on the Department of Homeland Security (DHS). Odlum offers a candid diagnosis of the bureaucratic and cultural impediments to effective strategic planning and programming in the State Department, which, though "sufficient to muddle through and with diplomatic tools and programs that remain planned and funded well enough to react" to an immediate, local crisis, can end in larger "policy failure [that] is most often the result of poor planning or poorly managed implementation or both." Patterson highlights the value to the United States of sustained funding for United Nations (UN) peacekeeping operations as an affordable hedge against instability in troubled regions. This argument, carried forward from the political science literature on post-conflict stability and reinforced with a detailed discussion of UN funding pathways and resourcing, is an intriguing direction that merits broader incorporation in discussions of force employment and competing operational demands. Troutman's chapter is equally illuminating, tracing the evolution of DHS since its founding nearly two decades ago. He diagnoses the fundamental challenge faced by the department clearly: "The DHS is neither a peripheral nor a temporary addition to U.S. national security. However, it is resourced and organized as though it were both." Of the various thoughtful recommendations for reform and process modernization across the volume, the succinct set of proposals that Troutman ends his chapter with hits the hardest.

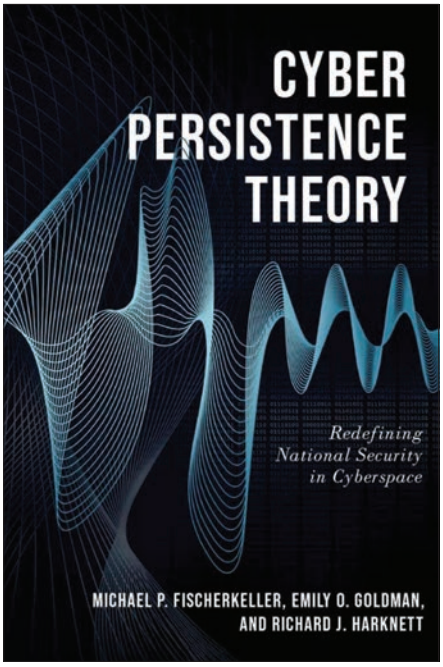
Resourcing the National Security Enterprise is at its softest when it bemoans larger trends such as increased nondiscretionary spending, the expanding national debt, and the projected slowing of economic growth. Although these trends do matter, the cursory treatment they receive at several points oversimplifies the uncertainty and complexity in such projections, ignores the sound advice offered elsewhere to acknowledge that some things are beyond a security strategist's control, and distracts from the overall thrust of the chapter. Left underdeveloped is the argument that many of these same trends—namely, rapidly increasing health care, higher education, housing, and pension costs—detract as much from the proportion of the military's overall budget spent narrowly on modernization and training as from DOD's overall relative share of the Nation's production. More narrowly, the book leaves unexplored the challenges facing the Navy as it balances tradeoffs between fleet size, emerging adversary capabilities, operational tempo, and modernization, all against the backdrop of limited shipyard capacity. The forces that led the sea Service to overinvest in some platforms at the expense of others in prior decades are worthy of separate, deep study, but (at a minimum) a nod to the dynamics driving the Navy's shipbuilding plans would have made *Resourcing the National Security Enterprise* a richer read.

Those minor critiques aside, a close reading of *Resourcing the National Security Enterprise* is a valuable starting point for the deeper understanding required to guide the fundamental processes that shape our national defense. As Ferrari, a retired Army major general, ends his contribution,

To have true positive influence on the process requires investing hundreds of hours in preparation and working multiple jobs in the Pentagon. High rank and position cannot shortcut the process. Part-time programming may alone account for the dismal outcomes associated with America's first battles.

This volume has earned a place on strategists' bookshelves and consideration for inclusion in higher-level professional military education curricula. Perhaps more important, its underlying message, that budgeting and programming experience is both invaluable and irreplaceable, should guide career managers and mentors as they steer promising officers toward assignments of greatest impact. **JFQ**

Lieutenant Colonel Stephan Pikner (FA59) is the Military Advisor to the Director, Office of the Secretary of Defense, Office of Net Assessment.



Cyber Persistence Theory: Redefining National Security in Cyberspace

By Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett
Oxford University Press, 2022
266 pp. $28.45
ISBN: 9780197638262

Reviewed by Stafford A. Ward

Few books have been written in the recent past whose stated intent has been to influence and shape the perceptions of foreign and defense policymakers. In the spirit of the famed Stanford University political scientist Alexander George, who wrote *Bridging the Gap: Theory and Policy in Foreign Policy*, the authors of *Cyber Persistence Theory: Redefining National Security in Cyberspace* have successfully bridged the gap with a thought-provoking, accessible academic analysis. *Cyber Persistence Theory* holistically examines the current cyberspace environment in a way that is sure to be useful to U.S. cyberspace policymakers and operators.

The arguments advanced by the writers artfully explore the structure of the new cyberspace environment. The authors are a qualified mix of

cyberspace academics and practitioners who succinctly capture their previously published thoughts on cyberspace to advance a coherent and novel concept of cyber persistence theory. Successfully communicating a theory to a range of communities can be a heavy lift, but the authors have included extensive footnotes that provide resources through which readers can delve deeper as needed into the concepts discussed, such as structural realism, agreed competition, balance of power, and offense-defense theory.

The heart of *Cyber Persistence Theory* explains that

the primary [cyber faits accomplis] and secondary [direct cyber engagement] behaviors of States in and through the cyber strategic environment . . . are consequences of a structural imperative to persist and of a structurally derived strategic incentive to pursue gains through cyber exploitation short of armed-attack equivalence.

This theory argues that cyberspace exploitation, the most dominant form of cyberspace activity, represents strategic competition and therefore should be understood as one state's gaining cyberspace advantage through another's cyberspace vulnerabilities in a short time frame. To make their case, the authors consider various international relations theories and strategic concepts to establish the foundation of persistence theory for the reader. They bridge the gap by drawing on international affairs scholarship by authors including military and nuclear strategists such as Thomas Schelling, Kenneth Waltz, Carl von Clausewitz, and Bernard Brodie, as well as scientific philosopher Thomas Kuhn. In particular, the authors acknowledge Waltz, the founder of neorealism, or structural realism, as defining the international system as a "condition of insecurity . . . that works against [international] cooperation." Because states in our era of Great Power competition are leveraging malicious cyberspace activities as an alternate means of accomplishing their geopolitical goals, there is no inherent incentive for those states to cooperate as they would in the concert of international diplomacy. In sum, there is no United Nations in cyberspace.

The first four chapters of the book thoroughly explain the theoretical concepts that define the cyberspace environment; they are followed by several chapters examining real-world cases of cyberspace campaigns among both micro-resilient and micro-vulnerable states. For example, the authors highlight the U.S. Government's cyberspace operations to disrupt the so-called Islamic State's online propaganda activities, Russia's compromise of U.S. networks, and China's zero-day exploitations of commonly used software applications, such as Microsoft Exchange and Adobe Flash.

With the foundations of cyber persistence theory established, the authors move to explain the three strategic environments that characterize the entire human history of security: conventional, nuclear, and cyberspace. Conventional security rests in the presence of war, nuclear security rests in the absence of war, and cyber security rests in the alternative to war. The authors point out that most policymakers and operators currently frame cyberspace in a Cold War context, which maps inaccurately to the current strategic cyberspace environment. The authors argue that "interconnectedness" is the core structural feature of the cyber strategic environment, requiring continuous integrated campaigning and supported by ongoing collaboration, integration, and synchronization across all relevant cyber planning and operational players and all instruments of national power. Cyber persistence theory also suggests that cyberspace operations are not inherently escalatory, and such operations rarely cross the upper bound of agreed competition, or the threshold of warfare, into kinetic operations.

Cyber Persistence Theory also defines the evolution from the two strategic environments to the current cyberspace strategic environment as a paradigm shift that necessitates a change in strategic thinking among policymakers, senior defense leaders, and joint force operators. Thomas Kuhn, the authors note, "writes that a paradigm provides a community with its basic assumptions, key concepts, and methodology. . . . For a shift, or 'change in worldview,' to occur, there must be a realization of the misalignment between theory and reality." The authors argue that the misapplication of the paradigms of conventional and nuclear environments to cyberspace represents a failure to understand the nature of the cyber environment. This is sure to generate discussion among scholars and strategists alike. For example, *Cyber Persistence Theory* argues that cyber policymakers who plan to hold cyber targets at risk fail to understand that cyberspace is an environment where seizing targets of opportunity is a better policy prescription, given the highly dynamic nature of cyberspace.

The authors also offer insights for diplomats and specialists in international law who must devise methods for minimizing risks inherent in the international system due to malicious cyber activities. As supplementary reading, policymakers and joint force operators should consider the late Columbia University political scientist Robert Jervis's essay "Cooperation Under the Security Dilemma," to aid in their addressing international cooperation in cyberspace. Would inter-state cooperation create security advantages among like-minded states in an environment of interconnectedness? Is Waltz correct that such cooperation in cyberspace might not completely provide states with security guarantees against states acting outside of responsible cyberspace norms?

Cyber Persistence Theory will help policymakers and cyberspace warriors and operators to make sense of the work they do daily, offer a sense of purpose, and help to both shape and articulate the cyberspace environment. *Cyberspace Persistence Theory* should be mandatory reading for joint force operators, policymakers, diplomats, and law enforcement specialists, to provide them with a richer understanding of early-21st-century cyberspace. **JFQ**

Stafford A. Ward is a Cyberspace Integration Planner in the Partnerships Division at U.S. Cyber Command (USCYBERCOM) and is also a USCYBERCOM Commander's Civilian Development Fellow, in a program established by USCYBERCOM Commander General Paul Nakasone.