

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

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

PART II WHY IT MATTERS 67

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

<i>A New Kind of Arms Race: What Are the Dangers of Cyber Proliferation?</i>	156
<i>Are There Lessons from Past Arms Races?</i>	160
<i>Behind the Scenes: Is There a Cyber-Industrial Complex?</i>	162

PART III WHAT CAN WE DO? 166

<i>Don't Get Fooled: Why Can't We Just Build a New, More Secure Internet?</i>	166
<i>Rethink Security: What Is Resilience, and Why Is It Important?</i>	169
<i>Reframe the Problem (and the Solution): What Can We Learn from Public Health?</i>	173
<i>Learn from History: What Can (Real) Pirates Teach Us about Cybersecurity?</i>	177
<i>Protect World Wide Governance for the World Wide Web: What Is the Role of International Institutions?</i>	180
<i>"Graft" the Rule of Law: Do We Need a Cyberspace Treaty?</i>	185
<i>Understand the Limits of the State in Cyberspace: Why Can't the Government Handle It?</i>	193
<i>Rethink Government's Role: How Can We Better Organize for Cybersecurity?</i>	197
<i>Approach It as a Public-Private Problem: How Do We Better Coordinate Defense?</i>	205
<i>Exercise Is Good for You: How Can We Better Prepare for Cyber Incidents?</i>	211
<i>Build Cybersecurity Incentives: Why Should I Do What You Want?</i>	216
<i>Learn to Share: How Can We Better Collaborate on Information?</i>	222
<i>Demand Disclosure: What Is the Role of Transparency?</i>	228
<i>Get "Vigorous" about Responsibility: How Can We Create Accountability for Security?</i>	231
<i>Find the IT Crowd: How Do We Solve the Cyber People Problem?</i>	235
<i>Do Your Part: How Can I Protect Myself (and the Internet)?</i>	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