Contents

Preface ix
Foreword xi
Introduction xiii
Biography xvii

1. Cyber Warfare: Here and Now

What Is Cyber War? 2
Is Cyber War a Credible Threat? 2
Attribution, Deception, and Intelligence 4
Information Assurance 6

I CYBER ATTACK

2. Political Cyber Attack Comes of Age in 2007

Reliance on Information as a Vulnerability 12
Rudimentary but Effective: Denial of Service 12
Leaving Unwanted Messages: Web Site
    Defacement 14
Tools for Denial of Service 14
The Difficulty of Assigning Blame: Why
    Attribution Is Tough in a DDoS Attack 15
Estonia Is Hit by Cyber Attacks 16
General Response to DDoS 20
Summary 21
Suggested Further Reading 21

3. How Cyber Attacks Augmented Russian Military Operations

The 2008 Russian Cyber Campaign Against
    Georgia 24
What Is Interesting About the Russian Cyber
    Campaign 26
Preparing for a Cyber-Enabled Adversary 29
Summary 31
Suggested Further Reading 31

4. When Who Tells the Best Story Wins: Cyber and Information Operations in
   the Middle East

Hijacking Noncombatant Civilian IP Addresses
to Help the War Effort: The Israel-Hizbollah
"July War" of 2006 34
Civilians in the Cyber Melee: Operation
    Cast Lead 38
Summary 41
Suggested Further Reading 41

5. Limiting Free Speech on the Internet: Cyber Attack Against Internal
   Dissidents in Iran and Russia

DDoS as a Censorship Tool: Why Dissident Groups Are Inherently Vulnerable to Cyber Attacks 44
Silencing Novaya Gazeta and Other Russian Dissidents 47
Iran—How the 2009 Elections Led to Aggressive Cyber Operations 53
Summary 61

6. Cyber Attacks by Nonstate Hacking Groups: The Case of Anonymous and Its Affiliates

“Chaotic” Beginnings: The Chaos Computer Club, CCC 69
The Roots of the Anon—4chan, 7chan, and Other Message Boards 71
How We Are Influenced by 4chan: Memes 72
II

CYBER ESPIONAGE AND EXPLOITATION

7. Enter the Dragon: Why Cyber Espionage Against Militaries, Dissidents, and Nondefense Corporations Is a Key Component of Chinese Cyber Strategy

Introduction 114
Why Cyber Espionage Is Important to China: A Look at Chinese Cyber Doctrine 116
Leveraging Resources Beyond the Military: The Cyber Warriors of China 120
Stealing Information from the U.S. Industrial-Military Complex: Titan Rain 124
Cyber War Against the Corporate World: A Case Study of Cyber Intrusion Attributed to China 128
Monitoring Dissidents: Gh0stNet 132
Using Legitimate Web Sites for Data Exfiltration: The Shadow Network 141
Cyber War Through Intellectual Property Theft: Operation Aurora 145
An Example of the Current State of the Art: Sykipot 150
Summary 152
Suggested Further Reading 153

8. Duqu, Flame, Gauss, the Next Generation of Cyber Exploitation

Introduction 160
Kernel Mode Rootkits 161

III

CYBER OPERATIONS FOR INFRASTRUCTURE ATTACK

11. Cyber Warfare Against Industry

Introduction 200
Industrial Control Systems: Critical Infrastructure for Modern Nations 200
Information Technology vs. Industrial Control Systems: Why Traditional Infosec Practices May Not Apply 201