Book Review

Cybersecurity and Cyberwar: What Everyone Needs to Know

by P.W. Singer and Allan Friedman

Oxford University Press, New York, New York, 2014, 320 pages

Reviewed by Lt. Col. Andrew K. Murray
- U.S. Army Command and General Staff College

One could immediately empathize with P.W. Singer and Allan Friedman's challenge of encapsulating "what everyone needs to know" about cyber security/cyber war into one book. To begin with, it is impossible to categorize "everyone." Despite the title, we projectively ascertain the book appeals to a specific market niche of professionals who are novices in the technical aspects of cyberspace, dilettantes in the analogous understanding of the cyber phenomenon, but Subject Matter Experts (SME) in their particular field.

The authors unambiguously open the book with their stated purpose. They speak of a vast knowledge gap, especially egregious among many policy makers in the cyberspace field. If policy makers are the tip of the pyramid, SMEs mentioned in the first paragraph most likely form the base of the intended audience. The book, in and of itself, is neither a placebo, nor a panacea to remedy this knowledge gap. It serves as a satisfactory commencement though, toward understanding the cyberspace phenomenon.

The authors tacitly imply that a foundational knowledge of the internet (what is it and how it works) is a prerequisite for launching into the more strategic and analogous aspects of cyber security/cyber war. This brings into question, how much foundational/technical knowledge is too much (or too little) for the intended readers? They gloss over some key foundational technical aspects of the internet such as packet switching and layered architecture. A methodology for addressing these key technical/foundational topics could be a "top-down" approach starting with the network edge; moving to the network core; addressing protocol layers beginning with the application layer; and finally working toward the physical layer.[1] The authors compensated for any dearth of technical foundation by addressing the salient question of what is cyberspace? The definitional disquisition is a practical segue into the history of the internet, which in turn, is an effective transition into evolving internet governance. The history and governance portion was captivating in and of itself but could have been rendered so much more pedagogically ergonomic if the authors had proceeded in sequential order. A timeline of key events would have been a coup. For example, an effective method could be the explanatory sentences and paragraphs culminating in a key events timeline.

With the technical and foundational aspects covered, the authors moved into the contemporary

intriguing aspects of cyberspace to include cyber attacks, hactivism, anonymous, spying, stuxnet and cyber terrorism. They delve into a rather enlightening (for the general public), "focused study" on the U.S. cyber force structure detailing the structure and mission of Cyber Command (CYBERCOM) and their symbiotic relationship with the National Security Agency (NSA). Beyond a few misinterpretations of the unique military parlance (double hatted versus dual hatted), Mr. Singer and Mr. Friedman did a fairly good job of representing the mission, organization, structure and parameters of our U.S. cyber forces! The next focus study covered the Chinese approach to cyber warfare. The organizational diagrams of suspected Chinese cyber units were validated against our Foreign Military Studies Office (FMSO) and were not found wanting. A missed opportunity for the authors is addressing the Chinese concept of campaign stratagems. China has creatively fused high-technology and stratagems in order to execute operational high-tech stratagem applications.[2] Possibly this could be addressed in a second publication? One can appreciate the author's elucidation, reference the pessimistic interpretation of the covariance between U.S. and Chinese cyber power (with the internet serving as the dependent variable, in this case). Singer and Friedman verily contend that China is not utterly besting us in the cyber domain. In doing so, they allay fears that we need to learn Mandarin. They skillfully illuminate the fact that, for one, the U.S. invented the internet and it is still under some form of U.S. governance or commercial dominance. Secondly, our overall economy and research/development is far ahead of China's. What Singer and Friedman do not wrestle with is the concept of our ingrained avant-garde nature, propelling innovation and keeping the U.S. on the leading-edge of cyber technological development.

The final part of the book is well suited for the military culture and mindset. In the first part of the book, they laid a foundational base, the second part of the book he expounded on the rueful problems associated with the cyber phenomenon including crime, terrorism and foreign relations. In the last phase of the book, they offer solutions, under the auspice of "what can we do?" They astutely propose we challenge the underlying basis of our analogies and metaphors.[3] Singer and Friedman challenge us to reframe the problem, move away from the cold war analogies and evaluate alternative models to deal with cyber challenges. They equate malware more to a communicable disease and consider the public health model. They also suggest a maritime piracy comparison and analogy. They prod law makers into greater action by suggesting meaningful legislation i.e. disclosure laws. They contend a codified system of cyber security incentives would prove useful. Importantly, they focus on personal actions and individual responsibility.

In conclusion, *Cybersecurity and Cyberwar* nourishes the intellectual desire to understand the world in which we live. It is valuable to both the policy maker and the practitioner. It has the potential to promote a common understanding in the realm of inter-agency cooperation between various governmental, as well as commercial entities. It is worth the read. ***IAJ***

Notes

1 Jim Kurose and Keith Ross, "Computer Networking: A Top-Down Approach," 2013, Pearson Education Inc., Addison-Wesley, New Jersey.

2 Timothy L. Thomas, "The Dragon's Quantum Leap: Transforming from a Mechanized to an Information Force," Foreign Military Studies Office (FMSO), Fort Leavenworth, Kansas.

3 Dr. Richard Paul and Dr. Linda Elder, "Fallacies …", The Foundation for Critical Thinking, Dillon Beach, California.