Inside Cyber Warfare

Jeffrey Carr
foreword by Lewis Shepherd

O'REILLY[4]
Beijing • Cambridge • Farnham • Kdln • Sebastopol • Tokyo

Table of Contents

Foreword xi

Preface xiii

1. Assessing the Problem 1

The Complex Domain of Cyberspace 1
Cyber Warfare in the 20th and 21st Centuries 2
Cyber Espionage 4
Cyber Crime 5
Future Threats 6
Increasing Awareness 7
Critical Infrastructure 8
The Conficker Worm: The Cyber Equivalent of an Extinction Event? 12
Africa: The Future Home of the World's Largest Botnet? 13
The Way Forward 14

2. The Rise of the Non-State Hacker 15

The StopGeorgia.ru Project Forum 15
Counter-Surveillance Measures in Place 16
The Russian Information War 16
The Foundation for Effective Politics' War on the Net (Day One) 17
The Gaza Cyber War Between Israeli and Arabic Hackers During Operation Cast Lead 19
Impact 19
Overview of Perpetrators 21
Hackers' Profiles 22
Methods of Attack 26
Israeli Retaliation 28
Control the Voice of the Opposition by Controlling the Content in Cyberspace: Nigeria 28
Are Non-State Hackers a Protected Asset? 29

3. The Legal Status of Cyber Warfare 31
Nuclear Nonproliferation Treaties 32
The Antarctic Treaty System and Space Law 33
UNCLOS 34
MALT 34
U.S. Versus Russian Federation: Two Different Approaches 34
The Law of Armed Conflict 35
Is This an Act of Cyber Warfare? 37
South Korea 37
Iran 37
Tatarstan 37
United States 37
Kyrgyzstan 38
Israel and the Palestinian National Authority 38
Zimbabwe 38
Myanmar 39
Cyber: The Chaotic Domain 39

4. Responding to International Cyber Attacks As Acts of War 45
Introduction by Jeffrey Carr 45
Introduction 45
The Legal Dilemma 47
The Road Ahead: A Proposal to Use Active Defenses 48
The Law of War 48
General Prohibition on the Use of Force 49
The First Exception: UN Security Council Actions 49
The Second Exception: Self-Defense 50
A Subset of Self-Defense: Anticipatory Self-Defense 51
An Alternate Basis for Using Active Defenses: Reprisals 52
Non-State Actors and the Law of War 52
Armed Attacks by Non-State Actors 53
Duties Between States 54
Imputing State Responsibility for Acts by Non-State Actors 55
Cross-Border Operations 56
Analyzing Cyber Attacks Under Jus ad Bellum 57
Cyber Attacks As Armed Attacks 58
Establishing State Responsibility for Cyber Attacks 61
The Duty to Prevent Cyber Attacks 62
Support from International Conventions 63
Support from State Practice 64
Support from the General Principles of Law 66
Support from Judicial Opinions 67
Fully Defining a State's Duty to Prevent Cyber Attacks 67

Sanctuary States and the Practices That Lead to State Responsibility 68
The Choice to Use Active Defenses 68
Technological Limitations and Jus ad Bellum Analysis 69
Jus in Bello Issues Related to the Use of Active Defenses 71
Conclusion 74

5. The Intelligence Component to Cyber Warfare. 77
The Korean DDoS Attacks (July 2009) 78
The Botnet Versus the Malware 80
The DPRK's Capabilities in Cyberspace 81
One Year After the RU-GE War, Social Networking Sites Fall to DDoS Attack 83
Ingushetia Conflict, August 2009 85
The Predictive Role of Intelligence 86

6. Non-State Hackers and the Social Web. 89
Russia 89
China 90
The Middle East 91
Pakistani Hackers and Facebook 92
The Dark Side of Social Networks 93
The Cognitive Shield 94
TwitterGate: A Real-World Example of a Social Engineering Attack with Dire Consequences 97
Automating the Process 99
Catching More Spies with Robots 99

7. Follow the Money. 103
False Identities 103
Components of a Bulletproof Network 105
ICANN 105
The Accredited Registrar 106
The Hosting Company 106
The Bulletproof Network of StopGeorgia.ru 106
StopGeorgia.ru 106
NAUNET.RU 107
SteadyHost.ru 108
Innovation IT Solutions Corp 110
Mirhosting.com 112
SoftLayer Technologies 112
SORM-2 114
The Kremlin and the Russian Internet 115
Nashi 115

The Kremlin Spy for Hire Program •- 117
Sergei Markov, Estonia, and Nashi 118
A Three-Tier Model of Command and Control 119

8. Organized Crime in Cyberspace 121
A Subtle Threat 125
Atrivo/Intercage 125
ESTDomains 126
McColo: Bulletproof Hosting for the World's Largest Botnets 127
Russian Organized Crime and the Kremlin 129

9. Investigating Attribution 131
Using Open Source Internet Data 131
Background 132
What Is an Autonomous System Network? 134
Team Cymru and Its Darknet Report 137
Using WHOIS 138
Caveats to Using WHOIS 140

10. Weaponizing Malware 141
A New Threat Landscape 141
StopGeorgia.ru Malware Discussions 141
Twitter As DDoS Command Post Against Iran 144
Social Engineering 146
Channel Consolidation 148
An Adversary's Look at Linkedln 149
BIOS-Based Rootkit Attack 150
Malware for Hire 151
Anti-Virus Software Cannot Protect You 151
Targeted Attacks Against Military Brass and Government Executives 152

11. The Role of Cyber in Military Doctrine 161
The Russian Federation 161
The Foundation for Effective Politics (FEP) 163
"Wars of the Future Will Be Information Wars" 165
"RF Military Policy in International Information Security" 166
The Art of Misdirection 169
China Military Doctrine 171
Anti-Access Strategies 174
The 36 Stratagems 174
U.S. Military Doctrine 176

12. A Cyber Early Warning Model **179**
Introduction by Jeffrey Carr 179
The Challenge We Face 179
Cyber Early Warning Networks 180
Building an Analytical Framework for Cyber Early Warning 180
Cases Studies of Previous Cyber Attacks 183
Lessons Learned 187
Defense Readiness Condition for Cyberspace 188

13. Advice for Policy Makers from the Field **191**
When It Comes to Cyber Warfare: Shoot the Hostage 191
The United States Should Use Active Defenses to Defend Its Critical Information Systems 194
Scenarios and Options to Responding to Cyber Attacks 196
Scenario 1 196
Scenario 2 197
Scenario 3 198
Scenario 4 198
In Summary 198
Whole-of-Nation Cyber Security 199

Afterword **203**

Index **207**