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

Ben BUCHANAN

Cambridge, Harvard University Press, 2020, 412 pages, ISBN (Hardcover): 9780674987555

Enescan LORCİ
PhD Candidate, Institute of China and Asia-Pacific Studies, National Sun Yat-Sen University, Kaohsiung
E-Mail: enescanlorci@g-mail.nsysu.edu.tw
Orcid: 0000-0003-0111-6331

In "Hacker and the State: Cyber Attacks and the New Normal of Geopolitics," a comprehensive work spanning three chapters, Ben Buchanan undertakes a significant exploration of the transformative effect that hackers have had on global affairs over the past two decades. Positioned at the intersection of cyberspace and international relations, Buchanan employs the established concepts of "signaling and shaping" from the field of International Relations (IR), which refer to the tactics and activities that governments or other players use to convey their intentions, sway public opinion, and mold geopolitical outcomes. In IR, signaling refers to deliberate acts or signals taken by states or other actors to tell others about their intentions or capacities, affecting perceptions and forming expectations in the process. Contrarily, shaping describes intentional attempts to alter the dynamics, norms, or structure of the international system to bring about outcomes that support one's strategic goals or interests. For example, in the field of IR, nuclear capabilities are frequently analyzed as signaling mechanisms due to their potential for catastrophic destruction. Similarly, contemporary scholarship suggests that cyber capabilities have become increasingly instrumental for signaling purposes, reflecting the evolving dynamics of international security and diplomacy.

However, Buchanan contends in the initial segments of the book that contrary to prevalent notions equating cyber capabilities with nuclear or conventional military capabilities, cyber operations are inherently unsuitable for signaling. Instead, he advocates for a conceptual framework grounded in shaping as the most appropriate lens to comprehend cyber operations. This framework revolves around the core concepts of espionage, attack, and destabilization, each addressed in dedicated chapters. Through this analytical approach, Buchanan systematically substantiates his argument and illuminates the ways in which cyber operations have shaped geopolitics over the past two decades.

In the inaugural chapter focused on espionage, Buchanan delves into the practice's historical context, drawing parallels with significant events like the Cold War and World War II. The narrative then seamlessly transitions to the cyber domain, highlighting the centrality of cyber capabilities in contemporary espionage activities such as PRISM system used by the United States (U, or Operation Aurora run by Chinese hackers against many US institutions and individuals.

A substantial portion of the chapter is dedicated to elucidating the distinct advantage enjoyed by the US and its Five Eyes allies – the United States, United Kingdom, Canada, Australia, and New Zealand – in signaling intelligence. Buchanan underscores the home-field advantages of these countries, strategically positioned along vital hubs and cables that constitute the global digital network. Notably, he emphasizes the pivotal role of technology companies rooted in these nations within the digital ecosystem, encompassing hardware, software, and network connectivity. The voluntary provision of data by individuals, corporations, and governments worldwide to technology giants like Google, Facebook, and Amazon becomes a crucial element, given these companies' adherence to US law and collaboration with the intelligence community. Consequently, the US government can legally access such data for foreign intelligence purposes.

First, Buchanan challenges the common view that geography is irrelevant in cyberspace, highlighting instead the enduring importance of geographic location, particularly in facilitating substantial cyber espionage through home-field advantages. Second, the author underscores the inadequacy of exclusive reliance on defensive measures such as implementing strong encryption protocols to protect sensitive data from unauthorized access or employing advanced firewall systems to prevent malicious intrusions into a state's network for securing cyberspace, advocating for a balanced approach that includes offensive actions such as cyber intrusions for surveillance, to enhance a state's cybersecurity. Last, the chapter dispels the notion that states engaging in espionage must necessarily be adversaries, highlighting instances where espionage activities are directed even towards close allies. Buchanan substantiates this point by illuminating US espionage on ideologically aligned countries such as Germany, Greece, and Japan.

In the second chapter, Buchanan meticulously examines prominent cyber-attacks, including the US and Israeli-perpetrated Stuxnet, Iranian-led Aramco Attack and Operation Ababil, and the North Korean-executed Sand Casino and Sony attacks. The comprehensive analysis aims to discern whether these cyber-attacks functioned as signaling or shaping mechanisms in geopolitics.

The author contends that assessing these attacks through the lens of signaling renders them potentially failures. Traditionally, successful signaling in IR necessitates clarity on two key aspects: the actor initiating the signaling and the message intended to be conveyed. On the other hand, shaping involves the deliberate efforts of states or actors to influence the structure, norms, institutions, or dynamics of the international system in a manner that aligns with their interests or objectives. Unlike signaling, which focuses on conveying specific messages or information, shaping entails broader and more proactive attempts to mold the international environment to suit one's strategic goals. Shaping strategies can encompass a wide range

of actions, including diplomacy, economic aid, military alliances, institution-building, norm entrepreneurship, and soft power projection.

The aim of shaping is to create conditions that are favorable to the interests and preferences of the actor undertaking the shaping efforts, thereby enhancing its security, prosperity, or influence on the global stage. Buchanan argues that, in the realm of cyber-attacks, adherence to traditional signaling criteria might deem them unsuccessful. This stems from the fact that, contrary to conventional IR signaling, the success of a cyber-attack is contingent upon its non-detection by the adversary. The perpetual concern of deniability in cyber operations further complicates the signaling aspect. The anonymity of the actor not only obscures the attribution of the attack but also renders the conveyed message ambiguous. The author effectively illustrates this point by scrutinizing each cyber-attack, examining the outcomes in relation to the attackers' intended objectives.

In Chapter 3, Buchanan delves into the strategic use of cyber operations by states to achieve manipulation and destabilization objectives against their adversaries. The chapter provides insights into various instances of destabilization-motivated cyber operations, such as Russia's interference in the 2016 US elections, the Shadow Broker's leaks of the US National Security Agency's (NSA) cyber capabilities, North Korean cyber operations involving theft, ransomware, and manipulation, and Russian cyberattacks targeting Ukrainian critical infrastructures. A key emphasis in this chapter revolves around the significance of data for nations so that they can analyze it and derive actionable intelligence about adversaries. The revelations from the Shadow Broker's leaks, which exposed some of the most crucial offensive cyber capabilities of the NSA initially designed for national security but later utilized by Russian and North Korean hackers, underscore the precarious nature of cyberspace and its profound implications.

In conclusion, Buchanan fulfills the commitment outlined in the introduction by demonstrating how hackers have actively shaped global geopolitics over the past two decades. Notably, he accomplishes this without delving excessively into the intricate technical details and jargon associated with cyber-attacks, ensuring accessibility for IR scholars who may not possess a deep technical background. The book's clarity in explaining every technical term in straightforward language positions it as a valuable and essential read for IR scholars seeking to comprehend the intersection of cyber-attacks and the dynamics of global politics.