H-Net Reviews
in the Humanities & Social Sciences

Herbert Lin, Amy B. Zegart, eds. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.* Washington, DC: Brookings Instutition Press, 2019. 438 pp. $45.99, paper, ISBN 978-0-8157-3547-2.

Reviewed by Nicholas Sambaluk (Air University)

Published on H-War (July, 2020)

Commissioned by Margaret Sankey (Air University)

The book, published by the Brookings Institution and edited by Hoover Institute scholars Herbert Lin and Amy Zegart, reflects effort to focus different perspectives on the crucial subject of cyber operations. In particular, the book, which evolved from a research workshop in early 2016 dealing with the strategic use of offensive cyber operations, aims to bring balance to discourse its creators feel has heretofore been fixated on the problems on cyber defense and neglected the impact and implications of the offensive side of the equation. Classification of capabilities contributed to a chronic dearth of information or serious strategic considerations about cyber offense. *Bytes, Bombs, and Spies* thus represents a notable contribution to the literature.

Because the book aims to address the absence of strategic thinking, its theme deals more with the subject of strategic perspectives than with a unified perspective. The book reflects a discussion more than a single idea; as such, its organization as an edited volume appropriately sets the stage for further study, and its contributors encompass many of the key figures in cybersecurity scholarship.

The various chapters include a number of interesting observations. For example, a multinational accord about norms of behavior in cyberspace will likely either be impossible to achieve or become watered down to the point that democratic and nondemocratic regimes would ascribe very different meanings to the same words. Martin Libicki notes that cyberattacks can be used specifically to direct defenders into undertaking adjustments that carry counterproductive costs, such as expensive repairs or inefficient changes to working procedures or even deteriorating a defender's trust for its partners. As he notes, "the best adjustments are known to create problems of their own" (p. 141). Steven Bellovin, Susan Lanau, and Herbert Lin explain that although cyberweapons "are not inherently indiscriminate," the intelligence and developmental investments needed for an effective and controllable cyberattack can exceed the costs of an alternative weapon (p. 284).

The chapters also include some insightful but potentially provocative assertions. Lin distinguishes between the opportunities and contexts of cyberattacks against a developmental technology on one hand and a deployed technology in combat on the other, since in the developmental case the technology will be of unconfirmed reliability and subject to testing and therefore associated with controls and monitors—all of which represent avenues for potential manipulation which can potentially even be misattributed to a range of entirely different technical problems in development. Erik Gartzke and Jon Lindsay point to the need for education of strategic and policy decision-makers, noting that war games suggest that escalation from cyber to kinetic conflict can otherwise occur swiftly. Jason Healey challenges assertions that cyber capabilities lead to deterrence, finding instead that in *most* historical cases the deployment of cyber capabilities triggered an escalatory response.

Lin points out powerfully that “cyber weapons are not magical tools that can be deployed at will and used with certain effect,” partly because of the extensive intelligence requirements on which sophisticated cyberattacks are predicated. Although cyberattacks “can also buy time for policymakers who are faced with the need for immediate action, … the utility of a deferral strategy depends on taking policy actions in the time thereby made available” (p. 168). This important point, almost buried in the middle of the four-hundred-page volume, suggests how much a proper conclusion would have sharpened this valuable work. It speaks to the need for the public and especially policymakers to appreciate that cyberweapons are not magic bullets; the cyber realm does not overturn but instead interacts with the existing factors that inform security considerations. This is a key point that links to the rationale for creating the book.

Bytes, Bombs, and Spies closes with three chapters that engage with the role of states and nonstates in struggle within the cyber realm. A consensus of sorts emerges regarding the need for further study of the impact of nonstate entities (for example, as proxies or cybersecurity firms) in providing capabilities while changing risks connected to factors like escalation and challenges in attribution. As intended, the book opens rather than closes an important area of scholarly debate.

If there is additional discussion of this review, you may access it through the network, at
https://networks.h-net.org/h-war

Citation: Nicholas Sambaluk. Review of Lin, Herbert; Zegart, Amy B., eds. ***Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.*** H-War, H-Net Reviews. July, 2020.

URL: https://www.h-net.org/reviews/showrev.php?id=54759