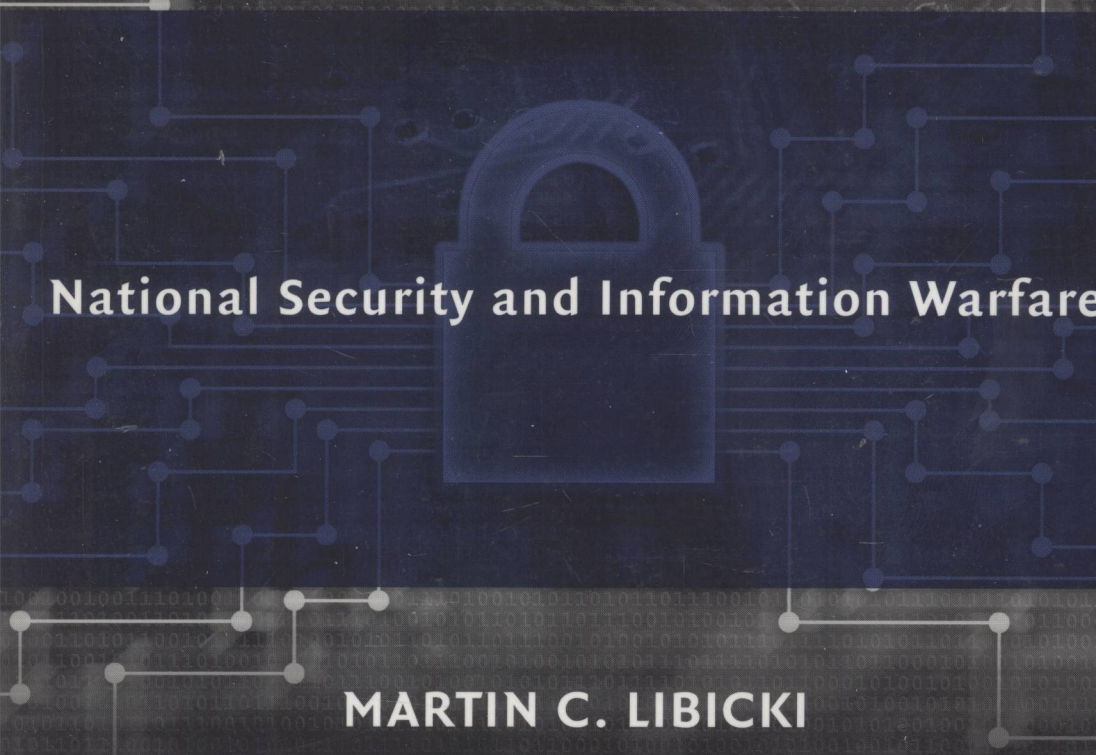
CONQUEST IN CYBERSPACE



National Security and Information Warfare

MARTIN C. LIBICKI

CAMBRIDGE

Conquest in Cyberspace

National Security and Information Warfare

MARTIN C. LIBICKI
The RAND Corporation

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521871600

First published 2007

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication Data

Libicki, Martin C.
Conquest in cyberspace : national security and information warfare / Martin C. Libicki ;
RAND Corporation.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-521-87160-0 (hardback)
ISBN-13: 978-0-521-69214-4 (pbk.)
1. Information warfare. 2. National security. 3. Cyberterrorism.
4. Computer networks – Security measures. I. Rand Corporation II. Title.
U163.L534 2007
355.3′43 – dc22 2006030973

ISBN 978-0-521-87160-0 hardback
ISBN 978-0-521-69214-4 paperback

CONQUEST IN CYBERSPACE

The global Internet has served primarily as an arena for peaceful commerce. Some analysts have become concerned that cyberspace could be used as a potential domain of warfare, however. Martin C. Libicki argues that the possibilities of hostile conquest are less threatening than these analysts suppose. It is in fact difficult to take control of other people's information systems, corrupt their data, and shut those systems down. Conversely, there is considerable untapped potential to influence other people's use of cyberspace, as computer systems are employed and linked in new ways over time.

The author explores both the potential for and limitations to information warfare, including its use in weapons systems and in command-and-control operations as well as in the generation of "noise." He also investigates how far "friendly conquest" in cyberspace extends, such as the power to persuade users to adopt new points of view. Libicki observes that friendly conquests can in some instances make hostile conquests easier or at least prompt distrust among network partners. He discusses the role of public policy in managing the conquest and defense of cyberspace and shows how cyberspace is becoming more ubiquitous and complex.

Martin C. Libicki, a senior policy analyst at the RAND Corporation since 1998, works on the relationship between information technology and national security. He has written numerous monographs on the subject, notably *What Is Information Warfare, The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon,* and *Who Runs What in the Global Information Grid.* Dr. Libicki is also the editor of the RAND textbook *New Challenges: New Tools for Defense Decisionmaking.* His most recent assignments at RAND have been to generate novel information system capabilities for counterinsurgency and to develop a post-9/11 information technology strategy for the U.S. Department of Justice and the Defense Advanced Research Projects Agency's (DARPA) Terrorist Information Awareness program; to conduct an information security analysis for the FBI; to investigate targeting strategies of al Qaeda; and to assess the CIA's research and development venture, In-Q-Tel. He previously worked at the National Defense University, was on the Navy Staff as program sponsor for industrial preparedness, and was a policy analyst for the Government Accountability Office's Energy and Minerals Division. Dr. Libicki received his Ph.D. from the University of California at Berkeley in 1978.

Acknowledgments

Perhaps the greatest joy in working for the RAND Corporation is the opportunity to work with interesting, intelligent, and inquisitive colleagues. When collaboration works, and it often does, it is far easier to determine with whose pen thoughts were rendered in English than to discern from whose mind such thoughts came. Three such colleagues merit note here, not least because this manuscript would never have been written without them.

James Mulvenon suggested that we work together on a project to define exactly what information warfare (IW) is. The trick in such endeavors is to hew to the art of the technically possible, without, at the same time, basing theory on the evanescent characteristics of today's information technology. Chapters 2, 3, and part of 11 arose from our joint work. We also worked together on another project that looked at what light a theory of command and control could shed on information warfare. Chapter 5 reflects that work.

David Frelinger arranged for us to think systematically about what an information warfare attack on an integrated air defense system (IADS) would look like. The question was prompted by inquiries over whether one could quantify the effects of information warfare on an IADS with as much confidence as one could for the effects of electronic or physical warfare. Short answer: no. Chapter 4, which deals broadly with information warfare against critical systems, grew out of the initial efforts to explain why not.

Laurent Murawiec led me into other chapters of the manuscript through a joint project that looked for a theory of command and control

of the sort that the Pentagon's Office of Net Assessment could use. Under his prompting, I developed the material that now constitutes parts of Chapters 1, 6, 8, and 10.

Big thanks are also due to those who reviewed and commented on the manuscript in its various incarnations: Paul Davis, Robert Klitgaard, Shari Lawrence Pfleeger, Charles Wolf, all at RAND, and Professor Anthony Oettinger of Harvard. In addition, Judy Lewis and Lisa Sheldone at RAND have been an invaluable source of assistance and support in making the review and publishing process work well.

Contents

List of Figures

1

Introduction

Despite its roots in the U.S. Department of Defense (DoD), the global Internet has primarily, although not exclusively, been an avenue and arena of peaceful commerce. With every year, an increasing percentage of the world's economy has migrated from physical media, or older electronic media such as telephones and telegraphs, to the public Internet and to private or semipublic internets. Systems that were once inaccessible to persons off-premises, such as power plant controls, are now theoretically accessible to anyone around the world. Other hitherto self-contained networks, such as those that transferred money, are now commingled with the larger, more public networks such as the Internet or the international phone system.

Indeed, its very success is what has turned the Internet into a potential venue of warfare. It is not only that defense systems of advanced militaries are being knit into more powerful systems of systems – thereby becoming the militaries' new center of gravity. The real impetus is that the more cyberspace is critical to a nation's economy and defense, the more attractive to enemies is the prospect of crippling either or both via attacks on or through it. Hackers can and do attack information systems through cyberspace. They can attack the cyberspace itself through operations against the networks that provide the basis for this new medium. Defenders thus must keep these hackers out of their systems. If hackers get in, they could wreak great damage. At a minimum they might steal information. Worse, they can make systems go haywire. Worst, they could inject phony information into systems to distort what users think they absorb when they deal with systems. Hackers might take over any

machine (such as a pump) controlled by a networked computer system and use it according to their ends and not those of its owners.

None of this requires mass, just guile. For that reason, attacks in cyberspace do not need the same government backing as attacks in older media do. Any group, or even individual, can play – even, perhaps especially, terrorists. Prior to 9/11, in fact, it was difficult to conceive of a strategic attack on the U.S. homeland by nonstate actors *except* through the medium of cyberspace. Such would be a bloodless attack from afar that left no traces but could cause the systems we rely on to crash mysteriously. The President's Commission on Critical Infrastructure Protection argued in 1996 that the capability to launch such an attack did not yet exist – but given five years (that is, by 2001), it very well might.

Perhaps needless to add, although advanced nations have more at stake in cyberspace than developing nations do, the latter are increasingly being drawn into its domain. Thus, they too are vulnerable to attacks from what are, in general, the larger and more sophisticated cohorts of hackers from the first world.

By such means, cyberspace has joined air and outer space as a new medium of conflict.[1] Granted, evidence that it has become a *significant* medium of conflict is sparse. This may be because the last three wars in which cyberspace could have played a role – Kosovo, Afghanistan, and Iraq, respectively – were against countries with minimal presence in cyberspace. They had little that the United States could attack, or at least attack more efficiently than conventional means already permitted it to do. So far, other countries have lacked the sophistication and will to do much damage to the U.S. use of cyberspace. But since participation

[1] The 2001 Department of Defense Quadrennial Defense Review Report listed four "Key Military–Technical Trends." The third was "Emergence of new arenas of military competition":

> Technological advances create the potential that competitions will develop in space and cyber space. Space and information operations have become the backbone of networked, highly distributed commercial civilian and military capabilities. This opens up the possibility that space control – the exploitation of space and the denial of the use of space to adversaries – will become a key objective in future military competition. Similarly, states will likely develop offensive information operations and be compelled to devote resources to protecting critical information infrastructure from disruption, either physically or through cyber space (p. 7).

in and dependence on cyberspace is growing, the odds of consequential conflict, and thus hostile conquest, must certainly be rising.

Lost in this clamor about the threat from hackers is another route to conquest in cyberspace, not through disruption and destruction but through seduction leading to asymmetric dependence. The seducer, for instance, could have an information system attractive enough to entice other individuals or institutions to interact with it by, for instance, exchanging information or being granted access. This exchange would be considered valuable; the value would be worth keeping. Over time, one side, typically the dominant system owner, would enjoy more discretion and influence over the relationship, with the other side becoming increasingly dependent. Sometimes the victim has cause to regret entering the relationship; sometimes all the victim regrets is not receiving its fair share of the joint benefits. But if the "friendly" conquest is successful, the conqueror is clearly even better off.

The central contention of this work is that the possibilities of hostile conquest may be less consequential than meets the eye while the possibilities of friendly conquest ought to be better appreciated. The current obsession with hostile conquest fosters a tilt toward closed systems, at least among those who have powerful systems to begin with. Those with the most attractive systems – in terms of information, knowledge, services, and reach – have an inherent advantage whose benefits they might deny themselves by concentrating on the threat to themselves. This is particularly so for the national and homeland security community (including law enforcement, homeland defense, and infrastructure). By taking a more open approach to cyberspace, they may extend their influence and the influence of their values more certainly than they would by taking a closed approach.

In a sense, this argument echoes the distinction made by Joseph Nye between a nation's hard power and its soft power.[2] Hard power is embodied in military force, soft power in its culture. Hard power, like hostile conquest in cyberspace, ultimately entails one nation doing to another what the other would prefer it not do. It is involuntary. Soft power, like

[2] Joseph Nye, *Bound to Lead: The Changing Nature of American Power*, New York (Basic Books), 1990.

friendly conquest in cyberspace, describes the process of enticement. It is voluntary, at least at first. In the case of soft power, the elites of the affected country may find themselves unable to roll back the tide of imported cultural and economic mores without facing resistance and revolt. But rarely can one nation control or manipulate the instruments of soft power to create such a dependency; more often, it works independent of national strategy. With friendly conquest in cyberspace, however, the seducer retains part of the leverage precisely because the controls over the seductive system are not relinquished.

Hence the choices, many of them public choices. Hence, too, the orientation of this work, one to be understood in its policy and management rather than technical context. It is aimed at educated individuals who are interested in public policy. Admittedly, issues of cyberspace can become quite technical, and so the text tries to clarify some key concepts. Cyberspace issues are not unique in that regard. It can be hard to understand, say, the pros and cons of strategic ballistic missile defense without some understanding of physics. Nevertheless, arguments about strategic defense are not entirely technical ones. Similarly, arguments about the proper use and exploitation of cyberspace are not entirely technical. Readers who happen to be information security experts may appreciate reading this or that point of view; they are unlikely to add much to their technical knowledge of their craft by reading this.

1.1 What Does Conquest Mean in Cyberspace?

This work is entitled not "The Conquest *of* Cyberspace" but "Conquest *in* Cyberspace" for a reason. To emphasize the "of" is to suggest that there is, in fact, *a* cyberspace that exists in the same sense that the oceans do. It has distinct parameters and perimeters, and one can define conquest within this space. This leaves the only interesting question one of determining who has, in fact, taken possession of what part of cyberspace and how they accomplished such feats. Emphasizing "in," by contrast, reflects the fact that while something akin to conquest can be defined for cyberspace, cyberspace itself cannot be conquered in any conventional sense.

To understand why, it helps to understand what cyberspace itself means. Ironically, that process is best begun by discussing what cyberspace does *not* mean – or at least does not mean yet.

The term "cyberspace" was coined in William Gibson's 1984 classic, *Neuromancer.* The concept was further described in compelling detail in Neil Stephenson's 1989 *Snow Crash.* Both portrayed it as an alternative universe that people could participate in ("jack into" pace Gibson). It may be seen, particularly in some movies, as being just on the other side of the twenty-first century's version of Alice's looking-glass. Cyberspace, so defined, may be evoked through a text-only medium such as a chat room, but it can also be evoked more tangibly by a virtual reality simulation in which what one sees, hears, and, to some extent, feels is all synthesized on the spot. Computer power and fat networks make this illusion easier to generate with every passing year.

This often attractive concept should not lead one to imagine cyberspace as being *the* parallel universe – as if a mapping of this reality into another dimension. Four tenets suggest why cyberspace should be understood on its own merits.

First, cyberspace is a replicable construct. Being replicable, it exists in multiple locations at once. Because it is replicable, it is also reparable.

By contrast, only confusion can follow the unconscious assumption that there is *one* cyberspace in the sense that there is, say, one outer space. The existence of a single something called outer space derives from the simple fact that there is a planet earth and that every point on or above the planet has a unique location relative to it. This uniqueness is firmly rooted in physical law. The planet, for instance, has only one geosynchronous belt, and locations[3] in it are carefully allocated for every satellite (of a given broadcast frequency). There is also one spectrum, uses of which are governed by international conventions such as the World Radio Conference. From a military perspective, one nation's fleets of hunter-killer satellites can keep another country from establishing its own constellation. Control in space, can, in theory, be exclusive.

Cyberspace, by contrast, is built, not born. Every system and every network can hold its own cyberspace – indeed, it can hold a limitless number of quasi-independent spaces. Cyberspace can appear in multiple,

[3] Satellites in geosynchronous orbit appear to linger above a single point on the equator. Satellites in such orbits have to be separated from each other by a certain arc length if they broadcast in the same frequencies. As such, there are a finite number of such orbits and each is assigned on a global basis.