatoriana em Londres, onde ainda reside. Os diálogos revelam como o grupo se considera envolvido em uma luta violenta contra o que ele enxerga como a "futura distopia da vigilância", organizada por países e poderosas empresas. Afirmam que eles e seus simpatizantes tiveram conflitos com quase todos os Estados poderosos [...] Sabemos disso a partir de uma perspectiva de combatente, porque tivemos de proteger nossos integrantes, nossas finanças e nossas fontes [contra eles]".



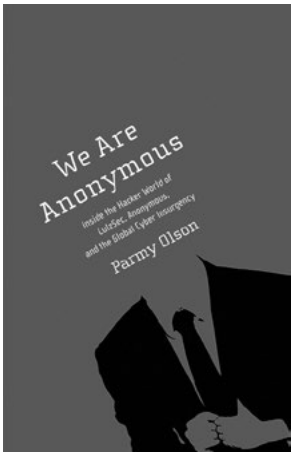
Grupos como Anonymous e WikiLeaks se consideram combatentes em uma guerra para alcançar o objetivo de liberdade na internet. Para eles, a libertação humana começa com a liberação das informações.

Entretanto, as discussões não se restringem a países apenas. O site *Google* é o tema do capítulo "Espionagem do Setor Privado". O diálogo apresentado a seguir é um exemplo típico e instigante:

> Jeremie: A vigilância apoiada pelo Estado é, de fato, uma importante questão, que desafia a própria estrutura de todas as democracias e a forma como elas funcionam, mas também existe a vigilância da indústria privada e, potencialmente, a coleta em massa de dados privados. Basta considerar o *Google*. Se você for um usuário típico, o *Google* sabe com quem tem se comunicado, quem conhece, o que tem pesquisado e, possivelmente, sua orientação sexual e crenças religiosas e filosóficas.
>
> Andy: Sabe mais sobre você do que você mesmo.
>
> Jeremie: Mais do que sua mãe sabe e talvez mais do que você mesmo. O *Google* sabe quando você está *on-line* ou não.
>
> Andy: Você se lembra do que pesquisou dois anos, três dias e quatro horas atrás? Não sabe; o *Google* sabe.

A retórica das conversas pode ser excessivamente dramática; rótulos como "juventude nazista" e "atos da Stasi" são utilizados sem cuidado. O capítulo sobre "A Militarização do Ciberespaço" começa com Assange defendendo que todas as comunicações ligadas à internet são monitoradas por organizações de inteligência militar. "É como ter um carro de combate no seu quarto. É um soldado entre você e sua esposa quando envia

uma mensagem de texto. Estamos todos vivendo sob a lei marcial no que diz respeito às nossas comunicações. Só não podemos ver os carros de combate" (p. 33). Muitos se irritarão com o uso constante de metáforas, analogias e retórica de guerra pelo grupo. Contudo, é importante ir em frente e lidar com as implicações de seus argumentos, em vez de se deixar paralisar pelo seu uso (ou abuso) linguístico. Sua ideologia sobre a liberdade da internet é mais problemática. Uma ideologia centrada no livre uso da tecnologia se torna irônica, especialmente no caso do Exército Eletrônico da Síria. Não está claro se o grupo de *cypherpunks* aprovaria as atividades virtuais de um outro grupo de hacktivistas, conduzidas em nome de um regime tirânico em Damasco, que usou um programa "*kill switch*" para interromper o tráfego de internet fora de suas fronteiras. Contudo, se a internet fosse completamente "liberada", as atividades do Exército Eletrônico da Síria seriam admitidas, se cometidas contra um Estado de vigilância como os EUA. Em suma, nem todo hacktivismo serve à causa da libertação humana: é uma faca de dois gumes. Parafraseando um observador da tecnologia, Farhad Manjoo, a internet é apenas uma série de tubos sem ideologia.

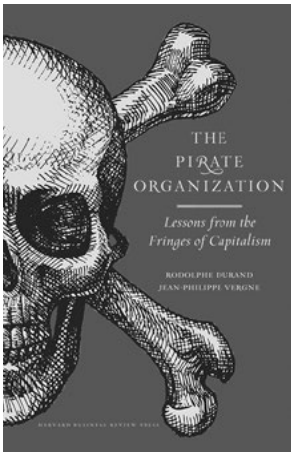


Enquanto o livro *Cypherpunks* descreve a ideologia defendida por um grupo central de hacktivistas, a obra de Parmy Olson, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency* (publicado no Brasil com o título *Nós Somos Anonymous — Por Dentro do Mundo dos Hackers*), é um relato jornalístico rico em detalhes sobre a história e os atos de um grupo cibernético, que promove sua ideologia com ataques cibernéticos. Em vez de se concentrar no círculo interno de envolvidos com o *WikiLeaks*, o livro de Olson narra a ascensão de um grupo hacktivista, que é, hoje, mais como um movimento social cibernético. Uma das observações mais importantes de Olson diz respeito à noção equivocada de que o *Anonymous* é uma "panelinha de *superhackers*". Com efeito, apenas alguns integrantes eram *hackers*; o restante consistia "simplesmente em jovens usuários da internet, que queriam fazer algo, em vez de desperdiçar seu tempo em [salas de bate-papo anônimas]" (p. 81). O lema dos *Anonymous* assemelha-se ao dos *cypherpunks*: "a informação quer ser livre".

Se os ataques russos contra a Estônia e a Geórgia são a condição *sine qua non* de uma guerra cibernética na esfera interestatal, os ataques pelo grupo *Anonymous* contra a Igreja da Cientologia, o *site PayPal* e a empresa Sony são a condição *sine qua non* do hacktivismo no mundo dos *hackers*. Olson detalha como o grupo ganhou projeção por suas operações contra a Igreja da Cientologia em 2008. Naquele ano, a Igreja pressionou o site *YouTube*, exigindo que retirasse um vídeo protagonizado pelo famoso ator Tom Cruise, um de seus seguidores, e que havia sido "vazado". A pressão exercida pela Igreja da Cientologia ia de encontro ao etos de transparência do grupo *Anonymous*. Em resposta, o *Anonymous* deu início a uma operação para derrubar o *site* da Igreja, conjugando ataques distribuídos de negação de serviço com trotes como ligações com música repetitiva, envio constante de faxes de papel preto para esgotar os cartuchos de tinta e pedidos falsos de pizza e serviço de táxi. O grupo tem uma causa em comum não apenas com o fundador do *WikiLeaks*, Julian Assange, mas também com os movimentos *Occupy* e o acusado de vazamento de informações, Bradley Manning. Olson também cobre as diversas operações do grupo *Anonymous* voltadas a agências e instituições como *PayPal*, Mastercard e Visa, que se recusaram a processar pagamentos para sites que estavam arrecadando verbas para a defesa jurídica de Assange, Manning e indivíduos ligados aos movimentos *Occupy*.

Especialmente reveladora no livro de Olson é a noção de que o etos do grupo corresponde à forma como é estruturado. As informações na internet

são dispersas e descentralizadas, como é o caso do grupo *Anonymous*. Marshall McLuhan proclamou que o "meio é a mensagem". Para os hacktivistas, o meio é o etos. A estrutura do grupo também é um reflexo de seu etos. Como um grupo fracamente ligado de ativistas sociais virtuais, o *Anonymous* se orgulha de ser desestruturado, sem uma hierarquia ou autoridade central. Essa estrutura nebulosa tem vantagens estratégicas, mas, como Olson aponta no capítulo "Guerra Civil", essas características têm se mostrado problemáticas operacionalmente. Devido à estrutura flexível do *Anonymous*, qualquer operação pode seguir adiante ou ser cancelada de forma imprevisível. Além disso, seus integrantes podem ir além de apenas discordar de uma operação planejada e decidir não participar: podem opor-se ativamente contra a operação, executando contra-ataques a facções com as quais discordem. Podem também impedir outros integrantes de acessar fóruns virtuais, onde muitos deles se encontram. Houve divisões internas entre membros do *Anonymous* que queriam conduzir operações em conformidade com o etos dos *hackers*; outros que queriam iniciar ataques motivados por questões morais contra organizações que coíbem a liberdade humana no mundo físico; e outros, ainda, que estavam exclusivamente interessados em atuar por "despeito e diversão".



Por fim, em vez de um livro voltado ao público em geral, um trabalho acadêmico, uma compilação de discussões ou uma investigação jornalística, *The Pirate Organization: Lessons from the Fringes of Capitalism* ("A Organização Pirata: Lições das Margens do Capitalismo", em tradução livre) é um ensaio, escrito por Rodolphe Durand e Jean-Philippe Verne. Embora não se concentrem exclusivamente no domínio cibernético, os autores discutem a luta histórica entre atores soberanos e aqueles que buscam e exploram áreas fora do controle de um governo. Para eles, organizações piratas:

> [I]ndependentemente da época, apresentam as seguintes características: têm um "relacionamento" antagônico com o Estado, especialmente quando este alega ser a única fonte de soberania; atuam de maneira organizada, a partir de um conjunto de bases de apoio localizadas fora desse território, sobre o qual o Estado normalmente declara controle soberano; desenvolvem, como comunidades alternativas, uma série de normas diferentes que, segundo eles, deveriam ser usadas para regulamentar áreas inexploradas; e, por fim, representam uma ameaça ao Estado, por abalarem as próprias ideias de soberania e território ao contestarem o controle estatal e as atividades das entidades legais que atuam sob sua jurisdição, como empresas com fins lucrativos e monopólios. (p. 15).

Com base nessa definição, o *WikiLeaks* e o *Anonymous* se enquadram facilmente dentro dos parâmetros de uma organização pirata. Com efeito, os autores deixam claro que é um erro concentrar-se exclusivamente na pirataria marítima contemporânea. "O Barba Negra, por exemplo, tem bem mais em comum com um pirata cibernético do que com um camponês somali que usa um fuzil *Kalashnikov* para atacar um barco pesqueiro a partir de uma embarcação improvisada" (p. 15). Os autores examinam, de forma sucinta e penetrante, a história das organizações piratas: os bucaneiros dos séculos XVII e XVIII, os DJ de rádio em alto-mar, os piratas cibernéticos na *web* e os biopiratas nos laboratórios. Segundo os autores, as organizações piratas surgem porque um novo território sem governo está pronto para ser explorado. Como visto nos quatro livros avaliados, o ciberespaço é o território sem governo por excelência. Com base na definição de uma organização pirata, os hacktivistas são, em alguns aspectos, atores mais importantes no domínio cibernético que os Estados-nação.

Grupos como *Anonymous* e *WikiLeaks* representam, claramente, um lado da tensão entre a

soberania e os atores não estatais. Além disso, a forma pela qual os autores configuram a tensão entre uma organização dessas e o Estado apoia aqueles que, como Clarke, veem o hacktivismo como uma "forma relativamente branda de protesto virtual" (p. 55). Aos que creem que haverá uma guerra cibernética entre Estados-nação, esse livro proporcionará uma perspectiva mais ampla sobre aspectos que desconhecem na discussão geral sobre o tema.

Há muito a criticar quando se trata de sua definição de organizações piratas, e a forma irrefletida pela qual descartam a pirataria marítima ao longo do Chifre da África é lamentável. Uma compreensão mais profunda mostraria que a atividade é bem mais complexa, o que, na verdade, apoiaria sua tese. A pirataria marítima contemporânea tira proveito de redes regionais e mundiais de finanças, seguro e transporte, que ocorrem bem longe dos ataques a embarcações em alto-mar. A rede é dispersa, relativamente duradoura e resistente à detecção e à eliminação.

Os cinco livros ilustram a crescente complexidade de conceituar ações virtuais nocivas. Os formuladores de políticas, profissionais de segurança nacional e acadêmicos muitas vezes descartam os hacktivistas ou piratas cibernéticos como sendo grupos de indivíduos desajeitados e insatisfeitos, que geram tumulto *on-line* para atender a um anseio de pertencer a uma comunidade. Concentram-se, em vez disso, na guerra cibernética conduzida ou apoiada por Estados-nação. É fácil recolocar mudanças complicadas no ambiente de segurança na "caixa" de Estado-nação, mas essa seria uma medida imediatista. É justamente o que fizemos não faz muito tempo, com resultados desastrosos. Entre a queda do Muro de Berlim e a destruição do World Trade Center, atores não estatais foram ignorados em prol de desafios relacionados a Estados. Mesmo hoje, após mais de uma década da Guerra contra o Terrorismo e das guerras no Iraque e no Afeganistão, nosso entendimento de assuntos como terrorismo, insurgência e guerra assimétrica não é totalmente sólido.

Além disso, considerando o caráter recente e extremamente mutável do domínio cibernético, seria um equívoco desconsiderar qualquer grupo que tenha, como etos, o desejo de definir o ciberespaço por meio de ações virtuais que desafiam os elementos básicos da segurança nacional. Esse é, em especial, o caso quando alguns desses grupos se sentem sitiados por governos e empregam, rotineiramente, a retórica da guerra: "[n]esse campo aparentemente platônico de ideias e fluxo de informações, pode haver uma noção de força coercitiva? Uma força que possa alterar fontes históricas, grampear telefones, separar pessoas, transformar a complexidade em escombros e erigir muros, como um exército de ocupação?" (p. 3) Os formuladores de políticas, profissionais de segurança nacional e acadêmicos descartaram, anteriormente, grupos que acreditam agir em defesa própria e, então, atacam de modo súbito e imprevisto, para nossa surpresa e prejuízo.

O que consta, em diversos graus, da literatura sobre o ciberespaço e a guerra cibernética são os cinco diferentes debates em curso sobre esse novo domínio e sobre como atuar nele. Os debates incluem: quem estabelece os limites do ciberespaço; como as informações virtuais devem ser controladas; para quem devem ser disponibilizadas; se hierarquias e redes de indivíduos podem coexistir no ciberespaço; e qual é a diferença entre "guerra" e "crime" nesse ambiente[1]. Nos livros analisados, fica evidente que cada ataque ou assalto cibernético não apenas agrega elementos a esses debates, como também contribui para a definição desse domínio. Paradoxalmente, os debates para definir o ciberespaço estão ocorrendo por meio dele.

Esse paradoxo provavelmente será reforçado com o avanço da tecnologia cibernética e caráter cada vez interligado da internet com a nossa vida diária. Com o surgimento de peças como os óculos inteligentes *Google Glass*, o relógio Apple Iwatch e até a possibilidade de um spray de *wi-fi*, esse caráter interligado se materializará. Não estaremos no ciberespaço: seremos o ciberespaço. Esses cinco livros são leitura essencial para nos prepararmos para esse futuro.***MR***

REFERÊNCIAS

1. Para uma análise aprofundada do debate sobre o que é "guerra", "crime" e "violência" no campo cibernético, veja a série de artigos de John Stone, Gary McGraw, Dale Peterson, Timothy Junio, Adam Liff e Thomas Rid na "Mesa Redonda sobre Guerra Cibernética" em *Journal of Strategic Studies* 36, no. 1 (Feb. 2013).