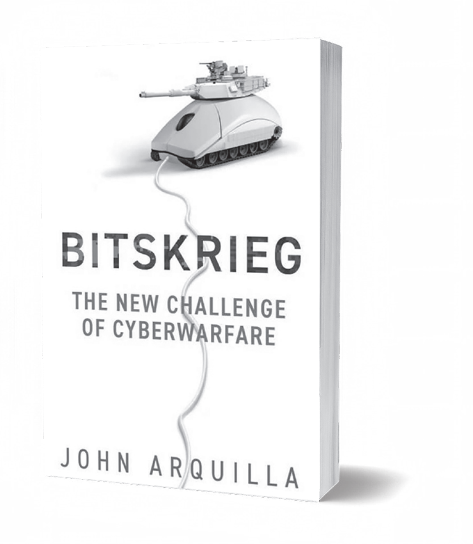
Bitskrieg: The New Challenge of Cyberwarfare

By John Arquilla

Reviewed by
Major Mathieu Couillard



EXECUTIVE SUMMARY

In the 1990s, John Arquilla and David Ronfeldt co-authored an influential series of articles in which they developed the concepts of cyberwar, swarming tactics, and netwar. Drawing on historical analogies that predate the information age, he articulated how information dominance would critically enable future warfare. Today, some senior leaders herald this concept as the centerpiece to strategic success. In Bitskrieg, the professor emeritus at the U.S. Naval Postgraduate School once again draws from history to envision the evolution of conflict. He possesses rich experience to complement it, as he has had fortune to witness and influence US strategic decision-making for the last three decades. In his book, Arquilla provides strategic context for ongoing efforts to increase the use of cloud computing and strong encryption, and articulates a new approach to cyber arms control agreements. His work is insightful to practitioners and leaders throughout the cyber domain.

REVIEW

The memorable title of the book is an obvious reference to the devastating armored breakthrough tactics employed by Germany at the onset of World War II—and, more optimistically, to the allies' ability to defeat this strategy over time. Arquilla laments that the United States has thus far failed to adapt to the cyber threat, allowing freedom

Major Mathieu Couillard is a Signals Officer in the Canadian Armed Forces. He has served with conventional and special operations forces in network and cyber operations leadership roles. Major Couillard holds a bachelor's degree in computer engineering and is currently a student at the U.S. Naval Postgraduate School in the Defense Analysis Department. His research will focus on the role of deception in cyber strategy.

of action in cyberspace to rival powers such as China and Russia, and even to lesser nations such as North Korea—described as a "strategic criminal." Bitskrieg goes beyond the cyber domain; it is an appeal for a paradigm shift from a centralized "few large" approach (i.e., Blitzkrieg) to a decentralized "many small" swarm, which heavily relies on information dominance. Arquilla suggests this can be achieved through technological, doctrinal, and organizational reform. He smoothly transitions between relevant historical analogies and firsthand accounts, notably of the Gulf War, to illustrate this concept.

Building on the title's World War II analogy, Arquilla compares traditional perimeter-based cyber defense to the catastrophically ineffective Maginot Line. Arquilla invites the reader to "imagine no lines," and assume the inevitable breach of perimeter defenses. He recommends the employment of strong encryption in depth, which is well underway with the ubiquity of Hypertext Transfer Protocol Secure (HTTPS) and rapid adoption of Zero Trust. He also promotes use of the cloud and data mobility, stating that "data at rest are data at risk." This is valid for the majority of organizations (including within the military), which benefit from the enhanced availability, data center security, monitoring, and up-to-date baselines that the cloud provides. However, there are attack strategies that specifically target data in transit, and cloud providers are not immune to breaches or subversion. Hence, one must carefully weigh the risks and benefits of the cloud relative to closed, on-premises networks for their most valuable data. Nonetheless, decision-makers must urgently adopt Arquilla's overall recommendation to evolve from perimeter defense to defense-in-depth.

In addition to deepening defenses, Arquilla argues that cyber arms control agreements could lead to greater stability in the cyber domain. He recognizes that most observers assume these efforts to be futile; the attribution problem in cyberspace and the “dual use” of information technology (i.e., the challenge in distinguishing offensive and defensive cyber capabilities) have long hindered such treaties. Instead of “structured arms control,” where cyber weapons would be inventoried like nuclear warheads, Arquilla suggests a behavioral approach. In this logic, agreements would focus on limiting attacks against certain targets (e.g., civilian infrastructure) rather than banning a certain type or quantity of cyber weapons. In a fascinating passage, many will be surprised to discover that Russia once proposed such agreements to the US. Indeed, Arquilla led a delegation to a summit where top Russian cyber officials made just such an overture which was promptly rejected by US decision-makers. These leaders presumably assumed that cyber superiority would guarantee protection, just as previous superiority in other domains; unfortunately, this assumption has resoundingly been proven wrong. Today, Russia is a declining power by nearly all metrics but continues to project power effectively through cyber attacks and information warfare. As all societies are increasingly dependent on the Internet and leaders become aware of its incongruent reflection of power, a solution must be found to better manage cyber conflict. One can only hope that Arquilla’s recommendations will lead down a fruitful path.

CONCLUSION

Ultimately, Bitskrieg is a quick and enlightening read that will satisfy both technically and policy-focused readers. Arquilla convincingly not only predicts how warfare will be waged but also how to defend against it. The pervasiveness of cloud deployments and strong encryption is empirical evidence that supports Arquilla's thesis but also suggests they may not be useful to practitioners who have already arrived at the same conclusion. However, there is still much progress to be made in these areas, and Arquilla’s narrative can help the technical community explain the imperatives in strategic terms that can be understood by policymakers.

Title: ***Bitskrieg: The New Challenge of Cyberwarfare***
Publisher: Polity
Paperback: 240 pages
Language: English
ISBN-13: 978-1-509-54363-2
EISBN: 978-1-509-54364-9
Price: $22.95 (Paperback)
Price: $64.95 (Hardcover)
Price: $14.00 Kindle edition

NOTES

1. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *in In Athena's Camp: Preparing for Conflict in the Information Age* (RAND Corporation, 1992), https://www.rand.org/pubs/reprints/RP223.html; John Arquilla and David Ronfeldt, "The Advent Of Netwar" (RAND Corporation, January 1, 1996), https://www.rand.org/pubs/monograph_reports/MR789.html; and John Arquilla and David Ronfeldt, "Swarming and the Future of Conflict" (RAND Corporation, January 1, 2000), https://www.rand.org/pubs/documented_briefings/DB311.html.
2. John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review* 22 (1994): 22-34.
3. Riad Kahwaji, "'The Future Is About Information Dominance': Gen. Nakasone," *Breaking Defense* (blog), June 29, 2021, https://breakingdefense.sites.breakingmedia.com/2021/06/the-future-is-about-information-dominance-gen-nakasone/.
4. John Arquilla, *Bitskrieg: The New Challenge of Cyberwarfare*, 1st edition (Polity, 2021), xix.
5. Arquilla, xvi.
6. Arquilla, 79.
7. Arquilla served as a member of an advisory team to U.S. Army General Norman Schwarzkopf from August 1990 to February 1991. See Arquilla, 15.
8. Arquilla, 43.
9. According to a report from Microsoft Security, Zero Trust is critical to 96 percent of security decision-makers, with 76 percent of organizations having at least started its implementation. However, only 35 percent of the organizations polled have completed their implementation. See Microsoft Security, "Zero Trust Adoption Report," July 2021, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha.
10. Arquilla, *Bitskrieg*, 45.
11. Bruce Schneier and Herr Trey, "Russia's Hacking Success Shows How Vulnerable the Cloud Is," *Foreign Policy* (blog), accessed October 26, 2021, https://foreignpolicy.com/2021/05/24/cybersecurity-cyberattack-russia-hackers-cloud-sunburst-microsoft-office-365-data-leak/.
12. For example, the US and China signed an agreement in 2015 but routinely accuse each other of violations, which the other party denies by leveraging the ambiguity of the cyber domain. See Emily Feng, "The White House Blamed China for Hacking Microsoft. China Is Pointing Fingers Back," *NPR*, July 20, 2021, sec. National Security, https://www.npr.org/2021/07/20/1018283149/china-blames-united-states-for-cyberattacks.
13. Arquilla, *Bitskrieg,* 110.
14. Arquilla, 105-6.
15. The Solar Winds Attack is the most recent example of Russian might in cyberspace. See David E. Sanger, Nicole Perlroth, and Julian E. Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm," *The New York Times,* January 2, 2021, sec. U.S., https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.