JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

Vol. 16, No. 2, 2025

Bradley Martin

How Drones Fight: How Small Drones Are Revolutionizing Warfare. By Lars Celander. Havertown, PA: Casemate Publishers, 2024. Pp. 208. $24.95 (paperback); $14.95 (ebook).

Cyber Wargaming: Research and Education for Security in a Dangerous Digital World. Edited by Frank L. Smith III, Nina A. Kollars, and Benjamin H. Schecter. Washington, DC: Georgetown University Press, 2023. Pp. 240. $164.95 (hardcover); $54.95 (paperback and ebook).

Author Lars Celander and editors Frank L. Smith III, Nina A. Kollars, and Benjamin H. Schecter compiled two distinct works that both consider the impact of emerging disruptive technologies on battlefields and national security. Both books provide valuable content in a condensed form. However, the book and edited volume take fundamentally different approaches. Lars Celander describes his book as "only about how things actually work, offering no recommendations on policy, acquisition, training, or organizational matters. Suitable conclusions are left to the reader" (p. ix). Celander is a former Swedish military systems engineer with a master of science in physics. In contrast, *Cyber Wargaming* comprises contributors and editors from multiple backgrounds and recognized experts, "whereas many cyber experts do not interact with wargamers, this book brings together innovative voices from across professional military education, civilian agencies, private industry, think tanks, and academia" (p. 3). Editors Frank L. Smith III, Nina A. Kollars, and Benjamin H. Schecter all have current or previous affiliation with the U.S. Naval War College and are recognized experts in the cyber domain.

How Drones Fight is organized into three distinct parts. The first part pres-

Bradley Martin is an intelligence analyst within the U.S. Intelligence Community. His research interests include emerging technologies, structured analytic techniques, and the use of wargaming as an analytic tool. The views expressed in this review are solely those of the author. They do not necessarily reflect the opinions of the organizations for which they work, Marine Corps University, the U.S. Marine Corps, the Department of the Navy, or the U.S. government.

ents an overview of the engineering and technical knowledge associated with drones. The second part examines the current and historical applications of drones in warfare. In the third part, the discussion shifts to the future of drone technology in conflict. Additionally, the book features a preface, glossary, introduction, 16 chapters, three appendices, a bibliography, and an index to provide a comprehensive resource.

The chapters in the book follow a logical progression, beginning with concise technical information. They cover various topics, including types of drones, navigation methods, drone sensors, and communication systems. The second part delves into weapons, drone tactics, antidrone strategies, and combined arms operations. Chapter 7 stands out as a particularly impactful section, where Celander delves into countering drones through the concept of "soft kill" (p. 59). Despite its brevity, spanning only two and a half pages, this chapter effectively tackles essential topics such as disrupting navigation, interfering with communications, and eavesdropping.

In the final one-third of the book, the author effectively connects technical information from earlier chapters to modern situations. Chapter 12 covers the use of drones in the Global War on Terrorism in just seven pages. Chapters 13 and 14 focus on the 2020 Armenia-Azerbaijan conflict and the 2022 Russia-Ukraine conflict, respectively, and are the highlights of the book. Chapter 14 is the longest and features maps, images from both conflicts, insights into command-and-control dynamics, and evolving drone tactics. While the practical applications are a significant strength, the narrative could benefit from more examples. Overall, the content and writing style are accessible, but inconsistencies in chapter length and subheadings may frustrate readers. Some subheadings include only a few sentences, creating a disjointed reading experience.

The bibliography includes sources, but the book lacks traditional citations apart from a few photographs. Celander downplays the necessity of source listings, stating, "Much of what is said in this book is based on various engineering textbooks. They are not listed as sources here as they all say the same thing. Ultimately, everything is just physics" (p. 175). While some photographs mention citations, many diagrams do not have corresponding references. The absence of a thorough conclusion addressing the potential impact of drones on the future of warfare presents the most significant challenge for readers. In the concluding chapter, Celander remarks that "the book is reluctant to draw conclusions. It is not its purpose. The purpose is to provide the reader with an understanding of how drone warfare works; the reader is expected to draw his or her conclusions" (p. 153).

Cyber Wargaming is a unique book; it focuses on cyber wargaming, not on specifics of cyber warfare technical knowledge, "contrary to popular belief, cybersecurity is also about human decision making: not just hardware, software,

network, and data" (p. 2). The authors divide the book into thirds. The book begins with an introduction, followed by the first one-third of the book discussing research games, the second one-third on educational games, and a final conclusion. While *How Drones Fight* builds on each chapter, leading to a disappointing conclusion, *Cyber Wargaming* takes an independent chapter approach. Readers can navigate much easier between chapters and only read chapters they find of interest.

As *Cyber Wargaming* illustrates, wargaming is a technique used for both research and education in a wide variety of environments: "Fortunately, as a general-purpose tool, wargaming is interdisciplinary. When used correctly, cyber wargaming can bridge the gaps between social and technical knowledge in university classrooms, corporate boardrooms, and military headquarters" (p. 3). The editors note in the introduction that, while wargaming is expanding as a technique, most cyber wargames remain shrouded in mystery.

After the introduction, the book's first one-third concentrates on research games or analytical games. Chapter 2 on cyber wargames as synthetic data is an excellent supplement to the introductory chapter. While the introductory chapter explains why cyber wargaming is a valuable technique, chapter 2 provides more information on cyber wargames as a tool to generate data and provides examples of wargames with alternative approaches to generate research data. The chapter concludes by stating, "It is our hope that the library of cyber wargames and the new knowledge they can create will continue to grow" (p. 34). Chapter topics in the book's first one-third include cyber and nuclear crises, wargaming international and domestic crises, imperfect information games, cyber kill chains, and games within games and critical infrastructure.

The most innovative chapter in the book is chapter 5, which discusses the topic of imperfect information in games. Many wargames assume near-perfect information processing and retrieval, which is a flawed method, as the editors explain: "In this chapter, we argue that the role of information—specifically imperfect information and the means to degrade information—is foundational to any realistic wargame. Imperfect information has always been important to real life" (p. 67). Specifically, in a wargame, the authors used videoconferencing, voice chat, text messaging, and maps, and those capabilities could be degraded based on various cyber or kinetic actions.

The second one-third of *Cyber Wargaming* focuses on educational wargames. It covers topics such as creating enjoyable cybersecurity games, the Cyber 9/12 Strategy Challenge, the North American Electric Reliability Corporation Grid Security Exercise (GridEx), private sector cyber wargames, prototyping virtual cyber wargames, military doctrine, and using matrix games for strategic cyber and information warfare.[1] This section offers numerous examples of lessons learned from various cyber wargames. It includes several graphics de-

picting mock gameboards, cards, and capabilities. The standout chapters in this part are chapter 13, which discusses military doctrine and cyber gameplay and chapter 14, which explores matrix-style games for strategic cyber and information warfare. In chapter 13, Colonel Benjamin C. Leitzel from the U.S. Army War College designed a cyber wargame to help students grasp cyber concepts. He notes that "even for officers who are familiar with the domain, this type of game can encourage creative and critical thinking about the strengths and weaknesses of current doctrine—doctrine they may one day help to update and improve" (p. 188). Chapter 14 highlights the wargame *Pinnacle Protagonist*, a capstone project from the National Defense University. The authors developed an adjudication tool called the National Strategic Program (NSP) framework to enhance cyber wargaming. Based on commercial board game designs, the NSP incentivized players to think carefully about their cyber capabilities. It required players to prepare specific courses of action in advance and limited their resources during gameplay, creating an atmosphere of uncertainty and anonymity (p. 200).

The final concluding chapter of *Cyber Wargaming* discusses the insights gained by using cyber wargames to spur thinking about emerging technology and innovation: "wargames that explore emerging technologies have the potential to influence not only our understanding of these technologies but also their subsequent development and application" (p. 211). To put it directly, "wargaming emerging technologies can affect technological innovation" (p. 212). The chapter concludes with a call for more wargames: "reading a book about riding bicycles is one thing, but riding a bike yourself is a very different experience. More practice playing wargames is good, regardless of your experience and expertise. This is true now, and we suspect the same for wargaming in the future" (p. 213).

Both books contribute to readers' understanding of emerging technologies that will likely remain important to the national security community during future conflicts across the conflict continuum. In summary, Lars Celander's book, *How Drones Fight*, is an excellent practical, tactical overview of drones on the battlefield. Analysts and researchers looking for a deep treatise on drones or those familiar with the technical exploitation of drones will find the information too basic. Readers will likely appreciate the concise nature, making it an excellent desk reference for nonengineers or scientists. This book is recommend as an introductory guide for intelligence and military personnel new to working drones. *Cyber Wargaming* is a different and more scholarly anthology. It is an excellent guide for those interested in wargaming, building, and designing cyber wargames and for scholars researching cyber concepts. The content targets individuals interested in wargaming and is more of a niche advanced text.

Endnote

1. "Cyber 9/12 Strategy Challenge," Atlantic Council, accessed 18 November 2025; and "GridEx," North American Electric Reliability Corporation, accessed 18 November 2025.