CONTENTS

INTRODUCTION 1

Why Write a Book about Cybersecurity and Cyberwar? 1

Why Is There a Cybersecurity Knowledge Gap, and Why Does It Matter? 4

How Did You Write the Book and What Do You Hope to Accomplish? 8

PART I HOW IT ALL WORKS 12

The World Wide What? Defining Cyberspace 12

Where Did This "Cyber Stuff" Come from Anyway? A Short History of the Internet 16

How Does the Internet Actually Work? 21

Who Runs It? Understanding Internet Governance 26

On the Internet, How Do They Know Whether You Are a Dog? Identity and Authentication 31

What Do We Mean by "Security" Anyway? 34

What Are the Threats? 36

One Phish, Two Phish, Red Phish, Cyber Phish: What Are Vulnerabilities? 39

How Do We Trust in Cyberspace? 45

Focus: What Happened in WikiLeaks? 51

What Is an Advanced Persistent Threat (APT)? 55
How Do We Keep the Bad Guys Out? The Basics of Computer Defense 60
Who Is the Weakest Link? Human Factors 64

PART II WHY IT MATTERS 67

What Is the Meaning of Cyberattack? The Importance of Terms and Frameworks 67
Whodunit? The Problem of Attribution 72
What Is Hactivism? 77
Focus: Who Is Anonymous? 80
The Crimes of Tomorrow, Today: What Is Cybercrime? 85
Shady RATs and Cyberspies: What Is Cyber Espionage? 91
How Afraid Should We Be of Cyberterrorism? 96
So How Do Terrorists Actually Use the Web? 99
What about Cyber Counterterrorism? 103
Security Risk or Human Right? Foreign Policy and the Internet 106
Focus: What Is Tor and Why Does Peeling Back the Onion Matter? 108
Who Are Patriotic Hackers? 110
Focus: What Was Stuxnet? 114
What Is the Hidden Lesson of Stuxnet? The Ethics of Cyberweapons 118
"Cyberwar, Ugh, What Are Zeros and Ones Good For?": Defining Cyberwar 120
A War by Any Other Name? The Legal Side of Cyber Conflict 122
What Might a "Cyberwar" Actually Look Like? Computer Network Operations 126
Focus: What Is the US Military Approach to Cyberwar? 133
Focus: What Is the Chinese Approach to Cyberwar? 138
What about Deterrence in an Era of Cyberwar? 144
Why Is Threat Assessment So Hard in Cyberspace? 148
Does the Cybersecurity World Favor the Weak or the Strong? 150
Who Has the Advantage, the Offense or the Defense? 153

A New Kind of Arms Race: What Are the Dangers of Cyber Proliferation? 156

Are There Lessons from Past Arms Races? 160

Behind the Scenes: Is There a Cyber-Industrial Complex? 162

PART III WHAT CAN WE DO? 166

Don't Get Fooled: Why Can't We Just Build a New, More Secure Internet? 166

Rethink Security: What Is Resilience, and Why Is It Important? 169

Reframe the Problem (and the Solution): What Can We Learn from Public Health? 173

Learn from History: What Can (Real) Pirates Teach Us about Cybersecurity? 177

Protect World Wide Governance for the World Wide Web: What Is the Role of International Institutions? 180

"Graft" the Rule of Law: Do We Need a Cyberspace Treaty? 185

Understand the Limits of the State in Cyberspace: Why Can't the Government Handle It? 193

Rethink Government's Role: How Can We Better Organize for Cybersecurity? 197

Approach It as a Public-Private Problem: How Do We Better Coordinate Defense? 205

Exercise Is Good for You: How Can We Better Prepare for Cyber Incidents? 211

Build Cybersecurity Incentives: Why Should I Do What You Want? 216

Learn to Share: How Can We Better Collaborate on Information? 222

Demand Disclosure: What Is the Role of Transparency? 228

Get "Vigorous" about Responsibility: How Can We Create Accountability for Security? 231

Find the IT Crowd: How Do We Solve the Cyber People Problem? 235

Do Your Part: How Can I Protect Myself (and the Internet)? 241

CONCLUSIONS 247

Where Is Cybersecurity Headed Next? 247

What Do I Really Need to Know in the End? 255

ACKNOWLEDGMENTS 257

NOTES 259

GLOSSARY 293

INDEX 301