

Cyberdeterrence and Cyberwar

Martin C. Libicki

Rand Corporation (<http://www.rand.org/pubs.html>), 1776 Main Street, Santa Monica, California 90401-3208, 2009, 238 páginas, US\$26,40 (brochura), ISBN 978-0-8330-4734-2.

Vamos supor que o leitor seja administrador de sistemas, executando certos testes rotineiros, pertinentes às funções de gerenciamento de dados, quando se depara com algo que, a princípio, parece ser apenas um lapso do sistema. Após exame minucioso, inclusive a verificação dos servidores e equipamento, encontra alterações em alguns códigos e dados, revelando problema mais sério. Seria talvez a ação de hackers em busca de diversão, tentativa interna de sabotagem ou ataque cibernético? Neste último caso, retalia ou simplesmente finge que nada aconteceu?

Cyberdeterrence and Cyberwar, de Martin Libicki, aborda os temas, examina a diferença radical entre guerra cibernética e guerra convencional e a dificuldade de implementação e emprego de diretrizes de dissuasão cibernética. No que diz respeito às nações que possuem diretivas, o autor levanta questões como a determinação da identidade do agressor, motivação e a natureza da reação (e.g., retaliar, ignorar o incidente ou fingir que o dano foi negligenciável); a avaliação da importância de tal determinação; a adoção de diretriz “tolerância zero” versus a tentativa de distinguir entre verdadeiro ataque cibernético e hacking; e como travar guerra cibernética ou implementar estratégia de dissuasão, que inclui a formulação de motivos para sua utilização e o término de guerra sem aparentes sinais de danos, baixas ou (teoricamente) efeitos imediatos.

Libicki conclui, discutindo defesa cibernética, seu desenvolvimento e procedimentos (e.g., “métodos de dissimulação”, “red teaming” [Red Team é um grupo composto de membros da organização, treinados e formados, que fornece capacidade independente para explorar alterna-

tivas de planos e operações em ambiente operacional, do ponto de vista do adversário e outros], pp 171 e 173).

O fato do *Cyberdeterrence and Cyberwar* receber o patrocínio do Tenente-General Reformado Robert Elder Jr. da USAF, ex-Comandante da Oitava Força Aérea e Comandante do Componente Prático Conjunto para o Espaço e Ataque Global do Comando Estratégico dos EUA, outorga considerável credibilidade. Os leitores bem informados sobre o tema (ataques levados a efeito por grupos tais como o Anonymous e o LulzSec) e aqueles que desempenham funções administrativas de sistemas e projetos de informática devem estar bem familiarizados com certas teorias e casos apresentados. O ponto forte da obra é apresentar a evolução rápida e a constante mudança na área de guerra e dissuasão cibernética em formato de fácil compreensão, sem detalhes excessivos de processos em termos técnicos.

No entanto, existem falhas de formatação, organização e uso de abreviações que depreciam o valor do estudo e seu impacto. Por exemplo, a presença de páginas apenas parcialmente preenchidas (e.g., pp 75, 147 e 149) e hifenização desnecessária (e.g., “locked-down” [P. 151], “more-violent” [p. 72], e “flow-rate” [p. 155]) dá a sensação de que o livro é um rascunho e não manuscrito final. Além disso, não consta informação sobre o autor, credenciais, motivação para a redação do livro, ou metodologia empregada. Finalmente, a inclusão de lista de abreviaturas (p. xxiii) já de conhecimento geral é desnecessária. A tendência em deixar de reidentificar abreviações raras cria dificuldades (e.g., “RF” [p. xxiv] , só mencionada outra vez na página 164).

Além do mais, outras falhas, como a ausência de índice, além de gráficos confusos e mal explicados no Apêndice B, certamente prejudicam e aumentam a impressão desfavorável. Será que *Cyberdeterrence and Cyberwar* é relevante para a comunidade da Força Aérea? Apesar dos problemas acima mencionados, o livro oferece questões e teorias interessantes de guerra e dissuasão cibernética bem como o que significa para as atuais operações militares e a população civil. Recomendo a

leitura a todo o pessoal militar, mesmo aos não diretamente envolvidos em segurança de sistema ou informática em geral.

Mel Staffeld
Council Bluffs, Iowa

My Life as a Spy: One of America's Most Notorious Spies Finally Tells His Story

John A. Walker Jr.

Prometheus Books (<http://www.prometheusbooks.com>), 59 John Glenn Drive, Amherst, New York 14228-2197, 2008, 349 páginas, US\$25,98 (capa dura), ISBN 978-159102-659-4.

Um livro intenso, fascinante e controverso, *My Life as a Spy*, de John Walker reflete o importante diálogo político referente à segurança da informação. Além do mais, capta a atenção por vários motivos: como relato de espionagem verdadeira, faz com que o leitor cogite como Walker conseguiu vender segredos à União Soviética com impunidade. Tentarão comparar a experiência do autor com a imagem do espião retratada pela cultura popular e meios de comunicação, quer fictícios ou não; o elemento de suspense na narrativa não só oferece a perspectiva de programa de espionagem bem sucedido, mas também aborda os erros que levaram Walker à ruína; o livro possui apelo pessoal, revelando quem era esse mestre em espionagem e porque arriscou a própria vida, assim como a de amigos e familiares. Salientamos que os planos de Walker para expandir a rede de espionagem, a longo prazo, abrangiam até mesmo o próprio filho; levanta questões políticas que estimulam o raciocínio, abordando a desonestidade dos políticos, a tendência histórica dos Estados Unidos de exagerar a gravidade da ameaça soviética, as medidas de segurança anêmicas da Marinha, a prática de longa data do Departamento de Defesa de ultra-classificar arquivos, muito mais do que o necessário, bem como a seguinte questão: Será que a exposição de documentos secretos realmente danifica a segurança nacional? Muitas das questões políticas descritas por Walker continuam a recorrer. O debate atual da divulgação de registros militares e

diplomáticos pelo Wikileaks comprova o fato, o que leva à questões que os governos mundiais enfrentam para decidir o patamar de acesso apropriado nesta era moderna da informação. Na verdade, deve-se questionar a existência de segredos, dada a proliferação de computadores e conexões da Rede. Walker obteve dados, fotocopiando documentos e tomando fotos com microcâmera. Atualmente, dispositivos como câmeras pinhole, câmeras de espionagem e equipamento altamente tecnológico estão disponíveis ao público. Os usuários de computadores contam com acesso à vasta gama de dados, inclusive documentos, arquivos de áudio e vídeo em tempo real de agências de transmissão e webcams, sem mencionar fotos via satélite – tudo facilmente colocado na Internet em segundos.

Assim, os governos devem considerar a possibilidade de que as informações facultadas ao público assistiriam diferentes povos em seu avanço a governos democráticos e/ou à derrota de ditadores. O acesso instantâneo à informação também pode levar a estado de agitação perpétuo, instigado por indivíduos que exigem gratificação e resultados imediatos. Consequentemente, os governos devem decidir se é mais importante controlar a informação, classificando-a de secreta ou manipular os dados disponíveis ao público.

Walker alega que divulgou dados secretos para assegurar à União Soviética que os Estados Unidos não estavam planejando um primeiro ataque [nuclear]. O argumento que apresenta em sua defesa é o seguinte: Se os dois países souberem mais a respeito um do outro, a probabilidade de travarem guerra seria menor. Os leitores é que devem decidir se ele está somente racionalizando suas ações ou genuinamente promovendo o melhor uso de dados.

Recomendo *My Life as a Spy* porque mantém o interesse do leitor em diferentes níveis e porque explora, de forma que intriga, uma série de questões políticas.

Este livro, que vale a pena, será de interesse a público variado.

Major Herman Reinhold, USAF, Reformado.
Athens, New York

Gostaríamos de receber sua opinião

Distribuição: Texto aprovado para o público. Distribuição irrestrita.

Isenção de Responsabilidade

As opiniões e pontos de vista expressos ou inferidos neste periódico pertencem aos autores e não contam com a sanção oficial do Departamento de Defesa [Department of Defense], Força Aérea [Air Force], Comando de Treinamento e Educação Aérea da Aeronáutica [Air Education and Training Command – AETC], Universidade da Aeronáutica [Air University], ou quaisquer outras agências ou departamentos do governo dos Estados Unidos.

Este artigo pode ser reproduzido, parcial ou totalmente, sem necessidade de autorização prévia. Caso seja reproduzido, o Air and Space Power Journal – Português solicita a cortesia de menção..

<http://www.airpower.au.af.mil>