Gregory J. Rattray

Strategic Warfare in Cyberspace

Strategic Warfare in Cyberspace

Gregory J. Rattray

The MIT Press
Cambridge, Massachusetts
London, England

This book was set in ITC Garamond by Best-set Typesetter Ltd., Hong Kong.

Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Rattray, Gregory J., 1962–
Strategic warfare in cyberspace / Gregory J. Rattray.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-262-18209-6 (hc. : alk. paper)
1. Information warfare. 2. Strategy. 3. United States—Military policy. I. Title.
U163 .R29 2001
355.3′43—dc21 00-046061

10 9 8 7 6 5 4 3

Contents

Preface vii

Introduction 1

ONE Delineating Strategic Information Warfare: Key Concepts, Boundaries, and Operating Environment 7

TWO Understanding the Conduct of Strategic Information Warfare 77

THREE Establishing Organizational Technological Capacity for Strategic Information Warfare 163

FOUR Development of U.S. Strategic Airpower, 1919–1945: Challenges, Execution, and Lessons 235

FIVE The United States and Strategic Information Warfare, 1991–1999: Confronting the Emergence of Another Form of Warfare 309

SIX Conclusion 461

Epilogue 481

Acronyms 497

Index 503

Preface

I am an unlikely "digital warrior." When I entered the Air Force Academy in 1984, I was determined to become a fighter pilot after getting my degree in aeronautical engineering. As it turned out, I quickly realized that understanding the interaction of technology, national security policy, and military power held a much greater fascination for me, and I majored in political science and history. I subsequently spent much of the first portion of my military career as an intelligence officer dealing with problems of nuclear deterrence, arms control, and the challenges presented by the proliferation of weapons of mass destruction.

As the Soviet threat waned and the United States remained engaged on the world stage, I became aware that the nature of conflict and the role of the U.S. military was likely to shift dramatically in the coming years. After returning to Colorado Springs to teach at the Air Force Academy, I happened upon the Tofflers' *War and Anti-War* in a local bookstore. I was captured by their depiction of the forces that were beginning to reshape aspects of our profession and felt compelled to teach cadets and myself more about this transformation. I soon realized that grasping the subject required a greater breadth of knowledge than provided by my past academic and military background.

When the Air Force allowed me to return to graduate school to pursue a doctoral degree, I decided to deepen my exploration of "information warfare." Study and research provided me insight into the fundamental import of the subject while increasing my concern about how we understand this emerging form of conflict. Working on the Headquarters Air Force staff for two years only reinforced my conviction that we must ground our policy decisions, military reorganization, and resource investment in historical context and detailed analysis. These interests and experiences afforded me the opportunity and motivation to write this book. I hope it helps others comprehend the complexities,

opportunities, and challenges presented for waging strategic warfare in cyberspace as we enter the twenty-first century.

I am deeply indebted to a great number of people for their accumulated learning, insight, and support. While a Ph.D. student, the committee that supervised my work provided an invaluable mix of wisdom and support. Professor Anthony G. Oettinger, Director of the Program on Information Resources Policy at Harvard University, offered a continual source of stimulating ideas, challenging feedback, and a deep well of reassurance about the value of my work. Professors Robert L. Pfaltzgraff, Jr., and Richard H. Shultz, Jr., at the Fletcher School of Law and Diplomacy at Tufts University were unflagging in their encouragement, patience, and guidance. I also received a great deal of support from others who gave their time to improve this work. The following individuals provided feedback on significant portions of this book: Dr. Dan Kuehl, School of Information Warfare and Strategy at National Defense University; Larry Rothenberg, Institute for Foreign Policy Analysis; Capt. Jason Healey (USAF) of the Joint Task Force—Computer Network Defense; and my parents, John and Virginia Rattray. Captain Richard P. O'Neill (USN ret.) was willing to engage me in a series of discussions that greatly improved my focus on the most important issues for the nation's future security and insight into how the defense bureaucracy was coping with these challenges. It would be impossible to thank everyone else whose insights and challenges improved my work. Those not mentioned here know who they are and have my thanks.

I also need to thank the editorial staff at MIT Press and, in particular, Michael Harrup. His eye for detail and sense of clear exposition have strengthened the argument presented in this book while the easing the reader's task of trying to understand a complex subject.

I must also thank two institutions for their support in my midcareer sojourn. The Department of Political Science at the Air Force Academy sponsored my Ph.D. program. The U.S. Air Force Institute for National Security Studies provided generous financial support to conduct research trips and interviews instrumental to the analysis and factual support in this work.

Finally my wife, Francesca, has my greatest thanks and love. She dealt graciously with countless inconveniences and frustrations. Even more, she unstintingly provided a daily sounding board for my ideas, an eloquent pen to improve my prose, and a partner who made the experience greatly more worthwhile.

Of course, no matter how much help and guidance others provided, errors of fact or interpretation are my sole responsibility. The reader must also remem-

ber that the views expressed in this work are the personal opinions of the author and do not represent the official positions of the Air Force, the Department of Defense, or the government of the United States.

Introduction

An Emerging Challenge

The United States is leading the world into an era often called "the information age." Developments such as the cellular phone, satellite TV, and personal computers with modems, faxes, the Internet, and the World Wide Web have made the world a much more interconnected place. The growing convergence of computer and communications technologies utilizing digital means for processing, transmitting, and storing information has revolutionized activities across society. The media have jumped on the bandwagon with almost daily features about the new world of "cyberspace." The business pages are filled with news about telecommunications and information technology deals and mergers. The U.S. government is endeavoring to create national and global "information infrastructures" while trying to decide on its role in regulating an explosion of activities in new areas. Many commentators have focused on how "information highways" will be paved with gold and good intentions. However, as the international environment adjusts to the end of the Cold War, a realization has dawned that this information age will also have a dramatic impact on security affairs.

As the Soviet empire fell into decline, a number of events highlighted the growing influence of information technology on national security. Successful integration of information systems in a sophisticated conventional force capability proved decisive during the spectacular U.S. military successes in the Gulf War. U.S. military involvement in Somalia and the Balkans has demonstrated the influence of increasingly global media coverage. At home, activities of hackers and systems failures affecting crucial institutions, such as the air traffic control system, the banking system, and the Department of Defense, have increased worries that a whole new type of national security threat may be emerging. Information systems may now serve as both weapons and targets.

Increasingly, these emerging national security concerns receive attention under the rubric of "information warfare." Futurists have outlined how a transition to a "third wave" information-based society has crucial implications for waging both war and peace. As the millennium ended, the Department of Defense and the military services were working vigorously on incorporating the impact of the information age into doctrine, operations, and organizations. At the same time, potential adversaries face a huge challenge in confronting the U.S. on the conventional battlefield and may pursue new approaches for waging conflict with the world's sole superpower.

Adversaries might choose to disrupt information infrastructures as a means of achieving political influence vis-à-vis the United States. Warnings of an impending "electronic Pearl Harbor" have been sounded. By 1996, the U.S. National Security Strategy stated that "the threat of intrusions to our military and commercial information systems poses a significant risk to national security."[1] Congress has focused attention on possible threats from digital attack and called for presidential action. Efforts by the Justice Department and FBI to deal with terrorism also now stress the "cyber" threat. Growing concern about this threat resulted in a Presidential Decision Directive addressing critical infrastructure protection. U.S. national security institutions enter the twenty-first century adapting to the challenges posed by potential threats arising from growing reliance on information infrastructures. The significance of commercial ownership and cooperation for developing an effective U.S. national strategy to protect such infrastructures has been recognized. However, the establishment of adequate mechanisms to bridge public and private interests has confronted difficult tradeoffs such as that involved in establishing a national policy on the control of encryption technology.

Yet in all this flurry of interest and activity, frameworks for evaluating the capabilities of international actors to conduct conflicts based on attacking information infrastructures remain underdeveloped. Treatments of information warfare are overly broad. The "information warfare" rubric includes concepts ranging from straightforward destruction of communications between commanders and fielded military forces to "simula-warfare," positing that computer simulations could prove to an enemy that it would lose a real war. Most discussions make little distinction between activities traditionally segregated by categories of peace and war.

Discussions of information warfare also make little reference to the history of strategic warfare. Numerous studies detail the ease of attacking information infrastructures and the widespread availability of digital means for attacks. These

studies, however, pay little heed to the relationship between ends sought and the utility of information warfare as a means of achieving these ends. Moreover, those who address information warfare generally gloss over the hurdles presented in adapting organizations and policies to deal with new technologies. The challenges of understanding fast-changing information infrastructures developed and operated outside the control of military institutions receive little attention. Academic treatments of, and government efforts to deal with, information warfare inadequately address trade-offs involved between commercial competitiveness, personal rights, and security concerns. The advent of an information age clearly has pervasive effects on security issues and its impact on warfare must be analyzed in a holistic fashion.

Overview of Contents

This work represents an effort to grapple with strategic information warfare as a distinct concern for the United States and other actors in the international system at the dawn of the twenty-first century. The analysis endeavors to provide frameworks to enable a deeper understanding of an emerging national security concern.

Chapter 1 delineates the possibility of "strategic" information warfare as a new means by which international actors may wage war by directly attacking an adversary's information infrastructures. My work focuses on the use of remote digital attacks as a new type of micro force for adversaries engaged in conflicts that can be analyzed with constructs used to address conventional and nuclear force. Distinctions are drawn between strategic information warfare and other types of information-based competition, such as financial crime and economic espionage. This chapter also provides a baseline regarding the nature of information infrastructures and their significance for the United States as potential centers of gravity for strategic attack. The analysis identifies implications of salient features of advanced information infrastructures—complexity of interconnection; civilian-sector technological leadership; dynamic change; and global interconnection, operation, and production—for the conduct of strategic information warfare. The chapter concludes by identifying how the distinct nature of the cyberspace operating environment will potentially affect warfare in this realm.

Chapter 2 extends past conceptualizations of the use of force and strategic warfare. A review and critique of the theoretical development and historical record provides an understanding of the beguiling aspects of strategic warfare

and the difficult challenges involved in achieving desired effects. This analysis serves as a basis for establishing a framework of four enabling conditions for the successful conduct of strategic warfare:

1. Offensive freedom of action
2. Significant vulnerability to attack
3. Minimal prospects for retaliation and escalation
4. Ability to identify and target an adversary's centers of gravity

The second half of the chapter details potential strategic information warfare technologies and approaches. The analysis highlights factors such as the dual-edged nature of strategic information warfare tools, the speed of interaction, ambiguities involved in characterizing digital attacks, and the crucial role of intelligence. The chapter concludes with a framework for evaluating the utility of strategic information warfare.

Chapter 3 addresses the requirements for creating organizational technological capability to wage strategic information warfare. The nature of technology and technological mastery are analyzed to provide a baseline for delineating these requirements. Five facilitating factors for the establishment of organizational technological capability are identified:

1. Supportive institutional environment
2. Demand-pull motivation
3. Management initiative
4. Technological expertise
5. Learning ability

Using this framework the chapter analyzes a set of challenges previously overlooked for establishing strategic information warfare capabilities. Tools for digital warfare may be easy to acquire and unleash, but establishing offensive capabilities requires developing the requisite expertise to target attacks and assess the political consequences of information infrastructure disruption. Defensively, difficult challenges face the coordination of activities normally considered outside the national security realm. The political character of an actor will heavily influence its information infrastructure development and vulnerability to strategic information warfare. Crucial policy trade-offs for the United States will involve economic competitiveness and individual rights. Nonstate actors have significant advantages in minimizing their vulnerabilities to digital attack.

Chapter 4 steps back in time to analyze U.S. efforts in the period between World War I and World War II to develop strategic thinking, military organizations, and the technological capability to conduct long-range bombing as a means for prosecuting strategic attacks against industrial infrastructures. The facilitating factors developed in chapter 3 help explain why, despite strong doctrinal advocacy and the rapid emergence of technological tools, the overall adaptation of the U.S. military establishment to leverage strategic bombing capabilities occurred slowly. The halting process of organizational change and struggles for resources necessitated that the Army Air Corps sharpen its ideas about the possibilities and requirements for U.S. airpower. The analysis details how a convergence of doctrine, organizational structure, and technological conditions in the mid-1930s resulted in a strong commitment to strategic air warfare based on unescorted, daylight precision bombing by U.S. airmen. This commitment largely blinded U.S. air leaders to experiential lessons in China, Spain, and England, as well as to technological developments such as radar and capable interceptors. Doctrinal "lock-in" initially proved very detrimental during U.S. strategic bombing campaign against Germany in World War II.

Chapter 4 also describes how effective defenses and early failures faced by the United States were eventually overcome through a combination of good fortune, material superiority, and effective adaptation. Utilizing the framework of the four enabling conditions developed in chapter 2, underlying problems are identified as lessons that should inform those who would consider waging strategic information warfare attacks. Lessons include the great difficulty the United States had in identifying German centers of gravity and understanding the adaptability of German infrastructures to air attack.

Chapter 5 provides a detailed analysis of U.S. efforts in the period between 1991 and 1999 to develop the necessary doctrine, organizations, and technological capability to conduct strategic information warfare, focusing on the defensive concerns. Important similarities to the previous development of air bombardment capabilities are pointed out. The possibility of strategic information warfare has severely stressed military institutions to fit new missions into organizational constructs and reallocate limited resources. Continuing inquiries about the new form of warfare, such as those conducted by the Defense Science Board, Congress, and the President's Commission on Critical Infrastructure Protection have increased understanding of U.S. vulnerabilities to digital attacks. The forces driving commercial technological leadership, ownership, and control of the cyberspace environment have hampered efforts to reach a consensus regard-

ing the proper balance of national security, commercial competitiveness, and privacy concerns. The analysis in chapter 5 delves into the role played by commercial technology producers in pouring weak technological foundations for U.S. infrastructure protection and the importance of properly managing limited human resources in dealing with decentralized defensive tasks.

The concluding chapter endeavors to bring together the principal threads of theoretical analysis and experiential lessons. The book concludes with recommendations for strengthening U.S. strategic information warfare defenses.

Note

1. White House, *National Security Strategy* (Washington, DC: Government Printing Office, 1996), 13.