Carlos Solar, *Cybersecurity Governance in Latin America: States, Threats, and Alliances*

State University of New York Press, 2023, pp. 352

María Paz Sandoval Bravo

University College London

(Received 9 November 2023; accepted 9 November 2023)

In a world increasingly concerned with cybersecurity matters, Carlos Solar turns the spotlight on Latin America, offering an insightful analysis of its governance in this crucial area. Through detailed research, Solar illustrates the region's particularities and challenges. The book consists of seven interconnected chapters exploring cyber governance in Latin America, from analysing correlations between internet penetration and governance (Chapter 1) to a deep review of cybersecurity maturity in the region (Chapter 7).

The author states that the book contains three fundamental pillars of research: (1) to assess the cybersecurity scenario in developed countries and illustrate current events in the developing Western hemisphere; (2) to explore the governance of cybersecurity in comparison to other perceived threats to national security in the region; and (3) to illustrate the militarisation of cybersecurity policy (p. 9).

Similarly, Solar states that under the definition of cybersecurity governance as the actions and policies adopted by civilians, the military, industry and the private sector to safeguard digital space, the focus of the book is directed at the military. Thus, Solar contextualises Latin American practices and policies concerning global and constantly evolving cybersecurity, mainly from six Latin American countries: Argentina, Brazil, Chile, Colombia, Mexico and Venezuela. These countries are analysed throughout the book alongside comparisons with great powers such as the United States, China and Russia (pp. 19, 26, 111).

The book begins in its first chapter by explaining the principles of online governance, providing a theoretical foundation for its analysis. Solar argues that the widespread adoption of internet technology has transformed both government and civil society. However, this transformation has been uneven in the region, resulting in differences in internet access and usage and, consequently, in the effectiveness of governance (p. 46). However, the dynamics of this transformation are complex and multifaceted. While there is a positive correlation between government effectiveness and internet penetration in Colombia, there is a negative correlation regarding corruption control, highlighting the multifaceted nature of this correlation. Brazil and Colombia show a positive correlation in accountability, while Chile, despite its high internet penetration, does not show significant correlations. In this part of the book, the author also emphasises the lack of attention towards Latin America in cybersecurity and governance studies compared to global powers, underscoring the need for further exploration and understanding of these regional relationships.

https://doi.org/10.1017/S0022216X24000221 Published online by Cambridge University Press

In Chapters 2 and 3, Solar explores the militarisation of cybersecurity in Latin America. The discussion focuses on how governments utilise cybersecurity for national defence and interests, including developing cyber weapons, cyber defence and international cooperation. These topics lead to discussions on these operations needing more transparency and ethical considerations. Solar raises critical questions about the future cybersecurity path in Latin America, pondering if it will follow the trajectory of advanced powers or diverge strategically. Chapter 3 further investigates the influence of military and security policies on cybersecurity, focusing on the industrialisation and technologisation of armed forces. The chapter highlights cyber weapons' anonymous and unregulated nature, which creates ethical and legal dilemmas, potentially leading to a cyber arms race.

The book then investigates case studies that explore the relationship between modern warfare and cybersecurity. Solar emphasises how technology has reshaped the nature of warfare, discussing cyber intelligence, defence, and surveillance strategies. The delicate balance between security and individual rights is also addressed in this context. Throughout the book, the author underscores the significance of cyberspace for defence and security and analyses how threats converge in the interconnected world. The book contemplates whether states will adopt an offensive or defensive approach to cybersecurity, considering the geopolitical dynamics at play.

In the subsequent chapter, Solar evaluates the array of strategic threats confronting Latin America, scrutinising the complex security environment and the rise of cybersecurity as a key governance challenge. The analysis foregrounds the adaptive strategies of regional states such as Colombia, Chile and Brazil as they bolster their military capacities in response to an intricate mix of conventional and cyber threats. The chapter further explores the nascent stage of cyber conflict within the region, suggesting a departure from the traditional state monopoly on violence.

The book's later chapters explore cyber alliances between Latin America and the United States, exploring their benefits and challenges. The author investigates technological dependence, privacy policy differences and the nature of bilateral relationships, underscoring the need for effective collaboration and communication amidst the escalating complexity of cybersecurity challenges. In the final chapter, Solar evaluates the cybersecurity maturity of Latin America. He assesses individual country capabilities, government policies and regional collaboration. While some countries have made significant progress in this area, others are still in nascent stages, and the absence of a unified regional strategy poses challenges for the future.

Solar concludes the book with a reflective interpretation of the findings, presenting prospective paths for future research and policy in cybersecurity in Latin America. His work is a valuable contribution to cybersecurity studies, particularly in the Latin American context. The book comprehensively analyses the region's cybersecurity governance landscape, making it relevant to academics, policymakers, decision-makers and professionals in cybersecurity, international relations and Latin American studies. The comparative data and relational analysis provided by the author form a foundation for further research and the implementation of best practices in the field of cybersecurity governance in Latin America.

This work represents a fundamental contribution and a remarkable milestone in cybersecurity, shedding light with great expertise on the governance landscape in Latin America. Through a robust comparative quantitative analysis, the book effectively

https://doi.org/10.1017/S0022216X24000221 Published online by Cambridge University Press

demonstrates a comprehensive understanding of various themes, such as the correlation between the internet and governance and the complexity of cyber weapons. The presentation could be further complemented with the integration of additional qualitative and empirical details, offering a richer narrative alongside the existing quantitative analysis.

The work excels in its detailed coverage of critical topics, offering a comprehensive analysis in several chapters. The inclusion of more global interactions could provide a broader perspective, enriching the current analysis with additional international dimensions. A notable strength is the coherent structure and precise transitions between topics; enhancing the interconnection between chapters could provide a more unified narrative.

The inclusion of Venezuela as a case study is insightful, given its unique geopolitical position in Latin America, and offers a valuable contrast with the region's emerging democracies. This comparison enriches the book's perspective on the geopolitics of cybersecurity in the region. (Unlike the other countries in Latin America studied in the work, which can be classified as emerging democracies, Venezuela falls into a different category, and is often considered an 'authoritarian regime' or an 'illiberal democracy'.)

With this book, Solar offers an innovative and significant contribution to the literature on cybersecurity. It underscores the multifaceted nature of cybersecurity as not merely a technical matter but also a pivotal political and military concern. Solar's thorough examination of the interplay between state policies, the military industry and cybersecurity provides an insightful and indispensable viewpoint, especially given the customary focus on regions outside Latin America. This work is particularly relevant for an audience comprising academics, policymakers and professionals involved in cybersecurity, international relations and Latin American studies. Its data contribution and comparative, relational analysis lay a solid groundwork for subsequent research and the adoption of best practices in cybersecurity.

doi:10.1017/S0022216X24000221

Rachel A. Schwartz, *Undermining the State from Within: The Institutional Legacies of Civil War in Central America*

Cambridge University Press, 2023, pp. xxii + 310

Rose J. Spalding

DePaul University

(Received 30 December 2023; accepted 30 January 2024)

Building on a growing body of scholarship that analyses state institutional development, Rachel A. Schwartz has written a bold and ambitious book that is both theoretically distinctive and empirically rich. Like many analysts working in Central