The US Army War College Quarterly: Parameters

Manuscript 3192

Hacking the Bomb and Cyber Threats and Nuclear Weapons

Jeffrey Caton

Review Essay

Hacking the Bomb: Cyber Threats and Nuclear Weapons

by Andrew Futter

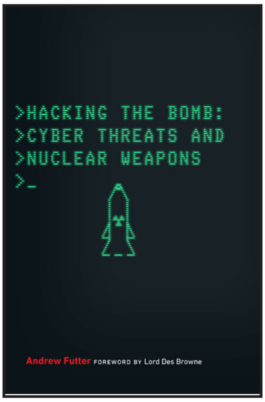
Washington, DC: Georgetown University Press, 2018
212 pages
$29.95

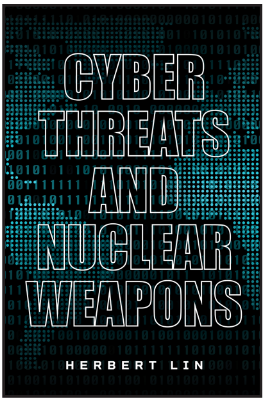
Cyber Threats and Nuclear Weapons

by Herbert Lin

Stanford, CA: Stanford University Press, 2021
216 pages
$25.00

Reviewed by Jeffrey Caton, colonel, US Air Force (retired),
president, Kepler Strategies LLC





Andrew Futter and Herbert Lin have written recent and similarly titled books—which, for clarity, I will refer to as *Hacking the Bomb* and *Cyber Threats and Nuclear Weapons*, respectively—aimed at helping senior government policymakers confront the complex interactions between modern cyberspace operations and nuclear operations. The outstanding sources both authors identify reflect their seriousness and credibility as researchers. But—remarkably—their books are tepid in content and offer little new information for the cyber-nuclear dialogue.

Andrew Futter, a professor of international politics at the University of Leicester, has published an impressive list of publications on nuclear weapons, missile defense, and cyberspace. In *Hacking the Bomb*, he aims "to assess, examine, and explore what this new global [cyber-nuclear] context means" for nuclear weapons, forces, and strategy (4). He posits this task is based on two dynamics: increasing use of information technology in nuclear weapons management and emerging new cyber capabilities. He organizes his treatise into four parts addressing the nature of the cyber-nuclear challenge, what hackers might do to nuclear systems, the cyber-nuclear nexus at the strategic level, and challenges for the cyber-nuclear future.

Part I of *Hacking the Bomb* begins with an abridged historical contextualization of the "cyber challenge," as Futter calls it, "involving four different domains of analysis: physical/mechanical, logical, informational, and human/cognitive" (23). Futter rails against the imprecise language that clouds ongoing cyber debate, but he uses imprecise and inconsistent terminology. With his context established, Futter explores the vulnerabilities of nuclear systems and their implications for the goal of ensuring weapons are always available when properly initiated but never available to unauthorized users. He emphasizes the increasing complexity of such command-and-control processes and suggests "a key part of the cyber challenge for nuclear systems security will be intrinsic, and not involve any attackers at all"—that is, normal accidents may be more likely to occur (45).

Part II opens with a concise summary of information breaches at the Departments of Defense and Energy with implications for nuclear weapon development. He surmises the cyber-espionage threat "probably represents more than 90 percent of the cyber challenge that we currently face in the nuclear realm" (69). Such statements are indicative of Futter's cavalier prioritization within his analysis that undermines the credibility of his synthesis. After all, are readers to believe the other material in this book addresses less than 10 percent of the cyber challenge? The remaining chapter of Part II explores how cyberattacks could lead to the unauthorized use of nuclear weapons or the disruption of authorized use. It largely rehashes well-known historical cases of cyberattack of nonnuclear systems and includes another account of Stuxnet.

Part III focuses on the strategic level of nuclear weapons and cyber deterrence with a discussion marred by simplifications and debatable assertions. Futter reveals his implicit bias of viewing cyber operations in Clausewitzian terms while treating nuclear operations as Jominian. To wit, Futter declares, "though we have come to understand just how powerful and destructive nuclear weapons are during the past seventy years, the same cannot yet be said for the diverse range of threats posed by the much newer cyber challenge" (95). Unlike atomic bombs, thermonuclear weapons have never been used in combat. Thus, while the immediate effects of nuclear warheads may be characterized by tests and analyses, the strategic effects of actual nuclear conflict remain unknown. To his credit, Futter raises the topic of a US declaratory nuclear policy with regard to potential aggression in cyberspace, citing the foundational 2011 International Strategy for Cyberspace. Yet, his narrative on how cyber operations may affect nuclear escalation is an unbalanced collage of existing issues surrounding an emerging "cyber-nuclear security dilemma"—a term he fails to define (119). Fixed on the negative implications of cyberspace, he fails to consider how information provided through cyberspace may enhance lucid decision making.

In Part IV, Futter examines nuclear weapon modernization and advanced conventional weapons through the lens of technological determinism where "technology drives social and societal change" (132). He tackles this broad topic by describing potential military capabilities with vague cyber-nuclear connections. The chapter concludes with unfounded speculation about a potential revolution in nuclear affairs and the third nuclear age. *Hacking the Bomb* ends with a whimper, its final chapter laden with adages and conjecture about the cyber-nuclear future. Despite his preceding insights, Futter can muster only three trifling recommendations: develop a consensus on what the term *cyber* means; protect nuclear systems against direct cyberattacks; and include cyber operations in other emerging strategic dynamics, such as nuclear arms control.

Hacking the Bomb promises a fecund discussion with a propitious opportunity to expand the dialogue surrounding the strategic use of cyber and nuclear capabilities. But its delivery is often repetitive and wordy with a diluted sense of priority in analysis—Futter identifies too many issues as *the* central concern. Certainly, much serious work went into the research of the book—to which its impressive, well-documented array of authoritative references attest. But its lack of a congruent lexicon or balanced analyses facilitates an ambiguous and unilateral discussion neither favorable to educate novices nor to inform serious decisionmakers.

Herbert Lin holds research positions at Stanford University's Center for International Security and Cooperation and Hoover Institution. A recognized expert on policy-related aspects of cybersecurity with a list of publications on par with Futter, Lin has little discernable experience with nuclear weapons. His version of *Cyber Threats and Nuclear Weapons* walks readers through background material and cyber-nuclear context, cybersecurity lessons for nuclear modernization, nuclear scenarios with cyber risks, and imperatives for the future. His target audience is White House and congressional policymakers who will influence the next *Nuclear Posture Review*. Lin claims "[t]his book addresses the relationship to and possible impact of cyber technology on all aspects on U.S. nuclear forces and operations" (ix). With this statement, Lin establishes a vast—but ultimately unachieved—scope of effort.

The first two chapters of the book provide very basic information on cyberspace and nuclear operations. Although the use of artificial intelligence is increasing in many cyberspace applications, Lin wisely defers any related discussions to other venues. While he notes the *2018 Nuclear Posture Review* includes strategically significant language "to indicate that the United States might contemplate a nuclear response to certain kinds of cyber attack" he explicitly decides not to address it in the book (27). His examples of cyberattacks—such as those on Sony Pictures, the Office of Personnel Management, and US election media sites—have no direct connection to nuclear operations.

While Lin's third chapter on the US nuclear enterprise is the longest chapter, it is far from comprehensive. Its content reveals Lin's forte is cyberspace, and that his aptitude for strategic nuclear affairs is questionable. A major portion of the chapter rehashes a 2019 report by the US Government Accountability Office that explored cyber vulnerabilities for weapon systems. Inexplicably, Lin completely ignores the 2019 version of Joint Publication 3-72, *Nuclear Operations*—a document that should be mandatory for anyone exploring an authoritative model of the nuclear enterprise.

The fourth chapter, "Cybersecurity Lessons for Nuclear Modernization," is short and forgettable. Its content has little direct relevance to anything nuclear, with only examples of mundane issues, such as physical security, Internet service outages, and supply chain vulnerabilities. The next chapter presents six scenarios designed to highlight cyber risks in nuclear crises, the first four of which are predictable and basic. The other two scenarios do not involve direct cyberattack on nuclear systems but deal instead with the use of social media to influence decisionmakers. Unfortunately, Lin does not discuss the concepts of information warfare and strategic communication that would contextualize such indirect attacks facilitated by means of cyberspace.

The sixth chapter is the book's intended core contribution to the cyber-nuclear dialogue and offers six observations and eight imperatives. None of the observations are original, and most involve cyber risks applicable to all modern weapons systems. The fourth observation, "[t]he legacy NC3 [nuclear command, control, and communications] has not failed catastrophically since 1985," is notable in that Lin neglects to give readers any clue as to what happened in 1985 (134). The companion eight imperatives are equally unremarkable—neither new nor unique to the nuclear enterprise. Like Futter, Lin's final chapter attempts to convince readers that the book provides a novel way ahead for decisionmakers to address cybersecurity in ongoing nuclear modernization efforts.

The back cover of *Cyber Threats and Nuclear Weapons* declares the work is "the first book to consider cyber risks across the entire nuclear enterprise." Clearly, this claim is erroneous, considering Lin cites Futter's *Hacking the Bomb* and fails to address significant portions of the nuclear enterprise. Like Futter, Lin often repeats himself and does not apply consistent terms and logic in his analysis. In fact, the unique and topical material in Lin's tome likely could be reduced to the length of a *Parameters* article. Such a concise and focused piece might better draw the attention of busy staffers in any presidential administration.

Both books suffer from at least three fatal flaws: scope, context, and military operations. First, Futter and Lin opt to tackle a research scope far too broad for a single book. The lack of systematic approaches for their analyses as well as blurring of the tactical, operational, and strategic aspects of both cyber and nuclear operations further hamper their work. In each book, nuclear war theory is simplified as a consensus dialogue vice a nuanced and evolving debate, though, to be fair, any detailed discussion of cyber or nuclear operations quickly enters the realm of classified information.

One could reduce the book's shared central themes to: cyber operations are dangerous; nuclear operations are dangerous; and mixing cyber and nuclear operations makes both more dangerous. Yet, neither author clearly defines the term *cyber threat* nor even *risk*. They do not consider the customary model of military risk as a function of the consequences for a given event and the probability of its occurrence. Including such context would help the authors add sorely needed objective priority to their musings. Finally, like the *2018 Nuclear Posture Review*, Futter and Lin claim to consider the global environment of US nuclear weapons but provide only cursory treatment of other nuclear powers.

For military operations, neither book mentions the evolving mission of US Strategic Command, which, in addition to its current missions of nuclear strike and integrated missile defense, was the birthplace of US Cyber Command. Futter and Lin foster the latent impression that military nuclear planners are unaware of the challenges and complexities hawked in their books—a great disservice to those leaders who made the current multibillion-dollar upgrade of the nuclear enterprise possible.

In summary, Futter and Lin do not fulfill their self-assigned goals. Both books are too convoluted for casual readers and too imprecise for an informed audience. Of the two works, *Hacking the Bomb* is the better by far. Prospective readers would do well to read the last chapter of either book first to decide if the authors' destinations are worth the arduous journeys through their prose.