

CONTENTS

<i>List of Acronyms</i>	vii
Introduction	1
<i>The Approach</i>	9
<i>Definitions and Limitations</i>	11
1. The Security Dilemma	15
<i>Overview</i>	15
<i>International Relations, Anarchy, and the Security Dilemma</i>	17
<i>The Security Dilemma and Intelligence</i>	22
<i>Conclusion: The Stakes of the Security Dilemma</i>	28
2. The Intruder's View	31
<i>Overview</i>	31
<i>An Intrusion Model</i>	33
<i>How Operational Incentives Drive the Cybersecurity Dilemma</i>	41
<i>Conclusion: The First Pillar of the Cybersecurity Dilemma</i>	48
3. The Defender's View	51
<i>Overview</i>	51
<i>A Network Defense Model</i>	53
<i>How Network Intrusions Can Help Defenders</i>	64
<i>Conclusion: The Second Pillar of the Cybersecurity Dilemma</i>	72
4. How Network Intrusions Threaten	75
<i>Overview</i>	75
<i>Network Intrusions Can Enable Targeted and Powerful Cyber Attacks</i>	77
<i>Network Intrusions Can Provide a Beachhead for Further Operations</i>	81

CONTENTS

<i>Network Intrusions Can Change the Conditions of Conflict and Competition</i>	85
<i>Network Intrusions Can Pose Major Counterintelligence Challenges</i>	92
<i>Conclusion: The Third Pillar of the Cybersecurity Dilemma</i>	96
5. The Failure of Traditional Mitigations	101
<i>Overview</i>	101
<i>Offense–Defense Balance</i>	103
<i>Offense–Defense Differentiation</i>	110
<i>Greed</i>	113
<i>Unit-Level Analysis</i>	116
<i>Conclusion: Reaffirmation, Not Mitigation</i>	119
6. Information Distribution and the Status Quo	121
<i>Overview</i>	121
<i>Information Distribution</i>	123
<i>An Uncertain Status Quo</i>	130
<i>Conclusion: New Variables, New Opportunities</i>	138
7. Limitations, Objections, and the Future of the Cybersecurity Dilemma	141
<i>Overview</i>	141
<i>Objection: Attribution is Impossible</i>	143
<i>Objection: The Cyber Threat is Not Existential</i>	147
<i>Objection: Cyber Capabilities are Unevenly Distributed</i>	151
<i>Conclusion: The Present and Future of the Cybersecurity Dilemma</i>	155
8. Mitigating the Cybersecurity Dilemma	157
<i>Overview</i>	157
<i>The Value of Baseline Defenses</i>	158
<i>Advancing Bilateral Trust</i>	163
<i>Contributions to System-wide Security</i>	169
<i>Establishing a Security Posture</i>	178
<i>Conclusion: Old Variables, New Mitigations</i>	185
<i>Conclusion: The Dangers of the Cybersecurity Dilemma</i>	187
<i>Notes</i>	195
<i>Bibliography</i>	243
<i>Acknowledgments</i>	277
<i>Index</i>	281