CYBER WAR: The Next Threat to National Security and What to Do About It
Buckham, Chris
Leatherneck; Aug 2012; 95, 8; Marine Corps Gazette & Leatherneck Magazine of the Marines
pg. 49

CYBER WAR: The Next Threat to National Security and What to Do About It. By Richard A. Clarke and Robert K. Knake. Published by Ecco (Harper Collins). 304 pages. Softcover. Stock #0061962244. $14.40 MCA Members. $15.99 Regular Price.

In a recent edition of the *International Herald Tribune*, there was an OpEd article by Vincent Cerf expressing concern about the potential limitations and oversight being considered for the Internet at an upcoming International Telecommunications Union (an organization within the UN) summit. The nature of the article underlines the fundamental debate raging in today's world where the unregulated Internet is being used for both positive and negative outcomes and provides the backbone within which threats could be directed at the world's increasingly digitized social and economic structures.

The premise of Richard A. Clarke and Robert K. Knake's book "Cyber War" addresses this issue directly with a broad-ranging review of what it is, how it is being used (both offensively and defensively), how prepared the world is for it and what recommendations they would suggest on how nation-states can ensure that they don't fall victim to it. Clarke acknowledges at the outset that this is a very complex subject; one fraught with aspects that transcend social, economic, national and cultural boundaries; and one where not enough attention is being paid.

Clarke approaches the issues, background and recommendations in such a manner that they are accessible to the common reader. He does not shy away from identifying positions that run contrary to his own. This approach is a major strength of the narrative.

Cyber warfare is unlike any potential battlefield that we, as nations, have ever faced. The potential for a nation with very limited traditional offensive capabilities to undermine the military strength of a first world power with a few keystrokes that shut down power grids or communication systems is a profound change in paradigm. Indeed, as Clarke points out, it fundamentally alters the art and practice of international relations (and warfare). Further complicating the issue is that access to this potential is not limited to nation-states but to individuals in the form of terrorists, hackers and activists.

This book is important because it provides education to those not familiar with the threat and promotes dialogue within the circles of government, industry and society on what we should do. A major stumbling block to the discussion is as basic as trying to identify what constitutes a threat that requires government intervention or oversight. For example, if you receive spam that shuts down your server, is that an attack or simply malicious behavior on the part of the originator of the spam? Does a self-replicating virus constitute a national-level threat?

Coming to common agreement on the definition of what constitutes cyber warfare is a huge undertaking in and of itself. Clarke points out that this agreement is not solely resting within the purview of national governments as traditional threats (i.e., gas warfare) have done. This also has to include industry and society as they will be profoundly affected by decisions based upon international agreement.

The creators of the Internet had no idea of the range and scope of its potential; neither did governments. Originally designed to support research and development within closed circles of scientists and academics, it has expanded through industry to provide a worldwide interface that largely has developed from the bottom up, free of regulatory oversight. This always has been touted as one of the Internet's strengths. Unfortunately, as "Cyber War" identifies, it also has resulted in being one of its great vulnerabilities (or opportunities depending upon your perspective). Clarke points out that this has been recognized, but that nothing has been done for a number of reasons.

Negotiations concerning traditional conventional weapons systems and the nuclear threat have been accomplished much through deterrence. That discussion centered on capability and included academics and military experts providing government negotiators with hard data that could be balanced against. In the world of cyber warfare, there is little idea of the offensive or defensive capabilities of potential adversaries (or even who those adversaries may be). Given that fact, how does a nation prepare itself and, within the realm of negotiated treaty, how does a nation ensure compliance?

Clarke identifies and explains the five main areas of vulnerability for nation-states: (1) lack of encryption, (2) the decentralization of the system, (3) border gateway protocols (essentially how information enters the system), (4) domain naming system (how information is identified), and (5) the propagation of malicious traffic. He then recommends methods by which these can be addressed (acknowledging, however, that this will require some form of regulation). For Clarke, the issue is not *should* there be a form of regulation, but more, what kind of and under whose authority should this be done.

The irony of cyber warfare to the first world nations is that the development and propagation of the Internet has made them more vulnerable than ever to threat due to the high level of digitization of banking, power, transportation, etc. That which has made the West stronger also has made it weaker. This is an excellent book to explain the issues at hand and to stimulate discussion toward addressing the challenges of ensuring that the Internet remains safe while continuing to provide a medium for making the world smaller.

Maj Chris Buckham

Editor's note: Major Buckham is a logistics officer in the Royal Canadian Air Force. A graduate of the Royal Military College of Canada, he holds a bachelor's in political science and a master's in international relations. He presently is a logistics officer with the multinational branch of EUCOM (J4) in Stuttgart, Germany.