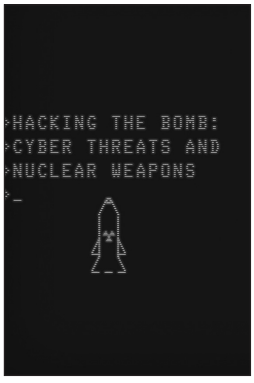

Hacking the Bomb: Cyber Threats and Nuclear Weapons

Andrew Futter

Georgetown University Press: Washington, D.C., 2018, 197 pp.

Reviewed by Kevin J. Latman
Countering WMD Graduate Fellow, National Defense University

Over the past several decades, technology has evolved rapidly, affecting innumerable aspects of life. As Andrew Futter highlights in *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, strategic nuclear weapons systems are no exception. Futter's book is timely, given that states continue to modernize their nuclear weapon systems and grapple with cyber security policy. Historically, strategists had no need to consider cyber threats aimed at disabling, tampering with, or launching nuclear weapons, because nuclear systems were more isolated than other defense systems. Today, in an increasingly interconnected world, more convenience comes with more security vulnerabilities. Although interagency officials may be inclined to modernize the nuclear triad in a more integrated manner, the fact that these systems remain independent is vital to their security—and ours. Futter reveals how the networking of U.S. nuclear systems could leave the U.S.'s arsenal vulnerable to cyber-attack. A thorough read of this well-researched text is likely to influence the thinking of policymakers, increasing the likelihood that they take more seriously the grave threats posed by cyber actors to strategic weapon systems.

Futter organizes *Hacking the Bomb* into four digestible parts. At the beginning of each chapter, he provides the structure and an overview of the content contained therein. He begins Part I by defining the cyber challenge. Because the term "cyber" has many contexts, these initial chapters delve into the general cyber threat and its implications, followed by a discussion of the impact of these threats on nuclear weapon systems. Although the book addresses some very serious potential vulnerabilities for nuclear weapon systems, the tone is not purely alarmist. For example, Futter points out that only a small handful of nations are capable of conducting sophisticated cyber-attacks on nuclear weapon systems.

Part I also examines the differing views of civilian leaders versus military officers on "negative" control, protecting nuclear weapons from unauthorized pre-emptive launch, versus "positive" control, ensuring the weapons are ready for launch when needed. In general, civilian leaders are more concerned about the security of nuclear weapons and negative control threats such as unauthorized use and accidents or mistakes. However, in the event that deterrence fails, military leaders desire constant availability of nuclear weapons and are more concerned about positive control threats, such as vulnerability to a surprise first strike attack. According to Futter, securing nuclear weapon systems requires a balancing act between negative and positive control, which inherently increases the vulnerability of these systems.

Part II of the book delves into what hackers could exploit within nuclear weapons systems. For example, nefarious actors may seek to steal data, disable systems, or, in a worst-case scenario, enable systems and launch or explode its weapons in place. Again, Futter deftly navigates this topic by avoiding abstraction and providing concrete historical examples that read like a spy novel. As James Adams, former chair of the Technology Advisory Panel at the United States National Security Agency, once described in *Foreign Affairs*, cyber-attacks have potential economic consequences as well, by threatening the billions of dollars spent on missile defense systems.[1]

Although much of the fanfare surrounding nuclear weapon systems focuses on warheads, Futter points out that every step of the U.S. procurement process contains vulnerabilities and presents opportunities for cyber exploitation. For example, in 2012 researchers realized that computer chips made in China and used worldwide possessed a major vulnerability, giving would-be hackers the ability to remotely disable or reprogram the chips. The implications of this single example are incredible: to think that any number of nuclear weapon states may have used these tiny chips in nuclear weapon systems, which presents a major vulnerability and security oversight!

Hacking the Bomb is not all doom and gloom. Futter notes how nuclear espionage by cyber means could actually lead to increased stability with respect to nuclear weapons. In the event that an adversary discovers that its rival possesses more advanced nuclear capabilities than previously known, the adversary may seek policies that reduce the chances of escalation and enhance the credibility of deterrence. Furthermore, cyber operations may even aid in counterproliferation efforts. Futter quotes journalist Eli Lake, who says it best: "The specific benefit of [cyber] sabotage is that it makes countries [and terrorists] wary of purchasing crucial [nuclear-related] materials on the black market."[2]

Part III of the book dives deeper into the strategic implications of the convergence of cyber-attacks and nuclear weapon systems. Cyber threats may lead to policy changes and shifting views on deterrence. These threats will force nuclear weapon states to make difficult decisions, and determine whether a cyber-attack on a nuclear weapon system is, for example, equivalent to a surprise, decapitating first strike with a nuclear weapon—which could in turn provoke a proportional response. Although Futter separates cyber threats from nuclear threats, cyber-attacks that threaten nuclear capabilities can quickly escalate global tensions to the brink of conventional or nuclear war.

Part IV explores the numerous challenges posed by the modernization-induced tendency to couple cyber capabilities with nuclear weapon systems. Although nuclear weapons systems are based on 1960s technology and might seem outdated, these systems are actually less vulnerable to cyber-attacks than modern networked systems. Additionally, more advanced systems run the risk of outpacing technical support personnel who troubleshoot them, and only a few select programmers may be capable of fixing issues that may arise. Second- and third-order effects from cyber-attacks may be devastating, and place more emphasis on the importance of advanced conventional weapons, Futter explains. If nuclear systems are compromised, he warns: "deterrence might fail, arms rac[es] return, escalation becomes unmanageable, and the threshold of nuclear use is lowered as a result of developments in advanced conventional weapons and cyber operations."

Throughout the text, Futter offers nuance by speaking to the full spectrum of cyber-nuclear activities, rather than simply focusing on the worst-case scenario of a nefarious actor hacking nuclear systems leading to a nuclear launch or explosion. Nuclear weapon states must guard against a wide variety of such activities, ranging from hacking to nuisances to espionage. All of these illicit activities pose threats to nuclear weapon systems in a variety of ways, from sabotage that makes

the systems behave unexpectedly to nuclear launches or explosions.

After providing the reader with a full typology of how cyber-attacks threaten nuclear weapon systems, Futter concludes with a number of welcome recommendations. These include the recommendation to increase cooperation between cyber and nuclear experts to physical hardening of systems. One of his more compelling recommendations is to establish global cyber-nuclear norms to prevent attacks on civilian targets, and using restraint when it comes to cyber operations. Since the cyber-nuclear interface is still relatively new, establishing norms is critical for setting ground rules early on. Doing so may enhance deterrence, as well, as nuclear weapon states seek to avoid escalation to full-blown nuclear war. Additionally, Futter suggests that nuclear weapon states harden their defensive capabilities against cyber-attacks in order to minimize potentially devastating impacts. Finally, Futter recommends that the global community eventually incorporate cyber into arms control agreements, recognizing the importance and worldwide reach of the threat.

Hacking the Bomb offers policymakers and nuclear enthusiasts alike a glimpse into the very near future and the serious threats posed by cyber-attacks. Although the subject matter lends itself to a textbook format and abstract critical thinking, Futter maintains the reader's focus and interest by interjecting a multitude of fascinating near misses, primarily from the United States' nuclear weapon history. These case study snippets provide an all-important context to understand that the cyber threat is real. Futter provides ample examples of how anything from tiny computer chips to connectivity to outside systems can undermine a nation's nuclear capabilities.

A must-read for anyone involved in modernizing nuclear forces, this book succinctly outlines considerations that policymakers must take into account in order to avoid wasting billions of dollars to create newer, more vulnerable systems. Since nuclear weapon systems often provide a nation's greatest security, policymakers—according to Futter—would be wise to ensure these systems are simple, secure, and separate. ***IAJ***

NOTES

1 Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons,* Georgetown University Press, Washington, D.C., 2018, p. 64.

2 Ibid., p. 84.