Clarke, Richard A. e Knake, Robert K. Guerra Cibernética: A Próxima Ameaça à Segurança e o Que Fazer a Respeito. BRASPORT, Rio de Janeiro, 2015.

DESAFIOS PARA A ESTRATÉGIA DE DEFESA CIBERNÉTICA

CT (T) Gleice Cordeiro Fernandes

Em sua obra, Richard Clarke estimula a análise e discussão sobre um novo tipo de arma e guerra, baseadas em tecnologias modernas e empregadas em um campo de batalha não convencional. Trata-se da guerra cibernética cujo campo de batalha é conhecido como ciberespaço ou espaço cibernético. Clarke apresenta esse tema como algo que já vem sendo empregado por diversas nações, mesmo em tempos de paz. Assim, uma nação deve possuir tanto capacidade técnica para lidar com a defesa e os ataques cibernéticos, quanto deve considerar as estratégias para tais tipos de ações.

Nos oito capítulos que compõe o livro, o autor apresenta registros da evolução do tema guerra cibernética nos EUA, primeira nação a criar um Comando Cibernético. Com base nas suas experiências atuando no governo norte-americano, Clarke relata diversos episódios de ataques cibernéticos que envolveram os EUA, detalhando as estratégias ofensivas e defensivas aplicadas pelos diversos órgãos que atuam na defesa dessa nação. Assim como, revelou o quão os EUA são vulneráveis às ameaças cibernéticas pela elevada dependência de sistemas digitais que podem ser controlados por meio do ciberespaço. De fato, na atualidade praticamente todos os segmentos de um país tem se tornados especialmente dependentes de sistemas computacionais e redes digitais que, de alguma forma, se conectam com o espaço cibernético, o qual engloba tanto a Internet quanto as redes internas de organizações ou instituições. Tal dependência expõe infraestruturas críticas, militares e do setor privado a ameças cibernéticas devido ao fato do ciberespaço ser um meio naturalmente vulnerável.

O autor também critica a desvalorização da importância da cibersegurança pelos EUA, especialmente durante o início da administração do ex-presidente Bush. Além do sigilo desnecessário ao qual o assunto era tratado pelo governo norte-americano, segundo a opinião do autor, havia também uma falta de cooperação entre o governo e o setor privado. Para a implementação de uma estratégia de defesa cibernética, Clarke defendia a elaboração de uma regulamentação de nível federal que englobasse três setores críticos: a espinha dorsal da Internet nos EUA, a proteção da rede elétrica e a proteção da rede do Departamento de Defesa. Entretanto, diversas questões problemáticas envolveriam os requisitos de segurança que deveriam ser adotados por esses setores, tais como questões quanto a privacidade dos dados que trafegam pela Internet e gastos financeiros adicionais pelas empresas de energia e telecomunicações. Tais questões demandariam uma discussão pública, assim como a participação do setor privado e transparência do governo a respeito da defesa cibernética no país.

A partir de então, o autor descreve um exercício hipotético de guerra cibernética, abordando cenários que poderiam acontecer em uma situação real e cujas lições aprendidas seriam úteis para a formulação de uma estratégia ofensiva por parte dos EUA. Certamente, tal iniciativa é essencial para a preparação de uma nação na definição de sua estratégia cibernética. Os exercícios são um meio para promover o treinamento e a capacitação dos órgãos responsáveis pela defesa de uma nação, assim como proporciona a colaboração entre setores do governo, militares e civis que gerenciam as infraestruturas críticas, a exemplo do Exercício Guardião Cibernético organizado pelo Comando de Defesa Cibernética do Exército Brasileiro (ComDCiber). Porém, o autor destaca, ainda, que para a

elaboração dessa estratégia deve-se pensar também nas questões sobre leis internacionais e demais convenções. Tal como existem leis de cooperação internacional, um acordo contra atos de ataques cibernéticos, especialmente contra alvos civis, seria do interesse dos EUA e, a propósito, também de outras nações.

Em suma, o livro não somente alerta sobre a importância do tema, mas também fornece uma série de informações que conduzem os leitores a uma reflexão sobre o alcance de um ataque cibernético e suas implicações. À época da publicação de sua obra, o autor já dizia que: a guerra cibernética é real; é global; e já começou, fato discutido recentemente na guerra da Rússia contra a Ucrânia, onde alguns especialistas consideraram o conflito híbrido, por envolver outros meios, a exemplos dos ataques cibernéticos. Logo, é indiscutível que essa obra é uma rica fonte de consulta para um aprofundamento no estudo sobre segurança cibernética, bem como no pensamento analítico para a definição de estratégias ofensivas e, principalmente, defensivas no ciberespaço.