# 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 7  
   Increasing Awareness 7  
   Critical Infrastructure 8  
   The Conficker Worm: The Cyber Equivalent of an Extinction Event? 12  
   The Way Forward 14  

2. **The Rise of the Nonstate Hacker** ............................. 15  
   The StopGeorgia.ru Project Forum 15  
   Counter-Surveillance Measures in Place 16  
   The Russian Information War 17  
   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 27  
   Israeli Retaliation 28  
   Control the Voice of the Opposition by Controlling the Content in  
   Cyberspace: Nigeria 29  
   Are Nonstate Hackers a Protected Asset? 29  

iii
3. **The Legal Status of Cyber Warfare** .................................................. 31
   - Nuclear Nonproliferation Treaties 32
   - The Antarctic Treaty System and Space Law 33
   - UNCLOS 34
   - MLAT 34
   - United States 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 38
     - 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
   - 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
   - Nonstate Actors and the Law of War 52
     - Armed Attacks by Nonstate Actors 53
     - Duties between States 54
     - Imputing State Responsibility for Acts by Nonstate 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
8. **Organized Crime in Cyberspace** ........................................... 121
   A Subtle Threat 125
   Atrivo/Intercage 126
   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 134
   What Is an Autonomous System Network? 135
   Team Cymru and Its Darknet Report 138
   Using WHOIS 139
   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 LinkedIn 149
    BIOS-Based Rootkit Attack 151
    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
    US Military Doctrine 176

12. **A Cyber Early Warning Model** ............................................ 179
    The Challenge We Face 179
    Cyber Early Warning Networks 180
Internal Security Services: Federal Security Service (FSB), Ministry of Interior (MVD), and Federal Security Organization (FSO) 229
   Federal Security Service Information Security Center (FSB ISC)—Military Unit (Vch) 64829 229
   Russian Federal Security Service Center for Electronic Surveillance of Communications (FSB TSRRSS)—Military Unit (Vch) 71330 230
   FSB Administrative Centers for Information Security 231
   Russian Interior Ministry Center E (MVD Center E) 232
   Russian Interior Ministry Cyber Crimes Directorate (MVD Directorate K) 232
   Russian Federal Security Organization (FSO)—Military Unit (Vch) 32152 235
   Russian Federation Ministry of Communications and Mass Communications (Minsvyaz) 237
      Roskomnadzor 238
Further Research Areas 241

16. Cyber Warfare Capabilities by Nation-State ........................................... 243
   Australia 243
   Brazil 244
   Canada 244
   Czech Republic 245
   Democratic People's Republic of Korea 246
   Estonia 247
   European Union 248
   France 248
   Germany 249
   India 250
   Iran 250
   Israel 251
   Italy 252
   Kenya 253
   Myanmar 253
   NATO 254
   Netherlands 255
   Nigeria 255
   Pakistan 256
   People's Republic of China 257
   Poland 258
   Republic of Korea 258
   Russian Federation 259
   Singapore 259
   South Africa 259
Sweden 260
Taiwan (Republic of China) 260
Turkey 261
United Kingdom 261

17. **US Department of Defense Cyber Command and Organizational Structure** .... 263
    Summary 263
    Organization 264
        The Joint Staff 264
        Office of the Secretary of Defense 266
        US Strategic Command (USSTRATCOM) 268

18. **Active Defense for Cyber: A Legal Framework for Covert Countermeasures** .... 273
    Covert Action 276
    Cyber Active Defense Under International Law 277
    Cyber Active Defenses as Covert Action Under International Law 280
    Cyber Attacks Under International Law: Nonstate Actors 281

Index ................................................................. 285