Cyberspace in Peace and War

By Martin C. Libicki
Naval Institute Press, 2016
496 pp., $54.98
ISBN-13: 978-1-68247-032-9

Reviewed By Julie Ryan

Martin Libicki has been a prolific writer in the field of information warfare since the mid-1990s. In this newer work, published by the Naval Institute Press, he aggregates his thinking during the past several decades into a single book. *Cyberspace in Peace and War* draws from work performed at RAND, both solely and with colleagues, and from lecture interactions with his students at various universities, to present a streamlined and consolidated overview of activities within and enabled by information technologies.

Before getting to the substance of this review, it is necessary to point out that this is a difficult book to read. *Cyberspace* is, in a word, dense. A naïve reader will likely have to do some additional research to truly understand the discussions and an informed reader will have to overlook stylistic annoyances so as to avoid getting lost in interpretative musings. For example, on page 73, Libicki uses the phrase, "hortatory injunctions." On one hand, the reader must pause to admire the sheer audacity of that phrasing. After, of course, looking up the definition of "hortatory"—tending or aiming to exhort—the phrase appears to be contradictory. An injunction is an order that either restrains desired behavior or compels undesired behavior. An exhortory injunction is a strange beast to contemplate—a command to act that requires additional exhortation? A command to stop action that requires additional exhortation?

Similarly, novice and expert readers alike may take exception to some of the more definitive assertions. For example, Libicki states that, "Controlling the effects of cyberattack entails controlling cyberwarriors." While it can be argued that cyberwarriors should be encouraged to limit the foreseeable effects of activities taken against cyber assets or against key terrain features of cyberspace, the fact is that it is impossible to control the unintended effects, particularly those that cascade, that result from cyberattacks. At the rate at which physical elements, such as light switches, refrigerators, or cars, are being integrated into cyberspace, the problem is going to get worse before it even has the chance to get better. Beyond that, some readers may also take issue with some of the language choices. For example, on page 145 Libicki says that "Originally all cyberattack operations came under the command and control of CYBERCOM." The purist will balk at that assertion, asking the question, "What about the cyberattacks that were performed prior to the creation of CYBERCOM?" After all, CYBERCOM was created in 2009—well after the ubiquity of networked communications systems created the reality of cyberspace. But these issues are distractions from the true value of the text, which lies in its breadth of coverage of cyber activities and thoughtful treatment of sensitive topics, such as equities.

Where *Cyberspace* shines is in its thoughtful treatment of philosophical questions. For example, Libicki invokes a variety of thought exercises to explore the nuances of operating in cyberspace. These include the so-called Las Vegas Rules—what happens in Vegas stays in Vegas—game theory, and effects versus means arguments. Exploring the

Dr. Julie Ryan is the author of Detecting and Combating Malicious Email and Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves. She joined the faculty of the College of Information and Cyberspace at National Defense University in August 2016.

arguments about what constitutes an attack, the functional equivalent of armed attacks, and rights of reprisal, he invokes customary law, norms, and influential publications such as the Tallinn Manual. Herein lies significant value. The reader need not agree with the conclusions to appreciate and benefit from the argument. Indeed, reasonable people do disagree on these issues, which are far from settled. Understanding the nuances of the arguments and the elements that underpin the perspective is a critical step to becoming an informed consumer.

A particularly useful part of *Cyberspace* is Libicki's treatment of deterrence. He explains concepts of deterrence, points of view from different players, and explores how deterrence might work out in different situations. The strategic focus of these discussions lays the groundwork for the reader to truly understand the interpretative reaction to actions taken in cyberspace, which then leads to the ability to make decisions about how different objectives might be achieved. His discussion is grounded in a discussion of law and the rule of law, which is far more important than a reader might imagine prior to indulging in this exploration.

Cyberspace is useful and can be a valuable resource. As noted by one reviewer, Robert Jervis, it is a "one-stop-shopping resource" covering the "range of issues, from the technical to the operational and political." The end notes are particularly useful for researchers, in that they point to contemporary sources as well as other publications that provide useful context and bibliographic grounding. At $55.00 for hard cover and $45.00 for a Kindle edition, *Cyberspace* is not inexpensive, but compared to other books, it is well worth the investment for the interested scholar. PRISM