H-Net Reviews
in the Humanities & Social Sciences

Fritz Allhoff, Adam Henschke, Bradley Jay Strawser, eds. *Binary Bullets: The Ethics of Cyberwarfare.* New York: Oxford University Press, 2016. 316 pp. $29.95 (paper), ISBN 978-0-19-022108-9; $99.00 (cloth), ISBN 978-0-19-022107-2.

Reviewed by Nicholas Sambaluk (Air University)

Published on H-War (July, 2016)

Commissioned by Margaret Sankey (Air War College)

Binary Bullets is an engaging collection of essays on ethics involved in cyberwarfare. Rather than a shared thesis, divergent voices and opinions advance the debate regarding the character and impact of conflict in the cyber realm. International relations scholar John Arquilla, a pioneering voice in identifying the contours of struggle in cyberspace, writes the foreword, and the bookâs twelve chapters are written mostly by ethics, law, and philosophy scholars from the United States, Israel, and Australia. One scholar each comes from Canada and the United Kingdom, and another is an information security scientist for the law and policy arm of the cyber defense training center of the North Atlantic Treaty Organization (NATO). Despite their generally shared fields of study and in some cases overlapping backgrounds (five of the twelve do or have taught at national military academies), these scholars present an array of ideas and conclusions about an important and emerging topic.

The authors helpfully explain terms to an audience that will include readers with education and background in other areas but not necessarily in cyber struggle. By page 3, an easily accessible footnote explains that âthe concepts themselves are still very much ill-defined and highly contentiousâ and therefore common agreement upon definitions of terms as seemingly basic as âcyberwarfareâ or âcyberattackâ is problematically elusive. Other footnotes in later chapters provide concise and accurate definitions of terms, including âlogic bombs,â âworms,â âkeystroke logging,â and âhoneypotâ (p. 211). In a similar vein, war ethics terminology such as *jus in bello* or proper ways of fighting are straightforwardly distinguished from *jus ad bellum*, regarding the time at which an entity can resort to force. Providing straightforward definitions is of particular value when addressing topics in controversial areas of potentially multidisciplinary interest.

To date, sinister activities in the cyber realm have overwhelmingly involved espionage rather than violence; furthermore, those instances wherein authors can point to physical damage or destruction, such as the damage caused by the Stuxnet virus that targeted Iranian nuclear production systems, has been limited to nonlethal damage. This leads George R. Lucas in the first chapter to ask whether this has an impact on decisions about the threshold for justifying preventive war. Ryan Jenkins suggests that âcyberwarfare has made possible … an ideal war … wherein civilian casualties were minimal or nonexistentâ (p. 89). Jenkins also discretely concedes that, depending on the choice of targets and means of execution, âa cyberattack could be *at least as bad* as any

conventional attack, and even any nonconventional attackâ and that the outcome would rely on âthe willingness and ability of states with powerful cybercapabilities to deploy cyberweapons in ways that are proportionate and discriminatoryâ (pp. 105, 111). Unfortunately, most chapters making such implications do not engage with military history that includes important examples of belligerents opting either at the outset or in the midst of conflict to recalibrate their policies and definitions of proportionality and target discrimination. David Whethamâs chapter, however, leverages an intriguing historical analog to challenge the famous assertion by Thomas Rid that cyberwar will not occur.

Cyberwarfare is a complex topic, and arguments abound within the volume itself. Matthew Beard contends that although sinister actions in cyber âwill not always be perfectly clean,â efforts should and implicitly can be taken to establish cyberwar as being âa near-bloodless mode of warfareâ (pp. 154-155). Heather Roff notes that although hostile cyber activity will probably seek to destroy industrially important facilities rather than directly target civilians, âcyberweapons are difficult to control once releasedâ (p. 221). For Roff, therefore, it is important ânot [to] be overly accepting of cyberoperationsâ (p. 224). Given the topic, the debates between contributing authors are both interesting and valuable, providing an opportunity for readers to explore a complex issue from multiple vantage points. The final chapter, offered by Michael Skerker, presciently anticipates that privacy concerns will prompt the US federal government to adopt policies by which it accesses data collected by telecommunications companies, rather than directly collecting and storing the data itself. Skerker, like many others, does little to persuasively show that this protects data either from unauthorized use by repository entities or makes it safer from exploitation by hackers.

One of the few places in which the book could have been materially improved is by providing a conclusion chapter. The contested topics throughout the book and the cacophony of voices are constructive, but a coherent summation of the arguments and issues at hand would have rounded out the volume more effectively. *Binary Bullets* would thus do well to include a conclusion chapter in a future release, particularly if the book were to appear in a second edition when intervening events will have provided further examples for consideration. Nevertheless, *Binary Bullets* is interesting to read and represents a valuable frame of reference for ethics perspectives based on the current character of hostile efforts in the cyber realm.