THE UNIVERSITY OF TENNESSEE KNOXVILLE

International Journal of Nuclear Security

Volume 7 | Number 1 Article 5

3-12-2021

Book Review of "Hacking the Bomb: Cyber Threats and Nuclear Weapons" by Andrew Futter

Lopamudra Bandyopadhyay
Panchur College (affiliated with the University of Calcutta)

Recommended Citation

Bandyopadhyay, Lopamudra (2021) "Book Review of "Hacking the Bomb: Cyber Threats and Nuclear Weapons" by Andrew Futter," *International Journal of Nuclear Security*: Vol. 7: No. 1, Article 5.
https://doi.org/10.7290/ijns070105
Available at: https://trace.tennessee.edu/ijns/vol7/iss1/5

International Journal of Nuclear Security, Vol. 7, No. 1, 2021

Book Review

Hacking the Bomb: Cyber Threats and Nuclear Weapons

Futter, Andrew

Washington, D.C., Georgetown University Press, 2018, 212 pages, ISBN 9781626165649 (hardcover) | ISBN 9781626165656 (paperback) | ISBN 9781626165663 (epub), Price: $89.95 (hardcover).

Reviewed By Dr. Lopamudra Bandyopadhyay
Assistant Professor and Head of the Department
Department of Political Science
Panchur College (affiliated with the University of Calcutta)
Kolkata, India

A Professor of International Politics at the University of Leicester, UK, Professor Andrew Futter is indeed a significant name when it comes to the study of contemporary nuclear weapons, nuclear strategy, and arms control. He has had such seminal publications to his credit, like *The Politics of Nuclear Weapons* (London, SAGE: 2015) and *Ballistic Missile Defence and US National Security: Normalisation and Acceptance after the Cold War* (New York & Basingstoke, Routledge: 2013), as well as important edited books, such as *Threats to Euro-Atlantic Security* (London, Palgrave: 2019), *The United Kingdom and the Future of Nuclear Weapons* (New York, Rowman & Littlefield: 2016), and *Reassessing the Revolution in Military Affairs: Transformation, Evolution and Lessons Learnt* with Jeffrey Collins (London, Palgrave: 2015) – not to mention innumerable articles on nuclear weapons, nuclear deterrence, nuclear disarmament, cyber security, and cyber semantics. It is relevant to mention here that Professor Futter is a member of the cyber-nuclear security threats task force run by the Nuclear Threat Initiative, an Honorary Research Fellow in Nuclear Strategy at the Institute for Conflict, Cooperation and Security at the University of Birmingham, and a member of the Euro-Atlantic Security Initiative Next Generation working group. His academic stints at the Center for Arms Control and Non-Proliferation in Washington, D.C.; the James Martin Center for Nonproliferation Studies in Monterey, California; and the Norwegian Nobel Peace Institute in Oslo are also worth mentioning at the commencement of this book review.

With the global nuclear systems becoming increasingly sophisticated and digitized, Andrew Futter's 2018 publication, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington, D.C.; Georgetown University Press, 2018), effectively stands upon the central theme of examining and exploring the way nuclear weapons are conceptualized, the evolution of the notion of nuclear strategy, and their current dalliance with the ascension of the significance of the cyber challenge, popularly stated by the author as "the emerging cyber-nuclear nexus" (p.5). In the present-day global environment of cyber threats challenging established notions of mutually assured destruction (MAD), deterrence, and proliferation, Andrew Futter's book is not only contemporary in content, but also extremely significant in more ways than one. Although the book begins on a cautionary note with reference to a fictionalized account of computer hacking with reference to the Hollywood Sci-Fi film of 1983, *WarGames*, it immediately graduates into a full-fledged discussion on how this fictionalized account has indeed become a force to reckon with. The introductory section of

doi:10.7290/ijns070105

the book further illustrates the shifting global scenario with regard to the field of nuclear technology and how cyber warfare can affect cardinal decisions involving nuclear safety and security both at present as well as in the near future.

Futter organizes *Hacking the Bomb: Cyber Threats and Nuclear Weapons* into four sections dealing with noteworthy academic content. At the beginning of each chapter, he provides a brief composition and a summary of the content enclosed therein. Since the term “cyber” has innumerable perspectives, Part I of the book delves into issues such as the broad meaning of the term “cyber challenge” as well as the vulnerabilities of nuclear systems to the aforementioned challenge. The primary objective of Part II is to consider the different threats and challenges to the nuclear systems, especially within the gamut of cyber operations. Part III focuses on the implications of the cyber threats and nuclear weapons management both at the strategic as well as the international levels. It is pointed out in this section, and quite aptly, that cyber threats may lead to policy changes and shifting views on deterrence. Part IV enunciates why nuclear modernization would involve the creation of strategic loopholes, and it also delves into ways and means of demolishing nuclear orthodoxy by placing the cyber challenge in a broader techno-military perspective. The conclusion primarily puts forth vital recommendations to those manning as well as protecting the global nuclear order and enumerates “the key dynamics” needed to prevent mammoth risks from happening in this cyber-nuclear age. These include the recommendation to increase cooperation between cyber and nuclear experts. A more realistic recommendation is to establish global cyber-nuclear norms to prevent attacks on civilian targets.

While *Hacking the Bomb: Cyber Threats and Nuclear Weapons* is comprehensive in its entirety, there are a couple of specifications that I would like to make with regard to the content of the book. The volume incorporates many captivating concepts, but it is often hindered by the author’s inability to verify some of his arguments due to the classified nature of the subjects contained therein. Most of the documentation regarding nuclear weapons and nuclear control systems are still very much classified. Similarly, the cyber capabilities of various nations across the world are also classified. Also, in the recommendation section, the author has upheld the need to establish global cyber-nuclear norms but has not provided any conclusive blueprint regarding these norms. Such a blueprint is a necessity, especially where international organizations like the United Nations’ involvement is the need of the hour for long-term global security.

The bibliography at the end of the book is indeed exhaustive and boasts of thorough research conducted through the usage of official documents, influential as well as path-breaking publications by authors of international repute, research publications, and articles from journals on nuclear security, cyber security, and foreign policy. Further, if the bibliography is to be intricately scanned, it also contains substantial amounts of Professor Futter’s own research papers, articles, and erstwhile publications on the subject at hand.

Futter’s language is lucid and is easy to grasp for the layman. In writing the book, he has taken an approach that he describes as “deliberately designed to be as inclusive, wide-ranging and holistic as possible” (4). He does not employ such elaborate jargon that is usually found gracing the pages of books dealing with the subject of nuclear weapons, nuclear disarmament, or the nuances of cyber security and cyber challenge. Neither does he confuse the reader with technical details pertaining to nuclear weapons or cyber security. The usage of the hyperbole and other such methods of drawing attention towards pure technical terminology are never indulged in. The language is not only refreshing and extremely modern with the necessary touch of academic intervention, when and where necessary, but it also holds the reader’s attention effectively through to the conclusion. Needless to say, the author uses multiple standard research methodologies in conceptualizing this volume.

In conclusion, it may be stated that *Hacking the Bomb: Cyber Threats and Nuclear Weapons* is indeed a book worth reading both within the academic sphere as well as for the general reader interested in examining the complexities of nuclear weapons and their safety with respect to cyber threats and non-state actors employing the same. This is a book that straddles international politics and attempts to disengage from nationalistic goals in order to study the current as well as impending threats from a global perspective. Professor Futter has undeniably been successful in upholding a contemporary strategic issue plaguing not only nations but also regional and international organizations. In a nutshell, this book may be termed as a pioneering endeavor when it comes to the study of nuclear weapons and the cyber challenge facing the security of critical infrastructures across the globe.

doi:10.7290/ijns070105