Book Review: *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*

Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press, Cambridge, MA, 2020. ISBN: 9780674987555. 319 pp. About $27.95

In his book, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, author Ben Buchanan attempts to contextualize modern-day cyber-attacks within the domain of geopolitics—a daunting task, as the cyber domain is inherently untrustworthy, making definitive proclamations suspect. That said, by applying the statecraft concepts of signaling and shaping, Buchanan builds a convincing case using practical comparisons to espionage and conventional warfare, underscoring the conclusion that cyber-attacks are not random acts of ever-increasing destruction; instead, they represent a conscious cyber struggle between states. In other words, cyber-attacks have become tools for the policymaker's signaling and shaping operations. "This is the new form of statecraft, more subtle than policymakers imagined, yet with impacts that are world-changing" (3). To this end, the author provides a convincing argument for cyber-attacks as tools of state power, rather than the random acts of criminals.

As the world becomes increasingly connected, dependence on information communication technology has become paramount to nearly every facet of modern society. Correspondingly, the complexity that characterizes the cyber milieu facilitates misunderstanding and fear as vulnerabilities are made apparent. As such, any event that destabilizes the cyber ecosystem immediately captures the attention of news media. Fear and sensationalism have prematurely concluded the inevitability of a catastrophic cyber event. To this extent, "while policymakers and scholars understand what nuclear weapons and tanks can do, the possibilities, pitfalls, and processes of hacking missions are comparatively opaque" (8).

Buchanan seeks to bring clarity to the subject by challenging the theoretical conclusion that cyber-attacks must end in a digital Pearl Harbor. Drawing on real-world events, Buchanan deconstructs the most significant cyber-attacks from the United States, Israel, China, Russia, Iran, and North Korea, analyzing their intent, significance, and meaning to the broader global community. Buchanan chronicles the transformation of cyber-based espionage in the form of passive collection, wherein the discovery of the operation equates to mission failure, to overt cyber-attacks conducted as a declaration to the world, where amplification is the intended end-state.

In an unprecedented collection, Buchanan leverages a wide variety of sources, including recently declassified information, to gain insight into state-spon-

doi: 10.18278/gsis.5.2.11

sored cyber-based operations, thus unraveling the seemingly anarchic nature of cyber-attacks and opening a new window into this phenomenon.

The book begins by exposing the profound cyber-based espionage advantage of the United States, and more broadly, the Five Eyes member nations. The enormity of the advantage resided in keeping the innovative tools, techniques, targets, and coverage a secret. Buchanan then unveils how these advantages were used and, more significantly, how they came to light. The chapters move quickly one by one as he uncovers the seminal events of technical superiority and subsequent exposure.

As espionage, in any form, does not survive the light of day, states moved quickly from passive collection to more aggressive efforts in the form of cyber-attacks and eventual disinformation operations in combination. Importantly, Buchanan details the differing intentions among states and how these newfound capabilities are leveraged to their end. Buchanan does an expert job weaving the transition from shadows into the new normal of cyber struggle. The leaks of Edward Snowden combined with the reach of WikiLeaks, the theft of tools by the Shadow Brokers, and the cunning Russian disinformation operations turning the news media potentially into an unwitting catalyst, all served to expose the advantages maintained by the US and the Five Eyes nations, and in doing so, irreparably removing them. The resultant cyber awakening has brought new, more unpredictable, players into the game, with the promise of more to come. Meaning that cyber-attacks, intended or not, have become the “new normal in geopolitics.”

This book is exceptionally well-researched and approachable for a broad audience. The theme is easily understood and consistent throughout the well-written chapters. The case selection is excellent and profound in its ability to highlight critical concepts within the text. Anyone interested in international relations and curious about the role that cyber may have within it should read this book. This book is the first of its kind in both depth and breadth, bridging the gap between international relations and cyber-attacks.

The primary argument of the book is that cyber-attacks are the new normal of geopolitics. The author does an excellent job confirming his assertion by detailing the world’s most significant cyber-attacks. However, a simple, yet powerful example of confirmation would have been the inclusion of the 2015 agreement between China and the United States to stop hacking. This agreement would have added gravitas to Buchanan’s central theme that cyber-attacks are a normal part of geopolitics, especially as the results of the agreement were met with a sharp decline in cyber-attacks against the United States originating from China. That said, its inclusion would not have changed the final analysis, which remains on point.

The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics is not a technical book. Those seeking to understand the nuance within the software application code of the greatest collection of hacking tools ever assembled will be disappointed. The book is, however, an excellent addition to the literature of international relations, adding the much needed and often misunderstood cyber-based component into the conversation. Buchanan frees cyber-attacks from the traditional cybersecurity paradigm, placing it firmly within the context of geopolitics. In doing so, Buchanan brings a fresh perspective to the mystique surrounding modern cyber-attacks moving away from the fear of a cyber Armageddon toward the practical struggle between states for power and influence. Impeccably researched, this book is a must-have for international relations students, senior policymakers, or anyone seeking to understand the role and current trajectory of cyber-attacks within the field of international relations.

Al Lewis

American Military University