

2001

The Changing Role of Information in Warfare,

Eric J. Dahl

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

Recommended Citation

Dahl, Eric J. (2001) "The Changing Role of Information in Warfare," *Naval War College Review*: Vol. 54 : No. 3 , Article 18.
Available at: <https://digital-commons.usnwc.edu/nwc-review/vol54/iss3/18>

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.

handling of chemically contaminated casualties.

In the end, this work comes off as not much more than a “*hoo ah*” for the Army Chemical Corps, who are billed as having redeemed the Department of Defense’s collective ineptitude with respect to chemical or biological attack. While Mauroni does offer an accurate overall accounting of the Army Chemical Corps’s efforts to deal with the asymmetrical threat of chemical and biological agents on the battlefield, he gives little more than a passing nod to the overall efforts of the other services and their collective attempts to counter or mitigate this omnipresent threat. Readers familiar with the subject of WMD should be cautioned that there is much with which to find exception in this work. Readers unfamiliar with the subject should be careful not to conclude that the capabilities of the Department of Defense are so uniformly one-sided.

PIETRO D. MARGHELLA
Lieutenant Commander
Medical Service Corps, U.S. Navy



Khalilzad, Zalmay M., and John P. White, eds.
The Changing Role of Information in Warfare. Santa Monica, Calif.: RAND, 1999. 452pp. \$25

Is there need for yet another book on the role of the military in the information age? To judge by this volume, a collection of essays published under RAND’s Project Air Force, the answer is yes—but this may be twice the book we need. In this case, more than enough is not necessarily better.

The Changing Role of Information in Warfare is part of RAND’s Strategic Appraisal series, and it primarily addresses the effects of information technology on

American military planning and operations. The fifteen chapters provide a useful review of the dangers and opportunities that information technology presents to U.S. military forces. While originally intended for the Air Force, the work should interest a wider professional audience, especially because it includes a broad spectrum of views, ranging from techno-optimists to info-war pessimists.

The editors are well regarded authorities: Zalmay Khalilzad is a former assistant deputy under secretary of defense for policy planning, and John White is a former deputy secretary of defense. Many of the articles were written by well-known writers on strategy and information warfare, and the foreword is by Andrew W. Marshall, Director of Net Assessment, Office of the Secretary of Defense; he is considered by many to be among the foremost thinkers in the U.S. government on future threats and strategies.

However, roughly half the articles cover ground familiar to anyone who has been following the discussion in recent years about the importance of information in warfare and the dangers of computer warfare. These chapters might be useful, for example, to someone looking for a review of the various ways computer hackers can disrupt military operations. But because so much has been written on this constantly changing topic, the more technical chapters do not cover much new territory and are already slightly outdated.

The chapter on information-age terrorism, for instance, warns that future terrorist attacks may take the form of “cybotage” aimed at information infrastructure. This may be true, although it hardly is a new idea; moreover, so far in the information age, old-fashioned terrorism remains dominant, as the attack on the USS *Cole* reminded us.

Similarly, the chapter on U.S. strategic vulnerabilities discusses the tentative steps being taken at the national level to deal with the information warfare threat—but it has been dated by more recent efforts at information warfare defense, including the Clinton administration's National Plan for Information Systems Protection, published after this book went to press.

Luckily, only about half the book discusses the familiar territory of information systems and technology. The second half examines many of the broader questions involved in how the U.S. military is adapting to the information age.

One of the best chapters is "The American Military Enterprise in the Information Age." The late Carl H. Builder argues that the most important effect of the information revolution may not be the application of technology to existing missions but the need for the military to adapt to, and find, new and different missions.

For Builder, it appears that the American military's "enterprise"—its primary purposeful activity—is no longer (if it ever was) to "fight and win our nation's wars." Deterrence and forward defense will not play the central roles they did in twentieth-century conflicts, he speculates, so the military may find itself reduced to providing constabulary and expeditionary capabilities, while keeping the military arts and sciences alive for the future.

Jeremy Shapiro takes a skeptical approach to the entire concept of an "information revolution." He argues that the information age is not producing the sort of wholesale change we would expect from a revolution, either in military affairs or in society at large. He cites the work of Stephen Biddle and others who have described the "productivity

paradox"—the idea that the outlays for information technology have not as yet led to the increases in productivity that would be expected in a social and economic revolution.

If the change is not revolutionary, Shapiro argues, the U.S. military should not hasten to make radical organizational or other changes. He quotes approvingly Eliot Cohen's observation that the creation of a corps of "information warriors" today might make as little sense as would the creation of a corps of internal-combustion warriors in the last century.

A chapter by Stephen T. Hosmer offers a welcome look at psychological operations (PSYOP), an important aspect of information warfare that is usually neglected by all but the U.S. Army. Army PSYOP advocates may not like what they read here, however. Hosmer argues that although psychological effects are indeed vital, history shows that actual PSYOP efforts are not nearly as effective in reducing the enemy's will to fight as are well-planned combat operations. Standard measures of psychological warfare effectiveness, such as the numbers of enemy surrenders and desertions, do not correlate directly with the intensity or quality of PSYOP efforts but closely reflect the nature of combat operations.

Military commanders can best produce catastrophic disintegration of enemy resistance, Hosmer writes, not through leaflets and loudspeaker broadcasts but by sustained, weeks-long air and artillery attacks combined with deliberate efforts to deprive the enemy of food, and ultimately with ground operations aimed at exploiting the enemy's weakened morale. His advice may appear obvious, but it suggests that commanders may be paying too much attention to technical PSYOP efforts and not enough to the psychological

effects of combat operations. In addition, his research seems to suggest that sustained, well-planned strikes may be more important than the sudden mass attacks designed to produce “shock and awe” that are heralded by many network-centric-warfare advocates.

Additional useful chapters review the ethical considerations arising in information warfare and examine whether or not such mechanisms as arms control and export regimes can apply to information warfare technologies. An article by Francis Fukuyama and Abram N. Shulsky reviews the lessons (familiar to a Naval War College audience) that the military can learn from business in adapting to the information age.

One minor complaint—the book does not offer biographical sketches of the contributors. A few pages devoted to that information would be more useful than the largely unnecessary listing of abbreviations and acronyms. Overall, this collection is useful, but a better introduction to many of these concepts is found in an earlier RAND work by John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (1997) [reviewed in the Spring 1999 issue].

ERIC J. DAHL
Commander, U.S. Navy
Naval War College



Szayna, Thomas S. *Identifying Potential Ethnic Conflict*. Santa Monica, Calif.: RAND, 1998. 329pp. \$25

Since 1989, the U.S. military has been involved in a number of intrastate conflicts integrally related to ethnicity. These ethnic conflicts have been devastating to those involved; the conflicts contributed

to regional destabilization; and they have been assumed to breed international terrorism. Most saliently, they have virtually destroyed the hope of peace benefits that were predicted to accrue at the end of the Cold War.

The intelligence community was tasked by the State and Defense Departments to provide explanations for ethnic conflict. Indications-and-warning systems were to be developed and used to alert policy and military decision makers to impending crises. It was assumed that good analysis and prediction would contribute to policies and practices designed to prevent, manage, or contain ethnic conflict and thereby minimize damage to international peace and stability. A number of studies were conducted internally or were outsourced. The task was apparently, but deceptively, simple—produce a predictive model of ethnic conflict. The criterion for a successful model was equally simple—did it work? That is, did the model provide more information of a critical nature than could be provided by country experts, and was it available in a timely fashion?

Identifying Potential Ethnic Conflict is the public report of research sponsored by the deputy chief of staff for intelligence of the U.S. Army. It was produced by a group at the top level at RAND Corporation in Santa Monica, California.

The stated purpose of the project was to help the intelligence community order its thinking about the logic and dynamics of ethnic conflict and to systematize information-collection requirements. The authors did not provide a comprehensive explanation of ethnic conflict but attempted to answer the questions of how ethnic mobilization occurs and under what conditions it leads to violence.