KNAKE, ROBERT; CLARKE, RICHARD A. "CYBER WAR: THE NEXT THREAT TO THE NATIONAL SECURITY AND WHAT TO DO ABOUT IT"

(New York: Harpercollins Usa, 2010)

Fellipe Leão[1]

No silêncio e quase anonimato, sem a percepção das grandes massas, trava-se uma guerra internacional que, apesar de quase total desconhecimento civil, é global, reconhecida, comprovada e decisiva para o nosso futuro: A cyber guerra.

Tendo como base os artigos "Cyberwar – it is time for countries to start talking about arms control on the Internet" e "War in the fifth domain – are the mouse and the keyboard the new weapons of conflict? ", publicados no the economist há três anos, o livro "Cyber war: the next threat to the National security and what to do about it" se baliza numa dicotomia gerada entre os que acham que uma guerra cibernética, que tenha como resultado uma catástrofe sem precedentes na maneira que vemos o mundo hoje, está longe de acontecer e daqueles que veem tal evento como totalmente possível e que deve ser evitado.

Defendendo esta segunda visão sobre o assunto, Richard Clarke e Robert Knake, responsáveis pela autoria do livro, expõem um

1 É aluno do curso de licenciatura plena em Computação da Universidade Federal Rural de Pernambuco (UFRP)

ponto de vista, logo nas primeiras páginas de sua obra, que nos dá uma ideia do porquê de tantos serem os descrentes quanto ao perigo iminente da guerra cibernética: a censura e sigilo quanto à informação a cerca de ataques cibernéticos, de quaisquer portes, que ocorrem com frequência assustadora entre governos.

"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." Com este trecho, fica claro tudo o que foi supracitado.

As grandes potências mundiais, principalmente os Estados Unidos da América, país o qual tem um maior investimento no que se refere à segurança do ciberespaço, têm grandes "escudos" contra uma possível catástrofe que viesse ocorrer como consequência de uma guerra propagada pela grande rede, mas será que é o suficiente?

O capítulo inicial do livro, portanto, reconta vários eventos associados à ciberguerra, os quais até tiveram um pouco de conhecimento do público em geral por suas consequências, de maneira clara e detalhista, com muitos dados minerados por Richard Clarke, que por muito serviu os governos americanos em departamentos relacionados à segurança, de uma maneira geral, e, no governo Bush, foi conselheiro especial para a segurança no ciberespaço.

No decorrer da leitura, nota-se a preocupação dos autores por evidenciar a fragilidade que os governos têm em seu ciberespaço, mesmo dedicando consideráveis quantias em pessoal e treinamento para protegerem-se de qualquer ameaça neste campo.

Estratégias de defesa, bem como as de ataque, a possíveis ameaças cibernéticas são bem detalhadas por Clarke, que cita casos como os ataques à Estônia e Geórgia (todos acontecidos nos últimos cinco anos) e alguns ataques de menor repercussão que ocorreram nos E.U.A, como exemplos do quão real e prejudicial é esta guerra que já está sendo travada por baixo dos narizes de todos aqueles desavisados que dela não escutam falar.

O grande problema, que torna a ciberguerra algo que mereça bastante atenção por parte dos governos, é que cada vez mais temos uma infraestrutura super dependente dos meios online de comunicação.

Portos, aeroportos, bancos e demais serviços prestados aos governos e a população estão quase que em sua totalidade unicamente dependentes da grande rede, o que faz de países bastante desenvolvidos nestes quesitos também sejam considerados mais vulneráveis.

Sobre a vulnerabilidade de países muito dependentes versus a sua capacidade de defesa sobre estas vulnerabilidades e seu potencial ofensivo, Clarke e Knake propõem, nos capítulos sequentes do livro, mensurar qual seria o "poder de ciberguerra" de diversos países ao redor do globo, segundo estes critérios.

Adotando uma média que vai de zero (0) a trinta (30), lê-se que, por mais assustador que pareça, a Coréia do norte teria o maior poderio numa guerra pautada no espaço virtual. Isto se deve a pouca dependência que o país tem em relação aos seus sistemas online e a facilidade de desconectar estes sistemas, criando uma barreira entre o espaço virtual e o real, fazendo com que o segundo estivesse mais protegido no caso do primeiro ser invadido.

Num cenário imaginário, a partir das análises feitas sobre o poderio de determinados países num ambiente de ciberguerra, supõe-se então o que poderia acontecer se os Estados Unidos fossem atacados e tivessem seu ciberespaço invadido. Quais seriam as consequências, como se identificariam os possíveis agressores e como seria feita a defesa num caso de invasões de maiores proporções tornam-se os assuntos abordados nos últimos capítulos do livro, bem como a proposta de um trabalho mais multilateral por parte dos E.U.A, que tem pouca associação com países aliados quando se trata de ciber segurança.

O contorno de catástrofe inserido com a possibilidade de uma guerra no ambiente virtual, somado ao contexto quase normativo que as sugestões de Clarke e Knake apresentam, faz com que o livro "Cyber war: The next Threat to the National Security and what to do about it." seja uma obra que, no mínimo, mereça a atenção de qualquer um que se interessa por ciência e tecnologia, e como estas influenciam e chegam quase a ditar, de maneira praticamente direta, o avanço da atividade humana em todas as suas áreas de atuação, bem como o retrocesso que a ciência e tecnologia, aplicadas à informação, pode trazer à nossa sociedade cada vez mais dependente e interligada a elas.