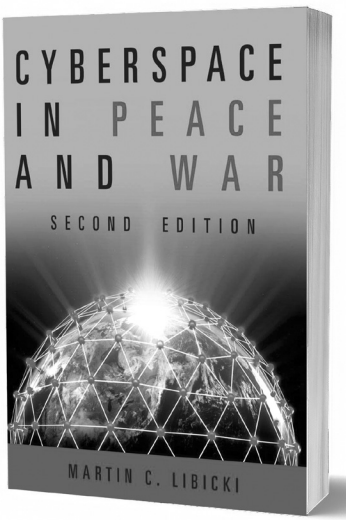
Cyberspace in Peace and War, 2nd Edition

By Martin C. Libicki

Reviewed by
Dr. Mark Grzegorzewski



RECOMMENDATION: Hall of Fame Worthy

EXECUTIVE SUMMARY

Martin Libicki's *Cyberspace in Peace and War* (2nd Edition) is a cyberwar strategy masterpiece. At this point in my career, rarely do I read books that are so impactful. Readers of Libicki's second edition will ultimately understand almost all aspects of deterrence, the shifting thinking on cyberspace-based effects as an element of national power, and whether cyber deterrence is achievable. Most importantly, readers will be treated to a sober assessment of "cyberwar" rather than predictions of an imminent "cyber-9/11." This important difference takes the focus off preventing a single catastrophic event and instead highlights the increasing complexity of executing cyber operations in a world of digital connectivity. Libicki claims this distinction, plus the many actors utilizing cyberspace, causes difficulties in establishing deterrence in and through cyberspace.

The updated edition, which could be used as a textbook, is out of necessity a voluminous work (250,000-words). Libicki attempts to thread the needle between computer science and strategy, two enormous individual topic areas made even more complex by their interplay. In this undertaking, he masters a complex objective, and this book should be read both the IT crowd and by military strategists (due to its non-technical approach, this book is accessible to readers without a tech background). For those, like myself, interested in the overlap of these two topics, this book is pure delight.

Mark Grzegorzewski, Ph.D., is a Resident Senior Fellow in the Department of Strategic Intelligence and Emerging Technology at the Joint Special Operations University, U.S. Special Operations Command. He has recently co-edited and contributed a chapter to a *JSOU Press* edited monograph titled "*Big Data for Generals... and Everyone Else over 40*" and published an article with *Cyber Defense Review* titled "Technology Adoption in Unconventional Warfare." He also recently co-authored a piece in *Lawfare* titled "Taking the Elf Off the Shelf: Why the U.S. Should Consider a Civilian Cyber Defense."

In the first part of the book, Libicki provides the terms of reference for any cyber discussion. By providing this overview, Libicki allows the reader to understand what is possible while not allowing their imagination from wandering into the fantastical. In the second part of the book, Libicki views cyberspace through the national security lens, including military operations, command and control, and espionage. In part three, Libicki focuses on national security strategy, more specifically deterrence. Part III is the largest portion of the book and puts Libicki's systematic approach to strategic thinking on display. In the final section of the book, Libicki brings it all together by discussing how cyberspace-based effects can be integrated into deterrence, while discussing specific deterrence strategies regarding China and Russia.

REVIEW

Cyberspace in Peace and War is broken out into four parts (Foundations, Operations, Strategies, and Norms), which on their own could be standalone books given the level of detail Libicki provides. In part I, Libicki discusses cyberspace foundations, including emblematic attacks; some basic cyber principles; how to compromise a computer; cybersecurity as a systems problem; defending against deep and wide attacks; and deterrence by denial. These sections force the reader to reconsider technology concepts that perhaps had been taken for granted (e.g., the distinction between information and instructions to computers). Cyber planners and students new to the cyberspace literature should read this section to better appreciate limitations and possibilities in cyberspace. What is possible is tempered by the reality of what is permissible, and part one lays out the guardrails on what is technologically feasible, which in turn keeps the discussion on cyber strategy from careening into fanciful ideas of what could be executed in and through cyberspace.

In part II, Libicki addresses operations that include tactical cyberwar; organizing a cyberwar campaign; professionalizing cyberwar; strategic implications of tactical cyberwar; the stability implications of tactical cyberwar; and asks if cyberspace is a warfighting domain. The theme of this section is that cyberwar's effects are overstated, which makes sense when one scrutinizes what is meant by cyberwar. In terms of how the U.S. conceptualizes cyberspace, a cyberspace operation could either deny, degrade, disrupt, or manipulate (D4M) information inside a technological system. Each of these effects are different degrees of interruptions and can be scaled and reversed. Therefore, as more information technology systems are backed up, upgraded/patched, and made more resilient, cyber operations can have lasting effects but the impacts need not necessarily be strategic, nor permanent. This nuanced point often gets lost when thinking through cyberspace operations. Many thinkers become over enchanted with what can be accomplished in and through cyberspace. These remarkable effects are real but also can be reversed with time. Therefore, Libicki concludes that most cyber effects are most effective when paired with kinetic effects.

In part III—the real meat of the book—the author unpacks strategies such as strategic cyberwar; cyberwar threats such as deterrence and compulsion; the unexpected asymmetry of cyberwar; responding to cyberattack; deterrence fundamentals; the will to retaliate; attribution; what threshold for response; a deterministic posture; punishment and holding targets at risk; cyberwar escalation; brandishing cyberwar capabilities; narratives and signals; cyberattack inferences from cyberespionage; and strategic stability. For military strategists and political scientists alike, Libicki leaves no stone unturned when examining deterrence. For those who ask, why not hack back?, Libicki demonstrates how escalation works in cyberspace, and in fact claims that actions in cyberspace are preferable since they do not often lead to real world violence. As Libicki claims, in cyberspace, nation-states are playing by Vegas rules. Put another way, in most cases, what happens in cyberspace stays in cyberspace.

In the concluding portion, part IV, Libicki address norms that include the norms for cyberspace; the rocky road to cyberespionage norms; Sino-US relations and norms in cyberspace; the enigma of Russian behavior in cyberspace; cybersecurity futures; and asks what is cyberwar good for? Aside from the norms discussion, this section may be the weakest part of the book. Nevertheless, it is still a very informative perspective for cyberspace scholar-practitioners. I particularly enjoyed Libicki bringing to the fore that, like the US, both Russia and China are still finding their way in cyberspace. Often, the US sees its adversaries as 10-foot-tall boogeymen who cannot be stopped. In the case of Russia, this impression is often fed by a misreading of the so-called Gerasimov Doctrine. In fact, US adversaries are still testing and learning in cyberspace, and they are just as vulnerable due to their own exposed attack surface. In addition, US adversaries are still developing their own thoughts on how to employ cyber effects, meaning it is a test and learn culture that currently limits the occurrence of

strategic level cyber effects. The good news from the last section of the book, is that the sky is not falling due to US' adversaries use of cyberspace operations. Therefore, we should understand this as welcome news and update our thinking on the impact of cyberspace-based effects.

CONCLUSION

One minor critique I have of Libicki's work is a broader general critique of deterrence theory. Frequently, deterrence theory is broken out into a reductionist formula in which decision makers and organizations act rationally, and policymakers do not have gaps in knowledge. The risk is that someone new to the cyberspace literature will translate this information into a checkbox mentality to "achieve" cyber deterrence. This is not Libicki's purpose. Rather, Libicki takes pains to highlight the uncertainty undergirding deterrence theory. This is demonstrated by the author posing many of his subsections as questions and highlighting the limits of what we can know. The other observation is not as much a critique as a caution to the reader. Given the technical and high-level strategic focus of this book, it must be read very closely. I found myself going back and re-reading several parts of Libicki's work just to make sure I completely understood the argument. This is not due to Libicki's writing style. He does a wonderful job communicating this complex topic. Rather, the reader must make sure to completely absorb Libicki's complex proposals if they are to successfully process the book. That is the accumulative nature of the book, and if readers take the time to fully absorb Libicki's cyber deterrence argument, they will not be disappointed.

Title: ***Cyberspace in Peace and War*** (2nd Edition)
Publisher: Naval Institute Press (2021)
Hardcover: 492 pages
Language: English
ISBN-13: 978-1682470329
Price: $56.44 (Hardcover)
$45.49 (Kindle)