Naval War College Review

Volume 72
Number 4 *Autumn 2019*

Article 11

2019

Review Essay: Full-Bodied Cyber without the Hype

Sam J. Tangredi

Martin C. Libicki

REVIEW ESSAYS

FULL-BODIED CYBER WITHOUT THE HYPE

Sam J. Tangredi

Cyberspace in Peace and War, by Martin C. Libicki. Annapolis, MD: Naval Institute Press, 2016. 478 pages. $55.

As a fellow at the Institute for National Strategic Studies at National Defense University in the early 1990s, Martin Libicki was one of the first defense analysts to write on the security implications of information warfare and the Internet. His monographs *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon* (1994) and *What Is Information Warfare?* (1995) were considered cutting-edge treatments, containing such recommendations as making heavy investments in smart sensors and establishing a corps of information warriors.

Many of his recommendations were met with varying degrees of skepticism at the time. In a review of *The Mesh and the Net* in the July–August 1994 edition of the prestigious policy journal *Foreign Affairs,* Professor Eliot Cohen displayed a retrospectively humorous lack of prescience by stating that Libicki's "proposed courses of action—the creation of a corps of information warriors, among others—make less sense than the author thinks. It would have made as much sense to create a corps of combustion engine warriors early in the twentieth century." What a difference a couple of decades can bring.

Dr. Sam J. Tangredi is a professor of national, naval, and maritime strategy and the recently appointed inaugural Leidos Chair of Future Warfare Studies at the Naval War College. A retired Navy captain, his active-duty billets included serving as head of the Strategy and Concepts Branch of the Office of the Chief of Naval Operations and director of strategic planning and business development for the Navy International Programs Office, in addition to command at sea. He is the author of numerous articles on strategy and defense policy and has published five books, including Anti-access Warfare: Countering A2/AD Strategies *(Naval Institute Press, 2013).*

Naval War College Review, Autumn 2019, Vol. 72, No. 4

Yet, throughout his early studies, Libicki himself remained skeptical that American civil infrastructure would face a major cyberwarfare threat. As he states in the introduction to *Cyberspace in Peace and War,* "Then, as now, it was hard to conclude that cyberwar was going to trump every

other form of warfare. I was confident that the threat from cyberspace could be contained, in part because I believed that people, aware of the threat, would not willy-nilly connect critical systems (such as those that supply electric power) to the Internet. In this, I was wrong" (p. 1). Once Libicki recognized how wrong his assumption was and how vulnerable American companies would make themselves for the sake of cost cutting, profit, and expediency, he built an influential career analyzing the topic of information warfare and cyber war, primarily as a senior policy analyst with the RAND Corporation. At RAND he has written or contributed to over a half-dozen studies sponsored by the Department of Defense. At the time of this book's publication, he also was a distinguished visiting professor in cybersecurity studies at the U.S. Naval Academy.

Drawing on his studies, previous work, articles, and reports, Libicki built *Cyberspace in Peace and War* into his masterwork, one of the most extensive yet clearly written compendiums on cybered threats, attacks, strategies, and vulnerabilities. At 478 pages, it looks like an encyclopedic manual—albeit with a well-written narrative—and in a sense it is. It may not have the conceptual depth of Chris C. Demchak's *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (2011) or the breezy, popular approach of P. W. Singer and Allan Friedman's *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014). Rather, it has thoroughness; there seems to be not a single cybered conflict topic that Libicki does not address in some detail, from "How to Compromise a Computer" (chapter 3) to "Sino-American Relations and Norms in Cyberspace" (chapter 33).

Libicki refers to his book as a "text" intended to "make readers more intelligent consumers of the news, more intelligent users of technical advice, and more intelligent critics of the decisions that countries make with respect to the threat from cyberspace" (p. 3). As is apparent, it is not a book for cyber specialists, who presumably know more than the basics of the author's long list of cybered topics. But it is a book for all others, particularly national security professionals who want an extremely comprehensive initial immersion into the subject. Libicki indeed scores a "hat trick" on his three goals.

The book's format is eminently logical, with thirty-four chapters divided into five sections. In the first section, "Foundations," Libicki discusses types of cybered attacks, methods of providing security, and what governments can and cannot do in terms of defense. The second section, "Policies," begins with an examination of cyber espionage, system vulnerabilities, and how an operational cyber war might begin—Libicki sees surprise attack as a likely scenario. Section 3, "Operations," views the conduct of cybered war in terms of an organized campaign that may or may not include kinetic effects.

It will be most surprising to die-hard proponents of the belief that "cyber is its own warfighting domain equal to land, sea, air, and space" that Libicki—with his long study of information warfare—disagrees with this approach, declaring that there is "no domain, no cyber equivalent of Billy Mitchell" (p. 165). Libicki instead states, "The desire to see cyberspace as a warfighting domain is deeply ingrained in doctrine and the minds of those who carry out such doctrine. This chapter argues that this concept is misleading, perhaps pernicious[;] . . . if cyberspace is not a 'domain,' what is it? [O]ne answer may be that 'it' is a set of tools that have a related set of objectives in common" (p. 167). In answering the argument that the military needs to assess cyber as if it were a domain if it is to properly man, train, and equip to fight in it, Libicki replies simply, "Militaries do this for electronic warfare without its having been elevated into a separate domain" (p. 167).

Section 4, "Strategies," expounds on both symmetric and asymmetric responses to cyber attack and the potential for escalation into kinetic warfare, and then focuses on the deterrence of such attacks, examining deterrence topics such as attribution, the will to retaliate, and punishment or denial. In the concluding chapter of this section, the author examines the outcome of cyber attacks against an opponent's nuclear command-and-control systems. Those who think that there should be an arms-control regime to prohibit this may be disappointed by Libicki's conclusion that the "low odds of making cyberwar work" against a hardened (and isolated) nuclear command-and-control system makes such a diplomatic effort essentially irrelevant.

Section 5 concludes the book by examining norms in cyberspace—with particular attention given to the *Tallinn Manual,* a document that the Naval War College Stockton Center for International Law played a major role in creating—and Sino-American discussions. During People's Republic of China president Xi Jinping's visit to the White House in September 2015, he and President Barack H. Obama announced, "The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property . . . with the intent of providing competitive advantages to companies or commercial sectors" (pp. 344–45). But notably there was no agreement on an enforcement mechanism or the use of cyber espionage for military purposes. Libicki seems agnostic about the effectiveness of norms.

One of the questions this worthy book poses but deliberately leaves unanswered for readers to debate as a "fundamental question for U.S. policy" is whether "it is more important [for the United States] to pursue advantage in cyberspace (for both espionage and attack) or to make cyberspace more secure for everyone" (p. 350). That is indeed a question for extensive debate, although it does raise a

second question: Can cyberspace really be made "secure"? On this question, the conclusion of *Cyberspace in Peace and War* seems to be "not really." As Libicki implies, the choice to make cyberspace an insecure tool for infrastructure control was a matter of choosing a bad bed in which we now must lie, while constantly straining to prevent somebody (hackers, opposing governments, and others) from yanking off the covers. That dire scenario makes one want to pull the plug.