

RESENHA

Book Review

CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT¹

Diego Rafael Canabarro*

A revista *The Economist* publicou, na edição de julho de 2010, duas reportagens intituladas, respectivamente, “*Cyberwar – it is time for countries to start talking about arms control on the Internet*”² e “*War in the fifth domain – are the mouse and the keyboard the new weapons of conflict?*”³. Nelas, a tônica da discussão gira em torno do uso do ciberespaço (e mais precisamente da Internet) tanto como uma arma de guerra a serviço de atores estatais e não estatais quanto um cenário próprio em que batalhas das mais variadas ordens podem ser travadas. Duas visões distintas a respeito dessas questões são apresentadas: a cética (por exemplo, do atual “czar” da cibersegurança do governo Obama, Howard Schmidt, bem como de outros especialistas das gigantes da TI mundial), segundo a qual a percepção apocalíptica a respeito do espalhamento das tecnologias da informação e da comunicação (TIC) pelo mundo está longe de se concretizar; e uma visão mais alarmada de pessoas como Richard Clarke que, por anos,

¹ CLARKE, Richard A; KNAKE, Robert K. (2010). *Cyber War: The Next Threat to National Security and What To Do About It*. Nova Iorque: HarperCollins, 290 p. [ISBN: 978-0-06-196223-3]

* Diego Rafael Canabarro é Mestre em Relações Internacionais e Doutorando em Ciência Política pela UFRGS.

² THE ECONOMIST (2010). *Cyberwar – it is time for countries to start talking about arms control on the Internet*. Publicado em Economist.com [http://www.economist.com/node/16481504?story_id=16481504]. Disponibilidade: 01/07/2010.

³ THE ECONOMIST (2010). *War in the fifth domain – are the mouse and the keyboard the new weapons of conflict?*, Publicado em Economist.com [http://www.economist.com/node/16478792]. Disponibilidade: 01/07/2010.

fora responsável por articular cibersegurança e contraterrorismo no governo dos Estados Unidos.

O debate inserido nas reportagens em questão decorre diretamente do ensaio publicado um pouco antes de julho de 2010 por Richard Clarke, em conjunto com Robert Knake, a respeito do tema. Clarke é professor da *Kennedy School of Government* da Universidade de Harvard. No governo americano, trabalhou para as administrações de Ronald Reagan, George Bush (pai), Bill Clinton e George Bush (filho) até pouco antes do início da guerra do Iraque. Na administração Clinton, ganhou o cargo de Coordenador Nacional de Segurança, Proteção de Infraestrutura e Contraterrorismo (criado pela Diretiva Presidencial No. 62/1998). Na administração Bush, Clarke foi alçado ao posto de Conselheiro Especial para a Segurança no Ciberespaço.⁴ O autor foi assessorado por Knake, para quem “*a Internet e o ciberespaço são naturais como o ar e a água*” (p. xii) segundo as palavras de Richard Clarke, que escreve toda a obra em primeira pessoa.

Desde a década de 1990, Clarke é conhecido por alertar o governo norte-americano a respeito das possibilidades de o país enfrentar um “*Pearl Harbor Eletrônico*”. No ensaio livre a respeito do tema – baseado muito mais na experiência do que na realização de uma pesquisa abrangente e metodologicamente estruturada a respeito do assunto – os autores procuram esclarecer as possibilidades e os limites da “nova arma” (e da “nova guerra tecnológica”, portanto) criada pelos Estados Unidos.

O livro tem alguns pontos de partida que merecem destaque. Em primeiro lugar, segundo os autores, “*o fenômeno da ciberguerra é tratado com tanto sigilo pelo governo que isso faz com que a guerra fria pareça um tempo de abertura e transparência.*” (p. xi). Além disso, “*antes de representar uma alternativa à guerra convencional, a ciberguerra pode, realmente, aumentar a chance de ocorrência de combates tradicionais com explosivos, mísseis e projéteis.*” (p. xiii). E, por conta disso, “*uma série de tarefas precisam ser desempenhadas: entender o que é a ciberguerra,*

⁴ As duas funções (de Coordenador e de Conselheiro) encontram-se inseridas no organograma do *Department of Homeland Security*.

aprender como e porque ela funciona, analisar seus riscos, preparar-se para ela e pensar a respeito de formas de controla-la.” (p. xiii).⁵

Em uma clara tentativa de dar conta dessas tarefas, o livro divide-se em oito capítulos.

O primeiro capítulo, intitulado “*Trial Runs*” dedica-se a recontar casos que receberam, nos últimos anos, ampla cobertura da mídia como sendo os primeiros grandes episódios de guerra cibernética, mas cada uma das histórias em questão é apresentada com detalhes que não vieram a público. Além disso, o autor dá detalhes das estratégias e práticas empregadas, tanto ofensiva quanto defensivamente, há mais de vinte anos pelos diversos órgãos envolvidos nas atividades de segurança e defesa dos Estados Unidos. Assim, no primeiro caso, são descritas as práticas usadas para os ataques virtuais que ocorreram contra a Estônia (2007) e contra a Geórgia (2008). Alguns episódios em que os Estados Unidos foram atacados são também descritos para se apresentar as diferentes vulnerabilidades e as alternativas encontradas para a defesa dos principais alvos atacados (os servidores que sustentam o Departamento de Estado e o Departamento de Segurança Doméstica e seus respectivos sítios virtuais). No segundo caso, o texto apresenta as diferentes estratégias norte-americanas desde a década de 1990 para empregar redes de telecomunicação distintas e a própria Internet tanto como uma arma de guerra quanto como cenário de operações propriamente dito. Tudo isso é feito para introduzir a ideia de que situações como as descritas tendem, com o tempo, a alterar o equilíbrio militar mundial e alterar de forma notória as relações políticas e econômicas no sistema internacional.

A partir desse ponto, as seções seguintes são direcionadas a esclarecer os conceitos articulados, organizando-os em capítulos especificamente dedicados a apresentar as diferentes categorias de “ciberguerreiros” (tanto agentes estatais quanto não estatais) [Capítulo 2]; a delimitar o ciberespaço enquanto campo de batalha e a explicar o tratamento de “nova arma” dispensado à Internet [Capítulo 3]; e a demonstrar

⁵ Ao empregar o termo *ciberguerra*, Clarke e Knake esclarecem que “quando o termo *ciberguerra* é usado no livro, ele refere-se apenas a ações que um país empreende para penetrar nos computadores e redes de outro país com a finalidade de causar danos e mau funcionamento.” (p. 6)

por que as vulnerabilidades identificadas nas seções precedentes para o caso dos Estados Unidos não foram contornadas [Capítulo 4]. Enquanto o segundo capítulo apresenta o despertar de diferentes países para a necessidade de se desenvolverem capacidades técnicas e tecnológicas relacionadas à Internet e ao ciberespaço como um todo, o terceiro capítulo é dedicado a conscientizar o leitor a respeito da dependência em relação a sistemas informatizados, a redes de computadores e à Internet que grande parte do planeta hoje tem. E, feito isso, exploram-se as *“três coisas envolvidas no ciberespaço que fazem a ciberguerra uma possibilidade real”* (p. 73 e ss.): as falhas na estruturação da Internet; as possíveis falhas (intencionais e não intencionais) em aparelhos eletrônicos e nos *softwares* por detrás de cada um; e a crescente tendência de se por *online* mais e mais sistemas informatizados críticos (como, por exemplo, os relativos às redes de transmissão de energia elétrica, aos controles de tráfego aéreo, às transações comerciais públicas e privadas, etc.). Esse conjunto de capítulos termina (Capítulo 4) com uma verdadeira crítica às estratégias de menosprezo à importância da cibersegurança na era Bush (filho) e com uma descrição das ações adotadas nos dois primeiros anos do governo Obama para incrementar a segurança no país no que se relaciona à Internet e ao ciberespaço como um todo. O capítulo quarto termina, além disso, com uma tentativa de se mensurar a “força para a ciberguerra” de EUA, Rússia, China, Irã e Coreia do Norte, apontados pelos autores como sendo os principais protagonistas dos eventos apresentados no capítulo inicial.

Sem qualquer aprofundamento metodológico para a avaliação da capacidade geral de cada país, Clarke e Knake estabelecem três critérios de comparação: (1) poder ofensivo [capacidade de atacar outros países]; (2) poder defensivo [capacidade de adotar medidas enquanto um ataque ocorre]; e (3) ciberdependência [medida do quanto uma nação depende de redes e sistemas informáticos que podem ser vulneráveis pelos critérios lançados no terceiro capítulo]. Uma nota de zero (0) a dez (10) é atribuída a cada critério para cada país. Ao fim, os resultados em cada critério são somados, indicando o que os autores chamam de “força global relativa à ciberguerra”. Os resultados alcançados são os seguintes: EUA = 11 pontos; Rússia = 16 pontos; China = 15 pontos; Irã = 12 pontos; e Coreia do Norte = 18 pontos. Ou seja, segundo a lógica

apresentada na obra, a Coreia do Norte teria uma maior capacidade de enfrentar se engajar em ciberguerra por dois motivos principais: a baixa dependência do país a sistemas informatizados e a capacidade de ‘desconectar’ as poucas conexões existentes entre o plano real e o plano virtual no país. De todos eles, o país mais vulnerável seriam os EUA, em virtude de grande parte de seus recursos críticos estarem fora do controle direto do governo, o que implicaria a maior dificuldade de defesa em relação a todos os outros países avaliados.

Por óbvio, a avaliação feita é de pouca valia para se conhecer, de fato, a realidade de cada um dos casos estudados, uma vez que não há a possibilidade de se controlar a pontuação atribuída a cada país a partir do referencial empírico empregado para se fazer a comparação. Além disso, por uma inversão lógica, a avaliação pode fazer o leitor incorrer em erro ao dar margem para que se interprete que quanto maior for a aplicação de TIC pelos Estados, automaticamente maiores serão as vulnerabilidades existentes e maior será, então, a insegurança decorrente, o que não é uma consequência necessária do incremento tecnológico, e, sim, apenas uma das possibilidades observáveis ao longo da história⁶.

A partir de então, a obra ganha contornos normativos e passa a esboçar uma estratégia mais apropriada para a “ciberdefesa” dos Estados Unidos, levando-se em consideração os pontos positivos e negativos indicados a partir da avaliação das políticas e iniciativas adotadas por Clinton, Bush e Obama (Capítulo 5). A principal “ferramenta” empregada pela política de sinergia entre o setor público e o setor privado do país deveria ser a regulamentação no nível federal em torno de três questões principais: a proteção da infraestrutura mais fundamental de cabos de fibra óptica que dão sustentação às telecomunicações via Internet no país (*backbone*); a proteção da rede de transmissão de energia elétrica; e a proteção das redes do Departamento de Defesa. Há uma série de questões controversas em relação a cada um desses itens como, por exemplo, o nível de controle do Estado sobre as atividades dos provedores de acesso à

⁶ Nesse sentido, ver HEADRICK, Daniel R (2009). *Technology: A World History*. Oxford-UK: Oxford University Press; e RENNSTICH, Joachim K (2008). *The Making of a Digital World: The Evolution of Technological Change and How it Shaped Our World*. Nova Iorque: Palgrave Macmillan.

Internet e sobre os dados privados que trafegam pela rede, a exigência de gastos adicionais em segurança das empresas prestadoras de serviços de telecomunicação e de fornecimento de energia elétrica tanto, para o governo quanto para os cidadãos dos Estados Unidos, o que demandaria participação popular, transparência e escolhas políticas a respeito da ciberdefesa no país. Ao mesmo tempo em que busca para contribuir com tais debates, esse capítulo é uma resposta à percepção inicial dos autores, de que o nível de sigilo com que isso vem sendo tratado pelas sucessivas administrações do país pode ser um indicativo de ausência de uma verdadeira estratégia concatenada para assegurar a segurança do país em mais essa frente.

Feito isso, os autores colocam-se a formular cenários imaginários que poderiam ser enfrentados daqui pra frente como forma de preparar uma estratégia ofensiva para o domínio militar dos Estados Unidos no ciberespaço (Capítulo 6). Tal estratégia engloba questões relativas à dissuasão; às hipóteses de primeiro ataque; às preparações necessárias para qualquer batalha no ciberespaço; ao espalhamento das hostilidades por todo o planeta; os efeitos reais, virtuais e colaterais da ciberguerra; à escalada da intensidade dos conflitos; às questões relativas à atribuição da responsabilidade por ataques; à dificuldade de se prever e de se perceber os diferentes tipos de ataque; e ao significado das assimetrias decorrentes dos distintos atores que atuam no ciberespaço.

Os dois capítulos finais (Capítulos 7 e 8) indicam a percepção dos atores de que chegou o momento de se romper com o isolacionismo dos Estados Unidos em relação ao tema do livro (motivado por desconfiança e por desconhecimento dos potenciais destrutivos decorrentes do alargamento do ciberespaço) e de se trabalhar, no âmbito multilateral, para o desenvolvimento de iniciativas de “controle de armas” e “desarmamento” (seguindo a lógica da construção de confiança característica da segunda metade do século XX) aplicadas à nova realidade das relações internacionais. Ao fim da obra, encontra-se – ainda – um glossário que torna acessível a parte mais técnica do livro aos não familiarizados com o jargão e as siglas empregadas na rotina de trabalho dos *geeks* da TI.

Em suma, apesar de não passar de um ensaio livre e sem amarras metodológicas, o livro apresenta um bom quadro geral de conceitos, temas e episódios que merecem



aprofundamento e tratamento analítico adequado no campo dos estudos de segurança e dos estudos estratégicos.

Recebido em 29 de maio de 2011. Aprovado em 10 de junho de 2011.