
Reviewed by Kendall Giles (Virginia Polytechnic Institute and State University)

Published on H-Sci-Med-Tech (August, 2023)

Commissioned by Penelope K. Hardy (University of Wisconsin-La Crosse)

Currently a senior research fellow in international security studies at the Royal United Services Institute think tank in the United Kingdom, Carlos Solar has previously written *Government and Governance of Security: The Politics of Organised Crime in Chile* (2018), edited "Governing the Military: The Armed Forces under Democracy in Chile" (expected 2024), and coedited (with Carlos A. Pérez Ricart) *Crime, Violence, and Justice in Latin America* (2023). His 2022 book, *Cybersecurity Governance in Latin America: States, Threats, and Alliances*, explores cybersecurity threats, alliances, and strategies in Latin America within the context of today’s militarization of cyberspace and rivalry between the United States and China. Not counting the introduction and conclusion, the seven chapters explore three main research themes: the state of cybersecurity today in Western Hemisphere countries, the governance of cybersecurity relative to other national security threats in the region, and the militarization of cybersecurity. Though Solar discusses many security examples and incidents, the level of analysis is mainly at the nation-state level, as common in political science, criminology, or international relations fields, rather than engineering-oriented analyses of algorithms and other lower-level technical details.

The premise of the book is that with the growth and reach of the internet, information and computing technologies (ICTs) play an increasingly active role in shaping and affecting relationships and activities among individual citizens; between citizens, companies, and governments; and between nation-states. With the incorporation of cyberspace in our daily lives, we are enjoying some benefits provided by these technologies, though unfortunately cybersecurity risks have similarly grown in complexity, scale, and scope to include not just technical concerns over the spread of computer malware and network intrusions but also sociotechnical concerns, such as the rise of cybercrime, terrorism, and hactivism, as well as political concerns, such as the creation of offensive cybercapabilities (so-called cyber-weapons) by competing states, militaries, and non-state actors. In fact, though Solar notes that tradi-
tional military conflicts in the world have been decreasing—setting aside the fact that the 2022 Russian invasion of Ukraine is still ongoing as I write this review—there has been tremendous growth in both military as well as civilian cybersecurity markets. In other words, we are now living in the era of the militarization of cyberspace. While such superpowers as the United States and China are at the forefront of this push, through a number of case studies and comparative analyses, the book examines in detail how emerging democracies and developing states in Latin America are responding to this cyber-situation by developing cybersecurity governance policies and strategies of their own.

Of particular interest to those in the United States might be the chapter on the US-China rivalry and the impact of that relationship on states in Latin America. While the United States obviously has a strong influence on its neighbors to the south, that influence has a fraught history, especially in certain Latin American countries, and recently changing US priorities have opened opportunities for such countries as China to play a larger role in the region; despite the shared geographic proximity, the perception of the United States as a model and ally for security, trade, and commerce is not uniformly distributed across the region. An additional chapter focuses specifically on alliances with the United States, showcasing six case studies profiling three positive and three negative examples of prospects of US-Latin America partnerships. Another chapter explores the changing nature of war by comparing the nature, scale, and scope of strategic threats with case studies of select Latin American countries. Solar assesses the effects of new technologies on how countries industrialize the means of war, political and economic factors that affect the growth of military capabilities, and the importance of cyberspace in dealing with national security strategic threats.

Some book contents (such as some text and tables) have been previously published by Solar in academic journals, which helps explain the scholarly tone and which shape the audience for the book. Though Solar includes qualitative methods, and while discussions of independent variable selection, statistical test metrics, degrees of freedom, and p-values found within the text of some of the book’s chapters are to be expected in some quantitative and empirical social science journal articles, books targeting broader policy or government audiences normally move such details to an appendix. However, perhaps the author is highlighting such analyses and statistical details, as well as walking through how he formulated research questions and testable hypotheses, to provide a template or aid for future researchers interested in conducting their own quantitative cybersecurity social science studies or extending the author’s line of research.

As the internet and ICTs become more global in their reach and further integrated into society, cyberspace is increasingly essential for economic growth, though it is also becoming exploited and in danger of fragmentation, especially by non-democratic countries and non-state actors, and so the book’s particular focus on the developing states in Latin America provides timely discussions and policy considerations. Alliances between nations need to be made, technology programs need to be established, cybersecurity policies that cover civilian, industry, military, and government concerns need to be created, and questions regarding the potential benefits and risks of cyberspace on peace and prosperity need to be considered. The case studies and analyses in this book may thus help stakeholders struggling with these types of decisions in our evermore interconnected world.
If there is additional discussion of this review, you may access it through the network, at
https://networks.h-net.org/h-sci-med-tech


URL: https://www.h-net.org/reviews/showrev.php?id=59317

This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License.