Cyberspace is essential for socializing, learning, shopping, and just about everything in modern life. Despite the importance of cyberspace, there is also a dark side where subnational, transnational, and international actors are challenging the ability of sovereign governments to provide a secure environment for their citizens. Criminal groups hold businesses and local governments hostage through ransomware, foreign intelligence services steal intellectual property and conduct influence operations, governments attempt to rewrite Internet Protocols to facilitate censorship, and militaries prepare to use cyberspace operations in wars. Security in the Cyber Age breaks down how cyberspace works, analyzes how state and nonstate actors exploit vulnerabilities in cyberspace, and provides ways to improve cybersecurity. Written by a computer scientist and a national security scholar-practitioner, the book offers technological, policy, and ethical ways to protect cyberspace. Its interdisciplinary approach and engaging style make the book accessible to the lay audience as well as computer science and political science students.

DEREK S. REVERON is Chair of the National Security Affairs Department at the US Naval War College in Newport, Rhode Island, Faculty Affiliate of the Belfer Center for Science and International Affairs, and Lecturer in Extension at Harvard University. He specializes in strategy development, national security challenges, and US defense policy. He served as a governor-appointed commissioner on the Rhode Island Cybersecurity Commission. His published work examines US foreign policy and defense strategy.

JOHN E. SAVAGE is the An Wang Professor Emeritus of Computer Science at Brown University. He is a fellow of the American Association for the Advancement of Science, the Association for Computing Machinery, and the Institute of Electrical and Electronics Engineers and a Guggenheim Fellow. He served as a Jefferson Science Fellow in the US State Department, a professorial fellow at the EastWest Institute, and a member of the Rhode Island Cybersecurity Commission. He has published over a hundred research articles and two books on theoretical computer science, has coauthored a book on computer literacy, and has coedited a book on Very Large Scale Integration (VLSI) and parallel systems. He has given more than 185 invited presentations worldwide.
“In *Security in the Cyber Age*, Reveron and Savage eloquently merge tech and policy, crafting an essential guide that educates readers about our digital past, present, and future. A must-read for those seeking to navigate the complexities of our interconnected world.”

– Max Smeets, Author of *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*

“A very useful and accessible overview of the technology and an important addition to the literature on its security.”

– Ciaran Martin, University of Oxford

“Reveron and Savage elegantly weave together technology and policy topics to explain the big cyber security issues societies face today. They effectively bring multiple disciplinary perspectives to bear giving the reader in-depth understanding in an accessible way.”

– Tyler Moore, The University of Tulsa
Security in the Cyber Age

An Introduction to Policy and Technology

Derek S. Reveron
US Naval War College

John E. Savage
Brown University
The triumph of the industrial arts will advance the cause of civilization more rapidly than its warmest advocates could have hoped, and contribute to the permanent prosperity and strength of the country far more than the most splendid victories of successful war.

Charles Babbage, inventor of the programmable computer
Contents

List of Boxes  xi
   Essential Principles  xi
   Exploits  xii
   Policy Matters  xii
   History Matters  xiii
   Preface  xv
   Acknowledgments  xvii

Introduction  1
The Promise and Perils of Cyberspace  1
A Shared Responsibility for Security  5
The Motivation for This Book  6
Chapter Overviews  7
Conclusions  11
Discussion Topics  12

1 The Emergence of Cyberspace and Its Implications  13
  1.1 The Emergence of Packet-Switching  17
  1.2 The Experimental ARPANET Packet-Based Network  19
  1.3 The World Wide Web Appears  22
  1.4 Defining Cyberspace  23
  1.5 Cyberspace Challenges  25
  1.6 Threats to the Information Environment  27
  1.7 Attribution  30
  1.8 Ethics, Norms, Regulations, and Law  33
  1.9 Cyberspace Is Unique  33
  1.10 Discussion Topics  34
Contents

2 From the Abacus to the Computer 35
  2.1 Mechanical Aids to Computation 36
  2.2 The Emergence of Programming 40
  2.3 Computer Architecture 43
  2.4 Programming 52
  2.5 Operating Systems 55
  2.6 Malicious Software 64
  2.7 Antivirus Software 66
  2.8 Hardware Side-Channel Attacks 67
  2.9 Ethical Issues in Hardware and Software Engineering 70
  2.10 Conclusions 72
  2.11 Discussion Topics 72

3 Communicating through Cyberspace 73
  3.1 Communication Networks 73
  3.2 Communication Technologies 73
  3.3 Telephone Networks 76
  3.4 Packet-Based Networks 76
  3.5 The Domain Name System 78
  3.6 Autonomous Systems 79
  3.7 Addressing Network Devices 80
  3.8 Internet Packets 81
  3.9 Internet Protocol Layers 81
  3.10 Internet Protocols 83
  3.11 Building Routing Tables Using the Border Gateway Protocol 86
  3.12 Local Area Networks 87
  3.13 Secure Communications 90
  3.14 Issues Introduced by Public-Key Cryptosystems 99
  3.15 Rivest–Shamir–Adleman Public-Key Cryptosystem 100
  3.16 Exceptional Access to Encrypted Information 103
  3.17 The Quantum Threat 103
  3.18 Post-quantum Cryptography 106
  3.19 Conclusions 106
  3.20 Discussion Topics 107

4 The Human Dimensions of Cyberspace 108
  4.1 The Security Environment 109
  4.2 Assessing Risk and Measuring Loss 110
  4.3 Protecting against Nation-State Cyberattacks 113
  4.4 Cognitive Limitations on Judgments and Decision-Making 120
  4.5 Cyber Economics 128
Contents

4.6 Designing an Ethical Organization 138
4.7 Conclusions: Managing Cybersecurity Risks 139
4.8 Discussion Topics 140

5 Strategy and Cyberspace 141
5.1 Strategy and National Power 142
5.2 Role of National Interests in Formulating Cybersecurity Strategy 146
5.3 Grand Strategy 149
5.4 Deterrence in the Cyber Age 151
5.5 Cyber and War 155
5.6 US Approach to Cybersecurity 162
5.7 Cyberspace Operations and the Policy Process in the United States 167
5.8 The International Agenda and the Cyber Policy Space 172
5.9 Discussion Topics 172

6 Domestic Regulation of Cyberspace 174
6.1 Emergence of the Internet 174
6.2 Supply Chain Regulation 177
6.3 Encryption 181
6.4 Content Regulation 187
6.5 Data Localization 194
6.6 Malware as Crime 196
6.7 Private but Public Network 197
6.8 Conclusions: From Internet to Internets 198
6.9 Discussion Topics 199

7 Internet Governance and International Institutions 200
7.1 Evolution of Internet Governance 203
7.2 Role of United Nations 207
7.3 Other International Agreements 211
7.4 Uniting Sovereignty: Case of the North Atlantic Treaty Organization 218
7.5 Overcoming Sovereignty: Case of the European Union 221
7.6 Conclusions 223
7.7 Discussion Topics 224

8 International Law and Norms in Cyberspace 226
8.1 International Law and Ethics 229
8.2 Defining an Armed Attack in Cyberspace 238
8.3 Norms Development Process 240
Contents

8.4 Role of Corporations 242
8.5 Role of the United Nations 244
8.6 Role of Nongovernmental Organizations 248
8.7 Norms for the Next Decade 249
8.8 Conclusions 251
8.9 Discussion Topics 252

9 Artificial Intelligence and Ethics 253
9.1 Artificial Intelligence 253
9.2 The Development of Intelligent Mechanical Machines 255
9.3 A Brief History of Artificial Intelligence 257
9.4 The Technologies of Artificial Intelligence 264
9.5 Surprises Introduced by Machine Learning Systems 275
9.6 Artificial General Intelligence 283
9.7 Robotics 284
9.8 Ethical Principles for Artificial Intelligence 286
9.9 Applications of Artificial Intelligence to Cybersecurity 289
9.10 Conclusions 292
9.11 Discussion Topics 293

10 Conclusions and Future Directions of Cybersecurity Policy 295
10.1 An Uncertain Future 296
10.2 Whose Internet? 299
10.3 Internet for Individuals 303
10.4 Internet for Corporations 305
10.5 Internet for Governments 308
10.6 Bridging the Divides 312
10.7 Importance of Framing Cybersecurity 314
10.8 Government Responses to International Crises 315
10.9 Concluding Thoughts 319
10.10 Discussion Topics 319

11 Leading in the Cyber Age 321
11.1 Superforecasting 322
11.2 Leading through Uncertainty 327
11.3 Discussion Topics 328

Glossary 329
References 347
Index 387
Essential Principles

1.1 Coding principles........................................................................... page 25
2.1 Computing with logarithms................................................................. 37
2.2 Strengthening password security...................................................... 58
2.3 Behavioral analysis............................................................................ 66
2.4 Software Engineering Code of Ethics (short version)......................... 71
3.1 Packet looping............................................................................... 77
3.2 Understanding an IP prefix............................................................... 80
3.3 The TCP three-way handshake......................................................... 84
3.4 Announcements of subprefixes have priority................................. 86
3.5 Automated mitigation of BGP hijacking............................................ 86
3.6 Route flapping............................................................................... 87
3.7 Kerckhoffs’ principle....................................................................... 90
3.8 Discrete logarithms....................................................................... 97
3.9 The totient function..................................................................... 101
3.10 Integer factorization................................................................... 101
3.11 An important RSA public-key cryptosystem vulnerability............. 102
4.1 Structured Query Language injection.............................................. 115
4.2 Security information and event management system....................... 119
4.3 Risk management....................................................................... 137
5.1 Sovereignty................................................................................ 147
5.2 Defense support of civil authorities................................................. 168
6.1 Virtual private network.................................................................. 177
6.2 Data confidentiality, integrity, and availability................................. 182
6.3 Intelligence collection process......................................................... 190
7.1 Collective defense....................................................................... 218
8.1 Principles on legality of war............................................................ 233
## List of Boxes

<table>
<thead>
<tr>
<th>Box</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 ChatGPT illustrations</td>
<td>281</td>
</tr>
<tr>
<td>10.1 Precautionary principle</td>
<td>314</td>
</tr>
</tbody>
</table>

### Exploits

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Spoofing domain names</td>
<td>21</td>
</tr>
<tr>
<td>1.2</td>
<td>Cybersquatting</td>
<td>22</td>
</tr>
<tr>
<td>1.3</td>
<td>The Aurora Generator Test</td>
<td>26</td>
</tr>
<tr>
<td>2.1</td>
<td>Configuration errors</td>
<td>60</td>
</tr>
<tr>
<td>2.2</td>
<td>NotPetya, extraordinarily damaging malware</td>
<td>65</td>
</tr>
<tr>
<td>2.3</td>
<td>Hardware side-channel attacks</td>
<td>68</td>
</tr>
<tr>
<td>3.1</td>
<td>Phone phreaking</td>
<td>75</td>
</tr>
<tr>
<td>3.2</td>
<td>Pakistan BGP hijacking of YouTube</td>
<td>85</td>
</tr>
<tr>
<td>4.1</td>
<td>Target data breach</td>
<td>115</td>
</tr>
<tr>
<td>4.2</td>
<td>Social engineering in practice</td>
<td>122</td>
</tr>
<tr>
<td>4.3</td>
<td>The Metcalf substation incident</td>
<td>129</td>
</tr>
<tr>
<td>4.4</td>
<td>Operation Aurora</td>
<td>131</td>
</tr>
<tr>
<td>4.5</td>
<td>Mirai botnet-based DDoS attack: 2016 Internet outage</td>
<td>134</td>
</tr>
<tr>
<td>5.1</td>
<td>BlackEnergy compromise of a Ukrainian power station</td>
<td>156</td>
</tr>
<tr>
<td>5.2</td>
<td>Stuxnet and zero-day vulnerabilities</td>
<td>157</td>
</tr>
<tr>
<td>5.3</td>
<td>Denial-of-service attacks against the US financial sector</td>
<td>163</td>
</tr>
<tr>
<td>6.1</td>
<td>A supply chain attack</td>
<td>179</td>
</tr>
<tr>
<td>6.2</td>
<td>SolarWinds supply chain attack</td>
<td>189</td>
</tr>
<tr>
<td>6.3</td>
<td>Russian intelligence hacks the Democratic Party</td>
<td>193</td>
</tr>
<tr>
<td>7.1</td>
<td>International cybercriminal ring’s use of botnets</td>
<td>211</td>
</tr>
<tr>
<td>8.1</td>
<td>Espionage at the Office of Personnel Management</td>
<td>239</td>
</tr>
<tr>
<td>9.1</td>
<td>Deepfake face swaps</td>
<td>276</td>
</tr>
<tr>
<td>10.1</td>
<td>Inauthentic behavior on Facebook</td>
<td>307</td>
</tr>
</tbody>
</table>

### Policy Matters

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Internet privacy in California</td>
<td>17</td>
</tr>
<tr>
<td>2.1</td>
<td>Nationalizing semiconductor manufacturing</td>
<td>51</td>
</tr>
<tr>
<td>3.1</td>
<td>Encryption and law enforcement</td>
<td>102</td>
</tr>
<tr>
<td>4.1</td>
<td>Promoting information-sharing</td>
<td>136</td>
</tr>
<tr>
<td>5.1</td>
<td>Bombing hackers</td>
<td>154</td>
</tr>
<tr>
<td>6.1</td>
<td>Defining economic espionage</td>
<td>196</td>
</tr>
<tr>
<td>7.1</td>
<td>Internet governance levels</td>
<td>202</td>
</tr>
<tr>
<td>7.2</td>
<td>Objections to the Cybercrime Treaty</td>
<td>213</td>
</tr>
<tr>
<td>8.1</td>
<td>Cyber’s Most Wanted</td>
<td>239</td>
</tr>
<tr>
<td>9.1</td>
<td>Algorithmic warfare</td>
<td>267</td>
</tr>
<tr>
<td>10.1</td>
<td>Banning technology</td>
<td>310</td>
</tr>
</tbody>
</table>
List of Boxes  xiii

History Matters
1.1 Technology gap and the Cold War     19
2.1 The abacus in a calculating contest  36
2.2 Lovelace’s observation about the Analytical Engine  41
2.3 Origin of the word “computer”  43
2.4 Software development processes  54
3.1 The browser and the World Wide Web  89
3.2 Substitution ciphers  92
3.3 PKC  95
4.1 Perfect code: The story of NASA software engineers  132
5.1 The Thucydides Trap  148
6.1 The right to privacy  176
7.1 IANA  205
8.1 Legal basis for restraint in domestic cybersecurity  237
10.1 The first webpage  300
The modern world has become more complex and less predictable over the last century. The world population doubled, radio and television emerged, and the airplane and the programmable electronic computer were invented. The transistor, which is both an amplifier and a switch, and the integrated circuit, which puts billions of transistors on a single chip, were invented, making computers and smartphones affordable and ubiquitous. Fiber-optic cables and communication satellites provided for global communications. Advances in computer science led to new ways to move data that sparked the information revolution, creating cyberspace and transforming how people lead their daily lives, corporations execute operations, and governments deliver services and function.

Cyberspace is essential for socializing, learning, shopping, and just about everything in modern life but also has become a dangerous place. Almost every day there are reports of major cyber incidents. These include businesses and local governments being held hostage through ransomware, foreign intelligence services stealing intellectual property to further national industries, governments attempting to rewrite the foundational protocol of the Internet to facilitate censorship, and militaries preparing to use cyber operations in future wars. One of the more ominous consequences of cyberspace is the possibility of undermining nuclear deterrence or of governments engaging in cyber conflict, where belligerent countries attack power grids, telecommunications networks, and banking systems, bringing conflict to individuals’ devices and doorsteps.

Cyberspace is also a place of rich potential. Global communications are now commonplace, vast quantities of knowledge are at our fingertips, and enormous amounts of computational power are readily available to work on complex problems such as gene sequencing or assessing climate change. Further, artificial intelligence helps make sense of large datasets, creating new opportunities for businesses and new types of work as it displaces existing
work. This is an exciting time but one with many hurdles. The challenge for humanity is to harness cyberspace’s new technologies and limit its misuses so that its full potential can be realized, enabling security for every citizen, community, and country. This book starts to chart an interdisciplinary course to help students conceptualize and understand security in the modern cyber age.

One of the authors of this book is from the national security policy sphere and the other is a computer scientist with experience in the national security sector. We both served on the Rhode Island Cybersecurity Commission. Our goal is to facilitate communication across the divide that normally characterizes the technological and policy communities. Security in the Cyber Age considers the current and future threats in cyberspace, discusses various approaches to advance and defend national interests in cyberspace, and posits a way to improve national security in the cyber age. Fundamentally, the book establishes a coherent framework for understanding how cyberspace has become an important venue for international security by exploring the technological, policy, social, and economic dimensions of cyberspace.

The book provides a comprehensive treatment of security in the modern cyber age. Portions of the book can be used for undergraduate cybersecurity policy courses without prerequisites. To achieve this goal technical subjects are introduced with attention to concepts and terminology. The book also has enough advanced material and references for it to be useful at the advanced undergraduate and early graduate levels. The goal is to teach computer science students to appreciate the national security implications of computer science and political science students to apply national security ideas to cyberspace. The book is also written for the layperson who needs a broad understanding of these issues.
Acknowledgments

A work like this has been in the making for decades. Our students at Brown University, Harvard University, and the US Naval War College all played a small part in shaping our thinking on how to analyze the interaction between computer science and the social sciences. As we tried to highlight throughout this book, improving cybersecurity is a team sport for educators, technologists, and policy analysts; no single discipline or field can provide the solutions we need to realize the benefits of cyberspace. Faculty members need books that can explain how cyberspace works, analyze how state and nonstate actors exploit vulnerabilities in cyberspace, and provide frameworks in which to explore ways to improve security in cyberspace. We hope this book is a small contribution to this effort.

Throughout our writing process, several colleagues were generous with their time. They reviewed chapters, contributed ideas, and shared resources. While any errors or misguided ideas are our own, we thank Hank Brightman, Mary Brooks, David Cooper, Jeremy Davis, Jeremy Francis, Nick Gvosdev, Anna Hayes, Chuck Houston, Vasileios Kermelis, Steve Knott, James Kraska, Roberta Lopes da Cruz Antonio, Ryan Maness, Bruce McConnell, Michael Miner, Tyler Moore, David Polatty, Mike Rizzotti, Terry Roehrig, Jeff Rogg, David Sanger, Jacquelyn Schneider, Paul Smith, Willem Speckmann, Judith Strotz, Dana Struckman, Fred Turner, and Heidi von Stein. John is grateful to Brown University for providing him with the opportunity to spend a year in the US State Department as a Jefferson Science Fellow and to teach a course in this area. He is also very grateful to the dozens of undergraduate teaching assistants who staffed his course in this area during the 10 years that he taught it. We also thank the Cambridge University Press team and especially Katie Leach who helped us realize our goals to make these ideas widely available.
We thank Christopher Savage who created the cover image using Midjourney and are grateful to him for his permission to use it. The cover is testament to the utility of artificial intelligence and the creativity of those who can harness it.

These are our personal views and, in Derek’s case, the views expressed in this publication are those of the author and do not necessarily reflect the official policy or position of the US Naval War College, the Department of the Navy, the Department of Defense, or the US government. The public release clearance of this publication by the Department of Defense does not imply Department of Defense endorsement or factual accuracy of the material.