

Cambridge University Press

978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare

Martin C. Libicki

Frontmatter

[More information](#)

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.

Cambridge University Press

978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare

Martin C. Libicki

Frontmatter

[More information](#)

Conquest in Cyberspace

National Security and Information Warfare

MARTIN C. LIBICKI

The RAND Corporation



CAMBRIDGE
UNIVERSITY PRESS

Cambridge University Press

978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare

Martin C. Libicki

Frontmatter

[More information](#)

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

© The RAND Corporation 2007

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

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

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party Internet Web sites referred to in this publication and does not guarantee that any content on such Web sites is, or will remain, accurate or appropriate.

Contents

<i>List of Figures</i>	<i>page</i> x
<i>Acknowledgments</i>	xi
1 Introduction	1
1.1 What Does Conquest Mean in Cyberspace?	4
1.2 Précis	10
2 Hostile Conquest as Information Warfare	15
2.1 An Ideal-Type Definition of Information Warfare	16
2.1.1 Control at One Layer Is Not Control at Another	24
2.1.2 Applying the Ideal-Type Definition	27
2.2 There Is No Forced Entry in Cyberspace	31
2.3 Information Warfare Only Looks Strategic	37
2.3.1 IW Strategy and Terrorism	43
2.4 Conclusions	49
3 Information Warfare as Noise	50
3.1 Disinformation and Misinformation	51
3.2 Defenses against Noise	55
3.2.1 Redundancy	55
3.2.2 Filtration	57
3.3 What Tolerance for Noise?	59
3.3.1 Tolerance in Real Environments	60
3.3.2 Castles and Agoras	62

vi	<i>Contents</i>	
	3.3.3 Hopping from Agoras to Castles?	64
	3.3.4 Castling Foes	66
	3.4 Concluding Observations	71
4	Can Information Warfare Be Strategic?	73
	4.1 Getting In	75
	4.2 Mucking Around	79
	4.2.1 Spying	79
	4.2.2 Denial of Service	80
	4.2.3 Corruption	81
	4.2.4 Distraction	83
	4.3 Countermeasures	84
	4.3.1 Redundancy	84
	4.3.2 Learning	85
	4.4 Damage Assessment	87
	4.5 Prediction	90
	4.5.1 Intelligence Is Necessary	90
	4.5.2 Intelligence Alone Is Hardly Sufficient	93
	4.6 Is Information Warfare Ready for War?	95
	4.6.1 The Paradox of Control	96
	4.6.2 Other Weaponization Criteria	97
	4.7 Conclusions	100
5	Information Warfare against Command and Control	102
	5.1 The Sources of Information Overload	103
	5.1.1 Its Effect on Conventional Information Warfare Techniques	105
	5.2 Coping Strategies	107
	5.2.1 Who Makes Decisions in a Hierarchy?	107
	5.2.2 Responses to Information Overload	111
	5.3 Know the Enemy's Information Architecture	116
	5.3.1 Elements of Information Culture	117
	5.3.2 Elements of Nodal Architecture	118
	5.3.3 Injecting Information into Adversary Decision Making	118
	5.4 Ping, Echo, Flood, and Sag	121

	<i>Contents</i>	vii
	5.4.1 Ping and Echo	121
	5.4.2 Flood and Sag	122
	5.5 Conclusions	124
6	Friendly Conquest in Cyberspace	125
	6.1 A Redefinition of Conquest	126
	6.2 The Mechanisms of Coalitions	128
	6.2.1 The Particular Benefits of Coalitions	130
	6.2.2 Information and Coalitions	131
	6.2.3 The Cost of Coalitions in Cyberspace	136
	6.3 Enterprise Architectures and Influence	142
	6.4 Alliances with Individuals	148
	6.4.1 The Special Case of Cell Phones	151
	6.5 Alliances of Organizations	155
	6.5.1 Ecologies of Technological Development	155
	6.5.2 DoD's Global Information Grid (GIG)	159
	6.5.3 Merging the Infrastructures of Allies	164
	6.6 Conclusions	166
7	Friendly Conquest Using Global Systems	169
	7.1 Geospatial Data	170
	7.1.1 Coping with Commercial Satellites	175
	7.1.2 Manipulation through Cyberspace	178
	7.1.3 Getting Others to Play the Game	180
	7.1.4 Some Conclusions about Geospatial Services	182
	7.2 National Identity Systems	182
	7.2.1 Two Rationales for a National Identity System	183
	7.2.2 Potential Parameters for a Notional System	184
	7.2.3 Constraints from and Influences over Foreign Systems	187
	7.3 Compare, Contrast, and Conclude	191
8	Retail Conquest in Cyberspace	193
	8.1 Information Trunks and Leaves	194
	8.2 Where Does Cheap Information Come From?	195
	8.3 Surveillance in Cyberspace	198

viii	<i>Contents</i>	
8.4	Making Information Global	203
8.5	Privacy	204
8.6	Amalgamating Private Information	206
8.7	Using the Information	208
8.7.1	General Coercion	208
8.7.2	Specific Coercion	209
8.7.3	Persuasion	211
8.8	Some Limits of Retail Warfare in Cyberspace	214
8.9	Using Retail Channels to Measure Wholesale Campaigns	215
8.10	Conclusions	218
9	From Intimacy, Vulnerability	220
9.1	Do the Walls Really Come Down?	220
9.2	Intimacy as a Target	222
9.3	The Fecklessness of Friends	225
9.4	Betrayal	228
9.5	Conclusions	230
10	Talking Conquest in Cyberspace	231
10.1	Four Layers of Communications	232
10.1.1	Human Conversation in Layers	232
10.1.2	Cyberspace in Layers	236
10.2	Complexity Facilitates Conquest	240
10.2.1	Complexity and Hostile Conquest	241
10.2.2	Complexity and Friendly Conquest	242
10.3	Semantics	245
10.4	Pragmatics	249
10.5	Lessons?	255
11	Managing Conquest in Cyberspace	256
11.1	Conducting Hostile Conquest in Cyberspace	257
11.2	Warding Off Hostile Conquest in Cyberspace	262
11.2.1	Byte Bullies	262
11.2.2	Headless Horsemen	265
11.2.3	Perfect Prevention	268

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Frontmatter
[More information](#)

<i>Contents</i>	<i>ix</i>
11.2.4 Total Transparency	270
11.2.5 Nasty Neighborhoods	272
11.3 Exploiting Unwarranted Influence	276
11.4 Against Unwarranted Influence	281
11.4.1 In Microsoft’s Shadow	282
11.4.2 Microsoft and Computer Security	285
11.5 Conclusions	289
Appendix A: Why Cyberspace Is Likely to Gain Consequence	291
A.1 More Powerful Hardware and Thus More Complex Software	292
A.2 Cyberspace in More Places	294
A.3 Fuzzier Borders between Systems	297
A.4 Accepted Cryptography	299
A.5 Privatized Trust	301
A.6 The Possible Substitution of Artificial for Natural Intelligence	303
A.7 Conclusions	306
<i>Index</i>	307

List of Figures

1	Attacks on Systems Information Compared to Attacks on Information for People	<i>page 26</i>
2	How Close Do Various Forms of Information Operations Come to a Canonical Definition of Information Warfare?	31
3	Protecting Castles and Agoras	62
4	Degrees of Membership in Closed and Open Organizations	68
5	Responses to Information Overload	116
6	Production Relationships in Cyberspace	156
7	Interoperability at Four Layers	238
8	The Linguistics Analogy: OSI and the Internet Compared	240

Cambridge University Press

978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare

Martin C. Libicki

Frontmatter

[More information](#)

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

Cambridge University Press

978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare

Martin C. Libicki

Frontmatter

[More information](#)

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 Sheldon at RAND have been an invaluable source of assistance and support in making the review and publishing process work well.