H-Diplo | ISSF

Review Essay 43

Andrew Futter. *Hacking the Bomb: Cyber Threats and Nuclear Weapons.* Washington, D.C.: Georgetown University Press, 2018. ISBN: 9781626165649 (hardcover, $89.95); 9781626165656 (paperback, $29.95).

Reviewed by **Jacquelyn Schneider**, U.S. Naval War College.[1]

Published **11 October 2018** | issforum.org

Editor: **Diane Labrosse**
Web and Production Editor: **George Fujii**

Shortlink: http://tiny.cc/ISSF-RE43
Permalink: https://issforum.org/essays/43-hacking-bomb
PDF URL: https://issforum.org/ISSF/PDF/RE43.pdf

Hacking the Bomb begins its narrative with *WarGames*—a 1980s sci-fi movie about a teenager who inadvertently almost starts nuclear war by hacking into a nuclear control program within a U.S. computer. This is a common vignette within the cyber literature (see, for example, the introductions of Fred Kaplan's *Dark Territory*[2] as well as "Thermonuclear War"[3]) and it represents what most scholars believe is the most dangerous potential implication of cyber operations—the cyber threat to nuclear command, control, and communications (NC3). As Erik Gartzke and Jon Lindsay conclude, "offensive cyber operations against NC3 raise the risk of nuclear war . . . today the proliferation and modernization of nuclear weapons may raise the risk slightly. Subversion of NC3 raises the danger of nuclear war slightly more. Cyberwar is not war per se, but in rare circumstances it may make escalation to thermonuclear war more likely."[4]

The potential of a cyber-nuclear threat becomes even more pressing as states move to digitize the technologies within their nuclear arsenal. The United States, for example, is currently in the midst of a major nuclear modernization effort prompted by a damning finding from the Government Accountability Office that "Defense is still using 8-inch floppy disks in a legacy system that coordinates the operational functions of the

[1] The views reflect those of the author's alone and do not represent those of the Naval War College, U.S. Navy, or the Department of Defense.

[2] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2016).

[3] Erik Gartzke and Jon Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3:1 (2017): 45.

[4] Gartzke and Lindsay, 45.

United States' nuclear forces."[5] In response, Strategic Command has prioritized the digitization of NC3, arguing to Congress that "any delay, deferment, or cancellation of NC3 modernization will create a capability gap potentially degrading the President's ability to respond appropriately to a strategic threat."[6] Further, recent Department of Defense cloud computing initiatives suggest that the U.S. might go so far as to store nuclear information in contractor-provided cloud computing services.[7] The bottom line is that modern nuclear arsenals are becoming more and more entangled with cyber infrastructure. Clearly Andrew Futter's *Hacking the Bomb* introduces an important puzzle at an extremely relevant time.

The book also has the potential to be a significant contribution to our limited understanding of the impact of cyber operations on nuclear stability. The literature on cyber deterrence, cyber escalation, and cyber war has proliferated over the last five to ten years. Early leaders such as Martin Libicki, Jason Healey, Fred Kaplan, Lucas Kello, Thomas Rid, and Herb Lin have laid a strong foundation of cyber puzzles and their books have generated a rich set of hypotheses about the implication of cyber operations on broader crisis stability.[8]

In order for books to be judged contributions to this now burgeoning field, works must move past this rich foundation of hypotheses and instead build knowledge and fill in theoretical gaps. Despite the increase in attention to cyber threats, authors have been so far unable to answer the fundamental question of international relations—do cyber operations increase or decrease the chance for war? In order to answer this pivotal question, the cyber field benefits from work that 1) characterizes the technical nature of the threat (i.e. can cyber operations pull off these kinds of attacks?), 2) provides empirical data on use of or response to cyber operations—especially about sensitive exploitation or attack planning, or 3) generates testable theories with clear independent variables, dependent variables, and causal mechanisms. While the framing of a cyber-nuclear puzzle is compelling, in order for the study to be a significant contribution it should either present new technical knowledge about the feasibility of impactful cyber attacks, new empirical data about the propensity for the use of or reaction to cyber operations against nuclear targets, or new theories about cyber operations and nuclear stability with clear logics and falsifiable hypotheses. Any one of these contributions

[5] GAO, *Information Technology, Federal Agencies Need to Address Aging Legacy Systems* (Washington, D.C.: 2016), https://www.gao.gov/assets/680/677436.pdf, 26.

[6] House Committee on Armed Services, *Statement of John E. Hyten Commander United States Strategic Command Before the House Committee on Armed Services* (Washington, D.C.: 8 March 2017), https://docs.house.gov/meetings/AS/AS00/20170308/105640/HHRG-115-AS00-Wstate-HytenUSAFJ-20170308.pdf, 6.

[7] Jacquelyn Schneider, "JEDI: Outlook for Stability Uncertain as Pentagon Migrates to the Cloud," *Bulletin of the Atomic Scientists,* 21 June 2018, https://thebulletin.org/jedi-outlook-stability-uncertain-pentagon-migrates-cloud11927.

[8] Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: Rand Corporation, 2009); Herbert Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law and Policy* 4:63 (2010): 63-75; Jason Healey and Karl Grindal, eds., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington, D.C.: Cyber Conflict Studies Association, 2013); Kaplan, *Dark Territory*, Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017); Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013).

could help us answer whether cyber operations increase, decrease, or have no effect on the chance for nuclear war.

Unfortunately, *Hacking the Bomb* is in the vein of much of the existing cyber literature and the ultimate question about nuclear war is left unresolved. It is primarily an exploratory presentation of various cyber-nuclear challenges with an articulation of debates within policy and popular discussion. It does not present new empirics on the use of cyber operations and relies on a limited amount of secondary sources for its analysis. It does, however, have the potential to generate new theoretical perspectives. Perhaps the most useful contribution of the book comes from Futter's typology of nuclear control in chapter 2. Here, Futter illustrates potential cyber vulnerabilities through the lens of two categorizations taken from the nuclear theory world: the vulnerabilities that incentivize negative control, or unwarranted use, and vulnerabilities that incentivize positive control, or first strike incentives. This is a useful frame and a good way to incorporate the very mature theories of nuclear use with our very immature understandings of the implications of cyber operations. Unfortunately, because the book is primarily an exploration and not an argument, Futter does not carry this frame beyond the chapter.

Hacking the Bomb might not solve the primary limitations of current cyber literature, but it does highlight the fertile landscape for future cyber work. In particular, the book suggests the need for three types of follow-on work. First, the lack of primary source knowledge about the technical feasibility of cyber attacks on NC3 severely limits the ability to generalize the potential impact of cyber operations on nuclear stability. Future work that provides more technical detail about the probability of success and the extent of effect would be extraordinarily helpful. In particular, analysis of the cascading effects to the NC3 from cyber attacks on civilian critical infrastructure would provide useful granularity about the impact of cyber operations on an under-studied vulnerability of NC3.

The lack of technical cyber contributions within larger international relations literature is partly due to the fact that the virtual and constantly changing nature of networks and cyber attacks makes it difficult to assess potential effects. However, a good scholarly analysis of technical cyber capabilities is not impossible. Rebecca Slayton's analysis of the cyber offense-defense balance is a particularly interesting way to broach the technical feasibility challenge.[9] Instead of delving into the technical details of cyber attacks, Slayton's work focuses on the limits and advantages of organizations in building offensive and defensive tools. By abstracting out from "cyber" to organizations, Slayton is able to trace the overall probability of cyber advantage without extraordinarily detailed technical work. Based on that kind of analysis, one could imagine follow-on research on the cyber-nuclear problem that walks through the technical characteristics of the NC3—satellite relays, fiber optic cabling, data storage and analytics—and abstracts out to organizations in order to perform an unclassified analysis of the ability to access, exploit, and then degrade or destroy functionality.

Second, much of *Hacking the Bomb* assumes states' reactions to cyber operations or at least proposes a range of potential responses without providing evidence for which responses are more or less likely to occur. However, some of those assumptions might be testable with either unclassified data sets, case studies, or the use of war

[9] Rebecca Slayton,"What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41:3 (2017): 72-109.

gaming. Some of this work is emerging,[10] and future use of innovative methodologies to generate empirics on cyber behaviors might help future literature lean less on assumptions about how states could react to exploits and vulnerabilities of NC3.

A third potential for follow-on research from *Hacking the Bomb* is the development of more explicit theories about what potential cyber effects and behaviors mean for nuclear policy, operations, and doctrine. For example, an analysis could theorize the potential span of cyber effects within discrete categories (degradation of trust in data, deletion of data, functionality of a weapon system, etc.) without making any technical claim about the probability of these effects. Then, the researcher could run logical experiments, game theory, or simulations in which the only difference between nuclear crises is the categorized cyber effects. By identifying the variable we are interested in, hypothesizing potential effects, and then controlling for the variable that we want to explore, future work could create theoretical advances in our understanding of the impact of cyber operations on nuclear stability.

Finally, the policy implications of much of this cyber literature have been either largely abstract, often contradictory, or stove-piped within the cyber domain. For example, authors often recommend better cyber defense and resiliency without acknowledging the large trade-off between cyber defense or resiliency and leveraging cutting-edge digital technologies in military operations. Futter's recommendations suffer from similar problems and he does not generate concrete recommendations outside the cyber realm for nuclear policy planners or nuclear acquisition strategies. Future work should generate empirics or theories that lead to recommendations not only for better cyber defense or deterrence, but also for investments in different nuclear delivery platforms, in decentralized versus centralized command and control, in the storage of targeting data, and in the operational concepts states develop to deliver or respond to nuclear weapons.

Jacquelyn Schneider is an Assistant Professor at the U.S. Naval War College where she is an affiliated faculty in the Center for Cyber Conflict Studies. Her work on cyber, unmanned technologies, and national security has appeared in a variety of outlets including *Journal of Conflict Resolution*, *Security Studies*, *Strategic Studies Quarterly*, *War on the Rocks*, *Foreign Affairs, Washington Post*, *Bulletin of the Atomic Scientists*, and *National Interest*.

[10] Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015); Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018); Jacquelyn Schneider. "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict." Ph.D. diss., The George Washington University, 2017; Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22:3 (2013): 365-404.