GUERRA CIBERNÉTICA

A próxima ameaça à segurança e o que fazer a respeito

RESENHA: Vinícius **Lacerda** Vasques[1]

O livro **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito** traça uma visão geral do domínio cibernético, bem como indica as capacidades, políticas e estratégias para um país mitigar suas vulnerabilidades nesse espaço. Por isso, ele atende a profissionais experientes da área tecnológica e estratégica, da mesma maneira que iniciantes nesse campo de estudo.

Richard Clarke, o autor, serviu na Casa Branca como Conselheiro Especial para Assuntos Nucleares durante quatro mandatos presidenciais. Sua experiência o levou a perceber como esta ameaça era perigosa para os EUA, credenciando-o para se tornar, no ano de 2000, o primeiro Conselheiro para Assuntos Cibernéticos dos presidentes norte-americanos. Para elaborar o livro, Clarke teve o auxílio de Robert K. Knake, um especialista em Relações Internacionais que possui diversos artigos sobre segurança internacional e cibernética publicados.

Clarke e Knake iniciam a obra apresentando como a guerra cibernética foi conduzida no passado e ilustra algumas vulnerabilidades potenciais para futuros ataques. Eles ainda sugerem que um conflito cibernético tenha o potencial de mudar o equilíbrio militar mundial alterando fundamentalmente as relações políticas e econômicas.

No segundo capítulo, os autores descrevem como as Forças Amadas norte-americanas conduziram a formação de suas Unidades de Guerra Cibernética, até criarem o *Cyber Command*, estrutura responsável por proteger as redes militares daquele país. Ele retrata a dificuldade no estabelecimento de responsabilidades para cada órgão, de forma a não

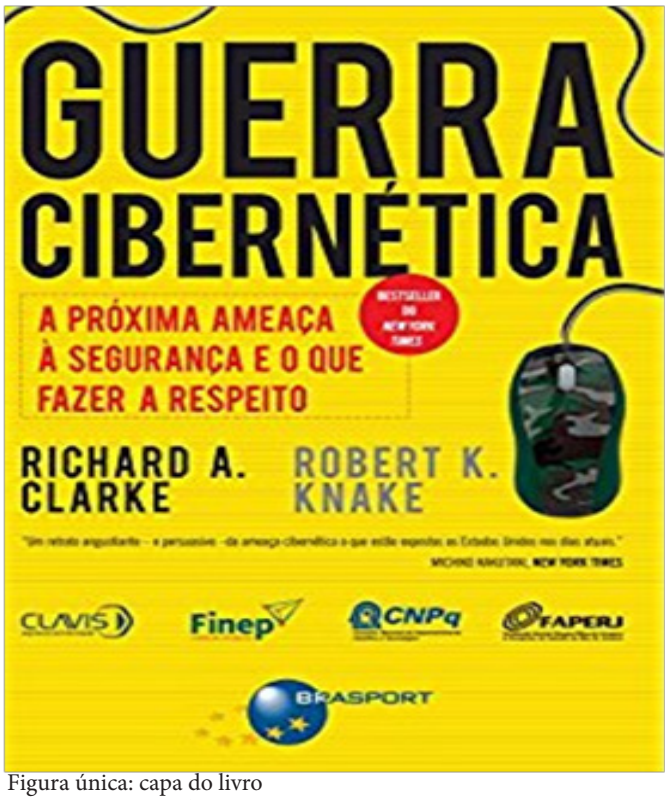

Figura única: capa do livro
Fonte: Brasport, Edição 1 (2015)

deixar lacunas na proteção cibernética do país. Eles também relatam a ativação de estruturas semelhantes em diversas Forças Armadas no mundo inteiro, destacando as russas e chinesas.

No capítulo seguinte, eles descrevem o "campo de batalha cibernético". Para tanto, detalham o espaço cibernético e todas as suas vulnerabilidades. Desta forma, eles traçam um cenário completo de um ataque cibernético e as suas consequências para uma nação.

O quarto capítulo trata das iniciativas norte-americanas para o setor, desde a década de 90. Eles apresentam que o insucesso do governo norte-americano em estabelecer medidas preventivas deve-se, principalmente, às dificuldades em regulamentar-se o setor privado e em rastrear-se um ataque cibernético. Aquele ramo controla as in-

[1]Oficial de Comunicações do Exército Brasileiro - Academia Militar das Agulhas Negras - Pós-graduado em Ciências Militares - Escola de Comando e Estado-Maior do Exército - lacerda.vinicius@eb.mil.br

fraestruturas críticas do país e não aceitam a interferência estatal. Deste modo, até a presente data não foi possível o estabelecimento de normas de segurança mínimas para o setor.

No capítulo 5, os autores propõem estratégias para criar políticas efetivas para lidar com operações cibernéticas. Clarke explica que a dissuasão cibernética não acontece da mesma maneira que da nuclear. Se por um lado, as armas cibernéticas não são usadas periodicamente, o oponente não saberá que você tem a capacidade. Por outro, o uso ostensivo dessa capacidade oferecerá a oportunidade ao adversário de neutralizar seu ataque. Sob o ponto de vista defensivo, esta capacidade por si só também não evitará um ataque.

No sexto capítulo, os autores utilizam a estratégia nuclear para ilustrar a complexidade em se estabelecer um planejamento para a utilização das novas armas fornecidas pela Guerra Cibernética. Eles ainda propõem uma tríade defensiva como mitgação aos efeitos de um ataque maciço cibernético. Tal proposta consiste em deixar o *backbone* da internet mais seguro, separa e fortalece os controles da rede elétrica e atualizar a segurança dos sistemas computacionais de Defesa.

No sétimo capitulo, Clarke ilustra uma suposta guerra cibernética dos EUA contra a China para explicar o poder ofensivo da Guerra Cibernética. Ele destaca que nações poderosas não foram para a guerra uns com os outros desde a Segunda Guerra Mundial por causa da dissuasão das capacidades letais que cada uma possui. Entretanto, atualmente, a guerra pode ocorrer no novo campo de batalha do ciberespaço em quais soldados não estão em combate direto. Desse exercício, ele destaca como aprendizado as seguintes questões: o uso da dissuasão, o conceito de começar primeiro, a preparação do campo de batalha antes da guerra, a disseminação global de um conflito regional, danos colaterais, controle de escalada, guerra acidental, atribuição, instabilidade de crise e assimetria defensiva.

O capítulo seguinte trata sobre as consequências de um tratado de controle de armas cibernéticas e o interesse dos EUA nesse tipo de acordo. Os autores destacam a vulnerabilidade norte-americana em face de um ataque dessa natureza, uma vez que aquela nação é extremamente dependente da internet. O capítulo também discute a abrangência desse acordo: incluir ou não a inteligência (espionagem) cibernética?

Finalmente, os autores propõem uma agenda a ser adotada, com base nas discussões anteriores, para garantir que os sistemas estejam seguros e impedir que as redes estratégicas de uma nação sejam alvos em uma guerra cibernética.

Desta forma, Guerra Cibernética é de leitura fácil e fornece informações valiosas sobre passado, atual e futuro situações cibernéticas e capacidades. A experiência no ramo dos autores adiciona emoção ao livro, tornando-o um excelente instrumento para que se aprenda mais sobre recursos e políticas cibernéticas.

REFERÊNCIA

CLARKE, A. Richard. KNAKE K. Robert. **Guerra Cibernética:** A próxima ameaça à segurança e o que fazer a respeito. Editora Brasport, 1ª edição, 2015.