

JONES & BARTLETT LEARNING

INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

# Cyberwarfare: Information Operations in a Connected World

MIKE CHAPPLE AND DAVID SEIDL



JONES & BARTLETT  
LEARNING



World Headquarters

**Jones & Bartlett Learning**

5 Wall Street

Burlington, MA 01803

978-443-5000

info@jblearning.com

www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, [www.jblearning.com](http://www.jblearning.com).

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to [specialsales@jblearning.com](mailto:specialsales@jblearning.com).

**Copyright © 2015 by Jones & Bartlett Learning, LLC, an Ascend Learning Company**

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

*Cyberwarfare: Information Operations in a Connected World* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product. The screenshots in this product are for educational and instructive purposes only. All trademarks displayed are the trademarks of the parties noted therein. Such use of trademarks is not an endorsement by said parties of Jones & Bartlett Learning, its products, or its services, nor should such use be deemed an endorsement by Jones & Bartlett Learning of said third party's products or services.

Microsoft, Internet Explorer, Windows, Microsoft Office, Microsoft Security Development Lifecycle, and Microsoft Baseline Security Analyzer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. (ISC)<sup>2</sup>, CISSP, ISSAP, ISSMP, ISSEP, CSSLP, CCFP, CAP, SSCP, and CBK are registered and service marks of (ISC)<sup>2</sup>, Inc.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the service of a competent professional person should be sought.

**Production Credits**

Chief Executive Officer: Ty Field

President: James Homer

Chief Product Officer: Eduardo Moura

SVP, Curriculum Solutions: Christopher Will

Director of Sales, Curriculum Solutions: Randi Roger

Editorial Management: High Stakes Writing, LLC,

Lawrence J. Goodrich, President

Copy Editor, High Stakes Writing: Karen Annett

Product Manager, Custom and Curriculum Solutions:

Rainna Erikson

Associate Director of Production: Julie Bolduc

Rights & Photo Research Manager: Lauren Miller

Manufacturing and Inventory Control Supervisor:

Amy Bacus

Senior Marketing Manager: Andrea DeFronzo

Composition: Gamut+Hue, LLC

Cover Design: Scott Moden

Cover Image: © HunThomas/Shutterstock, Inc.

Printing and Binding: Edwards Brothers Malloy

Cover Printing: Edwards Brothers Malloy

**ISBN: 978-1-284-10789-0**

Library of Congress Cataloging-in-Publication Data not available at time of printing

6048

18 17 16 15 10 9 8 7 6 5 4 3 2 1

# Contents

Preface	xv
Acknowledgments	xix

## **PART ONE** The Cyberwarfare Landscape 1

### **CHAPTER 1** Information as a Military Asset 3

What Is Cyberwarfare?	5
Likelihood of Cyberwar	6
The Evolving Nature of War	8
The Role of Information in Armed Conflict	9
Ancient Warfare	9
World Wars	10
Cold War	12
Iraq War and Weapons of Mass Destruction	12
Domains of Warfare	13
Exploring the Cyber Domain	14
Offensive Information Operations	15
Defensive Information Operations	15
Information Operations Techniques	16
Computer Network Attack	17
Computer Network Defense	18
Intelligence Gathering	18
Electronic Warfare	18
Psychological Operations	19
Military Deception	20
Operations Security	20
<b>CHAPTER SUMMARY</b>	<b>24</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>24</b>

**CHAPTER 2    Targets and Combatants    25**

- Traditional Military Targets    27
  - Military Targets in Conventional Warfare    28
  - Acceptable Targets, Treaties, and International Law    30
  - Cybertargets in Unconventional Warfare    32
  - Targets in Asymmetric Cyberwarfare    32
  - Total Cyberwarfare    33
- Cyberwarfare Targets    33
  - Cyberwarfare Against Traditional Military Targets    34
  - Nontraditional Cyberwarfare Targets    36
- Targets of Information Operations    41
- Combatants in Cyberwarfare    42
  - Military Forces    42
  - Guerrilla Cyberwarriors and Insurrectionists    43
  - Individuals and Small Groups    45
- Comparing Traditional Warfare, Guerrilla Warfare, and Cyberwarfare    47
  - How Cyberattack Differs from Traditional War    47
- CHAPTER SUMMARY    50**
- KEY CONCEPTS AND TERMS    50**

**CHAPTER 3    Cyberwarfare, Law, and Ethics    51**

- Kinetic Warfare    53
  - International Law and Kinetic Warfare    53
- Cyberwarfare Law    55
  - Cyberwarfare in a Kinetic Warfare Context    55
  - Kinetic Warfare Law in a Cyber Context    56
  - The Tallinn Manual    57
  - Sovereignty, Jurisdiction, and Control    58
  - Responsibility    60
  - The Use of Force    63
  - Self-Defense    65
  - Civilians and Infrastructure    66
  - Espionage, Treachery, and Ruses    69
  - Neutrality    69
- Ethics and Cyberwarfare    70
- CHAPTER SUMMARY    71**
- KEY CONCEPTS AND TERMS    71**

## **CHAPTER 4 Intelligence Operations in a Connected World 73**

Intelligence Operations	75
The Intelligence Cycle	75
Intelligence Disciplines	80
Human Intelligence (HUMINT)	80
Signals Intelligence (SIGINT)	83
Open Source Intelligence (OSINT)	84
Geospatial Intelligence (GEOINT)	85
Measurement and Signature Intelligence (MASINT)	87
Intelligence Support to Cyberwarfare	87
Supporting Offensive Cyberwarfare	88
Supporting Defensive Cyberwarfare	88
Case Studies: Media Reporting on Intelligence Activities	89
Echelon	89
Telephone Metadata	89
Data Center Eavesdropping	90
Follow the Money	90
Quantum	90
<b>CHAPTER SUMMARY</b>	<b>91</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>91</b>

## **PART TWO Offensive and Defensive Cyberwarfare 93**

### **CHAPTER 5 The Evolving Threat: From Script Kiddies to Advanced Attackers 95**

The Changing Threat Model	97
Historical Hacking	97
Modern Hacking	98
Inside the Advanced Persistent Threat	101
Characteristics of the APT	102
APT Motivations	103
APT Tradecraft	104
The Cyber Kill Chain®	106
Reconnaissance	106
Weaponize	108
Deliver	109
Exploit	110
Install	111
Command and Control	112
Act on Objectives	114
<b>CHAPTER SUMMARY</b>	<b>115</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>115</b>

**CHAPTER 6 Social Engineering and Cyberwarfare 117**

Humans: The Weak Link	119
Social Engineering	120
Influence as a Weapon	121
Reciprocity	122
Commitment and Consistency	123
Social Proof	125
Authority	125
Liking	127
Scarcity	128
Tools of the Social Engineer	129
Pretexting	129
Phishing	131
Baiting	133
Defending Against Social Engineering	133
Security Awareness and Education	133
Incident Reporting and Response	134
Content Filtering	134
Penetration Testing	135
Robin Sage: A Case Study in Social Engineering	135
<b>CHAPTER SUMMARY</b>	<b>137</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>137</b>

**CHAPTER 7 Weaponizing Cyberspace: A History 139**

Early Attacks: The 1990s	141
Solar Sunrise	141
Moonlight Maze	143
Honker Union	145
The 2000s: The Worm Turns	145
Code Red	146
SQL Slammer	147
Titan Rain	148
Stakkato	148
Poison Ivy	149
Senior Suter	149
Stuxnet and the Twenty-First Century	150
Stuxnet	150
Operation Aurora	151
Duqu	152
Flame	152
FOXACID	153
Careto	154
<b>CHAPTER SUMMARY</b>	<b>155</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>155</b>

**CHAPTER 8 Nonstate Actors in Cyberwar 157**

Understanding Nonstate Actors	159
Nongovernmental Organizations	159
Organized Crime	159
Corporations	160
Terrorists and Activists	161
Individuals and the Media	161
The Roles of Nonstate Actors in Cyberwar	162
Targets	163
Participants	164
Critics	164
Nongovernmental Organizations in Cyberwar	165
Aid Groups	165
Diplomatic Organizations	166
Religious Organizations	167
Organized Crime	167
Corporations	169
Industrial Espionage	169
Cooperation with Intelligence Agencies	170
Terrorists and Activists	171
Estonia	171
Syrian Electronic Army	171
Anonymous	172
Individuals and the Media	173
Individual Motivations	173
Hackers	174
Leakers and Whistleblowers	174
<b>CHAPTER SUMMARY</b>	<b>175</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>175</b>

**CHAPTER 9 Defense-in-Depth Strategies 117**

Defense in Depth	179
Defense-in-Depth Strategies	183
The NSA People, Technology, and Operations Defense Strategy	183
The Department of Defense and Defensive Design	189
Computer Network Defense and Defense in Depth	189
Where and Why Defense in Depth Fails	191
Neglecting Layers: Getting Past the Shell	191
System Administrators: Trusted Attackers	193
Attacking the User: Human Factors	194
Changes in Technology	195
Designing a Modern CND Strategy	196
Dynamic Defense	196

CND and Defense-in-Depth Design	198
Secure Networks	199
<b>CHAPTER SUMMARY</b>	<b>205</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>206</b>

**CHAPTER 10**   **Cryptography and Cyberwar**   **207**

An Introduction to Cryptography	209
Cryptographic Concepts	210
Ciphers and Encryption	211
Symmetric Ciphers	212
Asymmetric Ciphers	215
Modern Cryptosystems	220
Hashing and Message Digests	222
Cryptography in Cyberwar	224
Computer Network Defense and Cryptographic Systems	224
Computer Network Attack and Cryptographic Systems	225
Attacking Cryptography	226
Brute Force	227
Acquiring the Keys	228
Attacking the Algorithm	228
Defeating Attacks on Cryptographic Systems	229
Defenses	230
Defense in Depth Using Cryptographic Systems	230
Weaponizing Cryptography	231
Defensive Cryptography: Malware Encryption	231
Offensive Cryptography	232
The Future of Cryptography in Cyberwar	235
Attacks	235
Defenses	236
<b>CHAPTER SUMMARY</b>	<b>238</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>238</b>

**CHAPTER 11**   **Defending Endpoints**   **239**

Cyberwarfare Endpoints	241
Types of Endpoints	242
Computers	242
Mobile Devices	243
Industrial Control Systems	243
Military Systems	246
Embedded Systems	248
Attacking Endpoints	250



Protecting Endpoints	251
U.S. Department of Defense Strategy	252
Physical Security	254
Policy	254
Procedures	255
Configuration Standards	256
Central Management	256
Awareness	258
Anti-Malware and Antivirus	258
Network Protection	259
Encryption	260
Whitelisting and Blacklisting	261
Testing	264

**CHAPTER SUMMARY** 266

**KEY CONCEPTS AND TERMS** 266

**CHAPTER 12 Defending Networks 267**

Network Defense in Depth	269
Protect, Detect, React	271
Mission Assurance	272
Surviving Attacks	275
Network Operational Procedures	275
Network Security Design	276
Classification	277
Network Defense Technologies	278
Protocols	279
Network Access Control	280
Network Firewalls	280
Network Security Boundaries	283
Intrusion Detection and Prevention Systems	285
Security Event and Information Management Systems	286
Physical Network Protection	286
Wireless Network Security	287
Active Defense	289
Honeypots, Honeynets, and Darknets	290
Active Response	291

**CHAPTER SUMMARY** 292

**KEY CONCEPTS AND TERMS** 292

**CHAPTER 13 Defending Data 293**

Data Classification	295
Data Loss and Prevention	298

- Data Spills 298
- Data Loss Prevention 299
- Encryption and Data Loss 303
- Data Integrity and Availability 305
  - Integrity 306
  - Availability 306
- Data Retention and Disposal 308
  - Data Lifecycle Management 308
  - Drives and Media Management 310
- Data Loss Response 312
- CHAPTER SUMMARY 313**
- KEY CONCEPTS AND TERMS 314**

**PART THREE The Future of Cyberwarfare 315**

**CHAPTER 14 Cyberwarfare and Military Doctrine 317**

- Military Doctrine 319
  - Principles of War 319
  - Forms of Warfare 322
  - Levels of Warfare 323
- Organizing for Cyber Operations 326
  - U.S. Strategic Command (USSTRATCOM) 329
  - U.S. Cyber Command (USCYBERCOM) 329
- Five Pillars of Cyberwarfare 330
- CHAPTER SUMMARY 332**
- KEY CONCEPTS AND TERMS 332**

**CHAPTER 15 Pandora’s Box: The Future of Cyberwarfare 333**

- The Future of Cyberwar 335
- Blurred Boundaries: Cyberwar and Nonstate Actors 337
  - Advanced Persistent Threats 340
  - Continuous Warfare 343
  - Integrating Cyberwar and Kinetic Warfare 345
  - Alliances and Partnerships 346
- International Law and Cyberwarfare 347

Networks Everywhere: Cyberwar in a Highly Connected World	348
Cyberwar and Infrastructure	350
Advanced Tools and Training	351
The Future of Defensive Cyberwar	352
<b>CHAPTER SUMMARY</b>	<b>353</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>353</b>
<b>APPENDIX</b>	
<b>Standard Acronyms</b>	<b>355</b>
<b>Glossary of Key Terms</b>	<b>359</b>
<b>References</b>	<b>371</b>
<b>Index</b>	<b>387</b>



*This book is dedicated to our friend and colleague, Dewitt Latimer.  
Rest in peace, dear friend.*



# Preface

## Purpose of This Book

This book is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning ([www.jblearning.com](http://www.jblearning.com)). Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow, as well.

Consider this scenario: On a quiet June morning, sometime in the future, military commanders at U.S. Strategic Command in Nebraska gather around a computer screen, pointing at a series of social media posts that have just appeared on their screens. They are somewhat bewildered, because the posts seemed to come out of the blue, and they haven't heard anything from higher levels of command yet. Here's what they see:

### **International Cable News**

Breaking News: President Jones killed in attack on White House. More to come.

### **Unified Press Agencies**

Military troops ordered on high alert after DC attacks. Retaliatory strikes expected.

The commanding general picks up the hotline phone to place a call to the National Military Command Center to obtain further direction. She gets a puzzled look on her face when she hears a rapid busy signal. Normally, the watch officer in Washington answers the phone immediately. She quickly flips on the television and finds static instead of the normal cable news broadcast.

A young soldier in the command center turns to a computer connected to the public Internet and finds that he is unable to connect to any Web sites. The command center has no contact with the outside world and has received information that an attack against the nation's capital has resulted in the death of the commander in chief.

An alarmed airman approaches the general and reports: “Ma’am, we’ve lost control of one of our Predator drones. Station 6 is no longer able to control the flight and the drone appears to be following orders from someone else.” The alarmed command staff turns its attention to a monitor that is still streaming live video from the drone over a secure network and watches in horror as the drone begins to land at an airstrip in the Middle East. It is surrounded by inquisitive foreign military officers before the feed goes dead.

Did the attack against Washington actually take place? Is this the beginning of a major armed conflict? Were the social media posts legitimate or the results of cyberattacks against the press’s social media accounts? Are communications circuits dead because of a bomb dropped on a communications complex or a cyberwarfare attack against the command center? How did the enemy gain control of that drone? What is going to happen next?

Of course, this is a fictional scenario. But each of the attacks described here has occurred in one form or another over the past decade. In this book, you will learn about the role that cyberwarfare plays in modern military operations. In today’s connected world, it has become almost impossible to separate cyberwarfare from traditional warfare. The tools and techniques of cyberattacks have become part of the modern military arsenal, and cyberattacks can be expected before, during, and after armed conflict.

This book is divided into three parts. In Part 1, you will learn about the history of cyberwarfare. Information is a military asset and has played an important role in armed conflict from the days of Sun Tzu and Julius Caesar to the present. With the emergence of the cyber domain, electronic battles have joined the ranks of air, land, sea, and space warfare. This cyberwarfare leads to a variety of new concerns. Military planners must learn how to select and attack cybertargets. Military ethicists must apply long-standing principles of ethics and the law of armed conflict to domains that were never previously envisioned.

In Part 2 of this book, you will learn how offensive cyberwarfare has become an important part of the modern military arsenal. The rise of the advanced persistent threat has changed the face of cyberwarfare, and military planners must now be conscious of the Cyber Kill Chain: the series of cyberwarfare actions that include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and acting on objectives. You will read about the history of cyberwarfare and how it evolved from a novelty in the 1990s to a powerful integrated weapon in recent years. You will learn about the various types of malware that plagued the Internet in the 1990s and early 2000s and how they evolved into military weapons used to destroy nuclear facilities in recent years. You will also learn how nonstate actors have appeared on the cyberwarfare stage armed with more power than ever before.

You will also learn about the defensive strategies that militaries have evolved to protect themselves against cyberattacks. The concept of defense in depth is critical to building a well-rounded defense that will stand up to cyberwarfare events. Military defenses have evolved to include technological defenses such as cryptography, endpoint protection, firewalls, and data loss prevention systems.



In Part 3, you will learn how cyberwarfare may evolve in the future. You will read about military doctrine's evolution to include this new domain of warfare, and how military planners use threat modeling and deterrence to plan strategic and tactical cyberwarfare operations. You will also learn how recent events have opened a Pandora's box, setting the stage for future cyberwarfare attacks.

## **Learning Features**

The writing style of this book is practical and conversational. Step-by-step examples of information security concepts and procedures are presented throughout the text. Each chapter begins with a statement of learning objectives. Illustrations are used both to clarify the material and to vary the presentation. The text is sprinkled with Notes, Tips, FYIs, Warnings, and sidebars to alert the reader to additional helpful information related to the subject under discussion. Chapter Assessments appear at the end of each chapter, with solutions provided in the back of the book. Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

## **Audience**

The material is suitable for undergraduate or graduate computer science majors or information science majors, students at a two-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge.



# Acknowledgments

The authors would like to thank the many people who contributed to the successful publication of this book.

First and foremost, we had a tremendous team of subject matter experts assisting us in the preparation of our manuscript. Sam Liles, associate professor of computer and information technology at Purdue University, served as our technical editor and gave us valuable input during the writing process. Addam Schroll served as our lead researcher and provided us with background material that proved invaluable as we sought to flesh out the text with real-world examples of cyberwarfare activities.

We would like to thank Randi Roger of Jones & Bartlett Learning for her continued friendship and support on this project. Along with Chris Will and Rainna Erikson, Randi provided us with the inspiration for this book and helped bring together an incredible team of professionals who ensured its success.

This manuscript benefited from the skills of a top-notch editing team. Larry Goodrich and Karen Annett corrected our typos, pointed out areas of ambiguity in the text, and served as wonderful advisors throughout the project. Thank you both for your guidance and support.

We also extend our thanks to Carole Jelen of Waterside Productions, our literary agent. Carole's decades of experience and wonderful network of contacts proved themselves invaluable once again on this project.

Finally, we would like to thank the many people we never met who contributed to this book. Artists, layout specialists, and technical staff at Jones & Bartlett helped this book make the leap from our minds to the printed page or electronic text that you read today. Thank you all for your help.

## About the Authors

**MIKE CHAPPLE, PhD**, is senior director for IT Service Delivery at the University of Notre Dame. In this role, he oversees the information security, data governance, IT architecture, project management, strategic planning, and product management functions for the Office of Information Technologies. He also serves as a concurrent assistant professor in the university's computer applications and management departments, where he teaches undergraduate courses on information security. In past positions, he served as both a consultant and an active duty Air Force officer. He is a technical editor for *Information Security* magazine and has written 15 other books, including the *Security+ Training Kit*, *Information Security Illuminated*, *SQL Server 2008 for Dummies*, and the *CISSP Prep Guide*. He earned his undergraduate and PhD degrees from Notre Dame in computer science and engineering. He also holds a master's degree in computer science from the University of Idaho and an MBA from Auburn University.

**DAVID SEIDL** is the senior director for Campus Technology Services at the University of Notre Dame. In his role at Notre Dame, he leads identity and access management; database, application, and platform services; and communications and digital signage as part of the university's Office of Information Technologies. He also serves as a concurrent instructor for Notre Dame's Mendoza College of Business, where he teaches a popular networking and security course. He has written and acted as a technical editor of several computer security books. Prior to his current role, he served in a variety of information security positions, and was recognized in 2013 as a member of Network Computing's Security Seven for his contributions to information security in higher education. He holds CISSP, GCIH, and GPEN certifications, as well as a master's degree in information security.