Hacking the Bomb: Cyber Threats and Nuclear Weapons

Andrew Futter

(Washington, DC: Georgetown University Press, 2018)
ISBN 978-1626165656 pp 216

In the Information Age, the landscape of the battle space has undergone a rapid metamorphosis from the physical domain to the information and cognitive domains. In this transformed battle space, information is the unifying thread amongst various domains of warfare. Thus, the information domain has become an overarching domain and achieving information superiority an operational imperative for all battlefield commanders. The quest to achieve comprehensive information superiority across all domains has blurred the lines among various forms of information warfare. Electronic warfare and cyber warfare now have an overlapping area of Cyber and Electromagnetic Activities (CEMA). Such cross-domain capabilities enable kinetic as well as non-kinetic strikes launched from non-physical domains like the cyber domain. To defend against which, the strategic thinkers are already contemplating the cyber-nuclear weapon as the new 'mother of all weapons'.

The recent standoff between India and Pakistan post Pulwama gave rise to confrontation in the physical as well as non-physical domains. While incidents in the physical domain were covered by the local as well as global media with great enthusiasm, the activities of hackers, who were actively supporting the operations in the physical domain, were seldom publicised. Under such heightened tensions, the escalation of cyber operations to target the nuclear weapons of the adversary may not be ruled out. In the past too, there were well established cyber campaigns in Georgia, Crimea, Estonia and Palestine, to name a few, which banked upon hackers to support the war effort in the physical domain. While

talking of the cyber-nuclear interplay, we cannot skip the 'Stuxnet'. The Stuxnet was a well-planned cyber attack on Iran's nuclear facility, possibly in conjunction with operations in the physical domain. A few cyber experts opine that the Stuxnet was a field trial of '*hacking the bomb*'.

Connecting the dots, Andrew Futter in his book *Hacking the Bomb: Cyber Threats and Nuclear Weapons* takes the idea further and expresses his serious concerns regarding the possibility of triggering/disabling a nuclear weapon by hacking its associated computer system which may have a devastating effect on a particular nation or on all of mankind. The concerns of the author are well placed. The book finds immense relevance in the present day world order, especially for nuclear capable states like India, wherein, even non-nuclear states and non-state actors are exploring cross-domain cyber-nuclear capabilities to open new vistas of warfare.

Andrew Futter is a PhD in international relations and teaches the subject as Assistant Professor in the University of Leicester. He is an accomplished writer on nuclear technology and international relations, with books like *Ballistic Missile Defence* and *Politics of Nuclear Weapons* to his credit. This publication is the result of research work of three years based on secondary data which Futter has extensively quoted in his work.

The book has been methodically divided into four parts and has seven chapters to create a flow and build arguments. The author begins his narrative by referring to the 1980s' sci-fi movie called "Wargames" in which a teenager hacks into the Pentagon computers which control nuclear weapons, and nearly starts World War III. The movie raised hackles all over the world and the President of the United States personally issued directions to mitigate such a threat. Owing to this background, Futter has attempted a similar sensationalism with the cyber-nuclear nexus.

Andrew Futter initially builds up a correct understanding of the nature of the cyber challenge in the given context. He adds that cyber should be viewed as an integral part of Information Warfare (IW) but we should also understand that it is transforming the way IW is being conducted.

The book then delves into the vulnerabilities of nuclear systems which stem from their inherent management structures and exposure to the risk of accidents, mistakes from complexities, and exploitation of weaknesses in the system by cyber operations. The vulnerabilities have further been enhanced by the digitisation of the Nuclear Command, Control and Communication (NC3) structures.

The book further leads the reader through a number of related incidents and their analyses to create the argument that nuclear systems are vulnerable to cyber nuclear espionage as state nuclear secrets are akin to any digital data which can be stolen remotely, lending themselves to exploitation. Based on the types of controls on nuclear weapons, the author has very innovatively divided the possible cyber attacks on nuclear systems as "enabling attacks" wherein an unintended launch of a nuclear missile or a nuclear explosion is initiated or "disabling attacks" whereby the hackers disable the system and prevent a missile from being launched. Futter then rightly builds the argument that while nuclear nation states will be interested in disabling their opponents' systems it would be the non-state actors who would be interested in causing nuclear explosions.

Futter is of the opinion that the future cyber-nuclear strategies will be defined by five dynamics: implementation of technologies to jump the air gap, 3D printing to challenge nuclear non-proliferation, cyber proliferation due to reverse engineering of attack vectors, modernisation of nuclear systems leading to associated vulnerabilities and unlocking of unknown capabilities of computers. The author, thus, concludes that given the nature of the future battlefield, nuclear weapons management should be simple, that is, devoid of any unnecessary complexity, secure from both traditional and digital operations and separated from other weapon systems, including planning processes and sensors.

The main argument of the book is two-fold: first, the burgeoning cyber age is transforming the way we should think about, manage and control nuclear weapons; and, second, establishing a norm of hacking the bomb is a

bad idea fraught with danger, uncertainties and risks. Futter has successfully carried both arguments throughout the book and his articulations have been well organised and equally well supported. He has also extensively included statements from other seminal works which makes the reading lucid and interesting. Bibliographic references are a trove of information on the topic itself and can help to further the research. However, the absence of primary data on cyber attacks on sensitive infrastructure and nuclear systems was felt during the reading but is understandable.

In an overall assessment, Andrew Futter's *Hacking The Bomb* is a well-researched assessment which leaves the reader with valuable takeaways for further research. The author has assumed some state responses against cyber operations. The same can be verified against case studies or war-gamed to understand how opponents can react. It would help build policies on the subject. The book claims that cyber war is not possible and believes that the cyber challenge remains an environment or context but not a domain of military operations—it is a matter of interpretation and can be accordingly theorised. The author has also raised the issue of absence of international regulations for cyber attacks or threats, which can be a niche area of work and persuasion. Finally, while the recommendations of Futter to obviate the challenge largely remain confined to the cyber domain, no concrete recommendations have been provided for nuclear policy-makers. This vertical may be undertaken for further research work.

Overall, the book carries fresh ideas amidst stereotyped speculations of cyber war by various authors. It will be of great interest to scholars and students of cyber and nuclear warfare as well as defence practitioners and policy-makers.

Rajeev Sabherwal

Lieutenant General **Rajeev Sabherwal** is Signal Officer-in-Chief and Colonel Commandant, Indian Corps of Signals