2013

The George W. Bush Defense Program: Policy, Strategy & War

Tate Westbrook

Follow this and additional works at: https://digital-commons.usnwc.edu/nwc-review

Recommended Citation
Available at: https://digital-commons.usnwc.edu/nwc-review/vol66/iss1/12

This Book Review is brought to you for free and open access by the Journals at U.S. Naval War College Digital Commons. It has been accepted for inclusion in Naval War College Review by an authorized editor of U.S. Naval War College Digital Commons. For more information, please contact repository.inquiries@usnwc.edu.
There is no lack of analysis and opinions when it comes to the presidency of George W. Bush, particularly now, during an election year. However, the concise and competent analysis found in this work provides an objective review of that pivotal period in history, one that helps the modern reader draw valuable insights applicable to America’s defense acquisition process and to the foreign policy and global strategy of the United States going forward.

Stephen Cimbala, distinguished professor of political science at Penn State Brandywine, has assembled a series of eleven essays by leading academics and analysts of the military-industrial complex, who provide assessments of President Bush’s defense policy and strategy. This scholarly but thoroughly readable collection examines preparations for, and the execution of, war and regime change in Iraq, success and stalemate in Afghanistan, and the sobering effects of “transformation” on the Department of Defense. Additional insights into struggles within NATO and its relationship with the United States, the U.S. relationship with Russia, the critical issues of nuclear proliferation and terrorism, and the implications of foreign military sales complete this collection.

The editor sequenced the essays to provide first the context of the times, the political pressures, and the personalities of key members of the administration. These contextual essays are prefaced by an erudite commentary on defense planning, including the brilliant takeaway that the oxymoron “foreseeable future” deprecates the ability of planners to make reliable resource-allocation decisions. This chapter alone makes the book worthy of a place on the unofficial list of “books to read before reporting to a Pentagon tour.” The essays follow with a critical (if sometimes unnecessarily pejorative) look at Secretary of Defense Donald Rumsfeld’s behavior and his management of the department, along with the successes and failures of “transformation.” Afghanistan and Iraq are closely examined in several essays, in which are documented examples of Secretary Rumsfeld’s overreaching policies, his broken faith with uniformed leaders, and the systematic abuse of intelligence data used to fabricate the case for invading Iraq.

Subsequent chapters address future-oriented defense strategy and policy topics that were germane during the Bush presidency and continue to have implications now. One essay examines the primary questions facing the NATO alliance, including out-of-area missions and the ongoing debate regarding burden sharing among member states as they transition the institution from a posture of collective defense to one of collective security. This is followed by three essays that address arms-transfer policies and foreign military sales, weapons of mass destruction security, and U.S.-Russian nuclear arms control and missile defense.

This book will appeal to military and political scholars, but it also will be immensely appealing to the novice seeking insight into the national defense decision-making process. The lessons provided in this study are
directly applicable to current and future decision makers in the Pentagon, on Capitol Hill, and in the White House.

COMMANDER TATE WESTBROOK, USN
Assistant Director to the Deputy Assistant Secretary of the Navy—Financial Management and Budget (DASN-FMB)


This new collection of cyberspace policy essays includes the works of fourteen scholars and thinkers who present a panoply of views into how cyberspace can be contemplated as policy, doctrine, and strategy. The essays are not U.S.-centric but include focused views of Russian and Chinese thought on the domain, as ably presented by Nikolas Gvosdev and Nigel Inkster, respectively. Additionally, James Joyner provides an excellent synopsis of American and European Union thinking on cybersecurity and how these differing approaches affect not only national-level policy but also the debates within NATO. These perspectives lend texture to the questions of how cyberpower may be considered and how cyberpolicy may be crafted to be both credible and effective.

A section focuses on the legal aspects of cyberspace operations and the potential pitfalls of policy development. It pays particular attention to the concept of deterrence—an area that baffles policy thinkers and technical mavens equally. Of particular use is David Fidler’s chapter, which provides useful terminology and definitions that help the layperson participate in legal-focused discussions on the cyberspace domain.

Derek Reveron’s editing deserves specific and laudatory mention. Rather than merely a collection of articles arranged by topic, he has produced a broad web of writings that shows the interaction of varied scholarly efforts, makes few restatements of the same facts, and brings the volume as a whole to bear on a variety of subtopics.

Steven Bucci’s “Joining Cybercrime and Cyberterrorism: A Likely Scenario” lays out a useful rubric for understanding the operational environment of cyberspace and employs time-tested “most dangerous/most likely” threat-evaluation analysis. This chapter would be of particular benefit to planners and leaders looking to develop “tabletop” or other training events that would focus leaders on specific threats and the action, reaction, and counteraction options available to them.

Chris Demchak writes about “cybered conflict,” which I thought to be a most remarkable approach of how cyberspace should be contemplated in national security, either as a domain or as discrete operations. In it she raises the point that all conflict from now on will have some degree of cyberspace flavor. However, very little will actually be dominated by or within this domain. The key is how best to integrate cyberspace into a coherent strategy, recognizing cyberspace’s varied role. Her use of the term “cybered” is not random. It is a useful modifier and connotes “all sorts of systems of people, things, processes, and perceptions that are computer-related but not necessarily purely computerized.” More than any