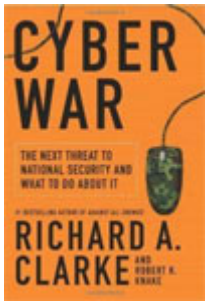

CSAF Book Review: Cyber War: The Next Threat to National Security and What to Do about It

Cyber War: The Next Threat to National Security and What to Do about It, (First edition, 2010), by Richard A. Clark and Robert K. Knake, HarperCollins Publishers, 10 East 53rd Street, New York, NY, 10022, 290 pages, US$26, ISBN: 978-0-06-196223-3.

Get the Book

A few years back, the US Air Force presented me with a professional development opportunity that proved to be a tremendous personal challenge. I received orders to become director of war-fighting integration in SAF/XC, our service's communications and computers directorate in the Pentagon. At the time of assignment notification, my beautiful bride astutely observed, "You know in this world of ones and zeroes, you're a zero, don't you?" Candidly speaking, I must confess that even after a year of Headquarters Air Force experience with all things cyber, I remain a zero in this area. That said, the SAF/XC job did pique my interest in this fascinating new domain through which we project airpower in defense of our nation.

This interest is what inspired me to select *Cyber War* as my first book off the Chief's 2011 Reading List. The highest praise I could offer is that even this "cyber zero" understood its contents. Former White House national security coordinator, Richard A. Clarke, and Council on Foreign Relations international security fellow, Robert K. Knake, have written a book that is remarkably readable and remarkably relevant. I highly recommend this fine work to anyone who wants to learn more about *The Next Threat to National Security and What to Do about It*, the book's intriguing subtitle.

For me, there are three big takeaways. First, and perhaps most significant for the citizenry of this country to comprehend, is the fact that cyber war is so much more than a military security matter; it is a genuine national security issue that demands a fully coordinated "whole of society" strategy, one developed and executed by all the key players in the government and the private sector. The authors rightly acknowledge the challenges posed by any governmental role in dealing with private-sector vulnerabilities, but they come down hard on the side of increased federal regulation in a domain originally conceived and birthed as "open and free." While any

proposal for more government involvement often generates potent antibodies among folks who associate themselves with both ends of the political spectrum (and every "leaning" in between), Clarke and Knake present a compelling case worthy of further debate.

The second big takeaway is the authors' hard-to-dispute assertion that cyber war presents a greater threat to our United States than it does to any other nation. This observation flows naturally from the recognition that cyber dependence equals cyber war vulnerability. From sea to shining sea, people across our great land enjoy the ease and power of e-mail, Google, Facebook, and all the other "net goodies" to be found in those fluffy, friendly cyber "clouds." But as Clarke and Knake note, we have critical infrastructures throughout the 50 states and US territories that are frighteningly net-dependent with no nonnet backups; their main concern being (say it with me; say it loudly; let me hear you say it; all together now) our nation's electric power grid. (Peruse the last chapter to appreciate the previous parenthetical comments.)

The third big takeaway is, for me, the most sobering of all. The cyber problem set is evolving more rapidly than the cyber solution set. Put another way, we are behind the power curve and falling even further behind each passing nanosecond due to the lightning quick pace of change in the "information age." As you turn the pages in *Cyber War*, this reality will eventually sink in and drive you to beg for answers to the question, So what can we do about it? And that is where the authors do not let their readers down. Clarke and Knake propose an innovative six-step agenda to address this rapidly emerging national security threat.

The agenda begins with a call for open, informed public dialogue about cyber war, or as the authors describe it, "thinking about the unseeable." Because this threat is not as visible as a Cold War mushroom cloud or an attack by terrorist-piloted airplanes, cyber war is something that some people would rather not think or talk about. But just as "hope is not a strategy," neither is "wishing it away." The second step defines a defensive triad that focuses on securing the tier-1 Internet service providers (ISP), the electric power grid, and the Defense Department's networks and cyber-dependent weapon systems. The third step advocates a more aggressive approach to combating cyber crime. When one contemplates a "fee for service" use of the tools of cyber criminality by, say, the perpetrators of 9/11, one fully understands why this particular step in on the agenda.

The fourth "must do" is the adoption by the United Nations of a cyber war limitation treaty (CWLT). Clarke and Knake detail what CWLT One would look like, but I leave that for you to discover on your own. Suffice to say, this proposal recognizes the importance of some form of international agreement on behavioral norms in the cyber realm. Step five simply highlights the need for research on more-secure network designs, with an emphasis on tomorrow's software fixes for today's software glitches that make us so vulnerable to cyber war. The sixth and last step reemphasizes the authors' earlier observation that cyber war is a *national* security threat that demands presidential involvement. Entitled "It's POTUS," this final section concludes with some proposed remarks for our president to deliver at a future UN General Assembly session. As Clarke and Knake conclude, "It could be a beautiful speech, and it could make us safer."

The book also includes interesting discussion on rethinking deterrence strategy in this brave new world. The interesting twist here is that the authors focus less on the oft-mentioned "attribution

difficulties" and more on the challenges associated with achieving a cyber "demonstration effect," similar to that provided by nuclear tests during the twentieth century. The good news: such a "demonstration effect" would serve to underscore both key ingredients of successful deterrents, capability and will. The not-so-good news: such a demonstration effect may not be feasible in the cyber era.

Clarke and Knake also describe the importance of "resilience" in the face of cyber attack. I found this portion particularly interesting in light of what I perceive to be an encouraging shift in DoD strategy away from a "Maginot Line" defense mentality toward a mindset of "mission assurance." Interestingly, this new idea for handling cyber war mirrors a concept we still exercise in operational readiness inspections when under simulated attack from nuclear, biological, chemical, and other life-threatening weapons, a concept known as the "ability to survive and operate."

Some final food for thought as I prepare to assume duties as the next commander and president of the Air University. This regionally accredited and internationally recognized academic institution has its roots in the Air Corps Tactical School, better known by its acronym, ACTS. During the interwar years, some of the greatest minds in the Army Air Corps applied innovative and forward thinking to advance theory on the application of airpower. Their ideas greatly influenced how the Air Corps planned and executed in World War II. One of those great ACTS minds, Maj Gen Muir Fairchild, became the first Air University commander. At opening ceremonies in 1946, General Fairchild cautioned, "We must guard rigorously against the danger of looking backward too much, against the feeling that we have learned the answers to future war. . . . This is not a post-war school, it is a pre-war school."

A fellow general officer noted recently that with regard to the cyber domain, we are in the interwar years. A thought dawned on me. If we are indeed in the cyber interwar years, perhaps now is the time to establish a "cyber ACTS" to enable some of the greatest minds in today's Air Force to advance thinking about cyber war. A cyber ACTS could build upon the exceptional work already being done at the Air Force Institute of Technology (AFIT) Center for Cyberspace Research and other cyber-focused service institutions. It could consist of Air University students, faculty, and researchers (whether at Maxwell AFB, Wright-Patterson AFB, or elsewhere), and subject matter experts from the Air Staff, Air Force Space Command, and the Air Force Research Laboratory, to name but a few organizations. A cyber ACTS could allow for both real and virtual attendance and participation. Finally, a cyber ACTS would be in keeping with General Fairchild's vision of Air University as a prewar school. Just a thought.

Let me conclude where I began. Whether you consider yourself a "one" or a "zero," you will find *Cyber War* to be informative and well worth your time. While the contents are alarming, I do not believe the authors are alarmists. Richard Clarke and Robert Knake have issued and justified a strong call for action. It is a call which I believe our great nation ignores at its own peril.

Lt Gen David S. Fadok, USAF
Commander, Air University