CLARKE, Richard A. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito**. BRASPORT, Rio de Janeiro, 2015.

Autor: CT 98.0453.34 **IGOR** DA SILVA **ALVES.** **OM:** DPMM

A Guerra Cibernética e seus desdobramentos no meio civil

O aumento exponencial da conectividade e dos sistemas de automação observado na última década ocasionou, principalmente, um substancial incremento na exploração de vulnerabilidades desses sistemas. Neste contexto, o autor do livro, que possui vasta experiência nas área de espionagem e estratégia nuclear, enumera diversas ações que utilizaram o espaço cibernético como ambiente para ações ofensivas, discorre sobre as brechas dos EUA no campo cibernético e propõe, em seu epílogo, medidas para se estabelecer uma estratégia de defesa contra tais ações.

Os diversos relatos de ações ofensivas desenvolvidas no ciberespaço expostas ao longo do livro demonstram como o termo "Guerra Cibernética" deixou de ser exclusivamente militar e passou a ser cada vez mais pervasivo no meio civil. Nesse contexto o autor destaca, de forma bastante apropriada, os múltiplos ataques cibernéticos russos contra a Estônia desencadeados após o desentendimento gerado pela remoção de um símbolo patriótico russo de uma praça na cidade de Talim. Tal episódio demonstrou como ataques cibernéticos podem afetar à população civil de maneira bastante profunda.

No que concerne à defesa cibernética, são apresentadas críticas bastante contundentes em relação ao atual modelo de defesa cibernética dos EUA, no qual as Forças Armadas Norte Americanas são responsáveis pela defesa das redes militares enquanto a defesa do ciberespaço civil é atribuição das grandes empresas de comunicação que fornecem, aos provedores de internet, acesso à rede mundial. No entanto, é oportuno ressaltar que tal concepção, mesmo nos dias de hoje, certamente encontraria diversas limitações tecnológicas e altíssimo custo. Tal proposta compreenderia a análise de todo o tráfego da rede, com diminuição da privacidade online e esperada resistência da sociedade civil, tal qual foi observada nas denúncias de vigilância do tráfego da WEB, por parte do governo dos EUA, reveladas por Edward Snowden, ex-administrador de sistemas da CIA.

Ao propor uma estratégia defensiva cibernética, o autor se posiciona de maneira contrária à adoção de sistemas digitais de controle da geração de energia e transporte ferroviário. Tal alegação, segundo o autor, se deve ao fato que o dano colateral ocasionado por uma ofensiva cibernética a essas estruturas afetaria, profundamente, a capacidade de se contrapor aos ataques originários. Ao assumir uma posição antagonista à adoção de tais sistemas, o autor deixa de reconhecer os inegáveis avanços proporcionados pela modernização dos sistemas de energia e ferroviário e a atual eficácia da defesa de tais sistemas que, s.m.j., ainda não apresentaram falhas graves a ponto da sua adoção ser discutida. Também cabe ressaltar que não há relatos de atentados terroristas executados nessas infraestruturas.

Por fim, em que pese o fato do autor se posicionar, em alguns momentos, de maneira oposta à diversos especialistas no assunto - presumivelmente por ter vivenciado situações delicadas, quando ocupou o cargo de Assessor Especial do Presidente dos EUA para Segurança Cibernética - é inegável que tal obra constitui um marco no debate da questão da segurança do ciberespaço e as terríveis consequências as quais os alvos de tais ataques estão submetidos. Em tempo, é imprescindível ressaltar que, passados cerca de quatro anos da publicação do livro, armas cibernéticas com maior poder destrutivo não abordadas pelo autor já tenham sido utilizadas ou encontram-se inertes até a próxima ofensiva cibernética.