

Contents

List of Illustrations

List of Acronyms and Abbreviations

INTRODUCTION

PART I. FOUNDATIONS

CHAPTER 1. EMBLEMATIC ATTACKS

Prototypical Events

Cybercrime and Other System Intrusions

Advanced Persistent Threat

Distributed Denial-of-Service Attacks

Disruptive and Destructive Attacks

Doxing Attacks

Conclusions

CHAPTER 2. SOME BASIC PRINCIPLES

Cyberwar and Cyberspace

Layers

How Hacks Work

Agoras and Castles

Most Cyberattacks Have Transitory Effects

CHAPTER 3. HOW TO COMPROMISE A COMPUTER

Abuses by Random External Users

Abuses by Authorized Internal Users

Altered Instructions via Supply-Chain Attack

Malware

Conclusions

CHAPTER 4. CYBERSECURITY AS A SYSTEMS PROBLEM

Applications Are Often the Weak Links in the Security Chain
The Role of Input Filtering
The Role of Browsers and Operating Systems
The Role of People
The Role of Cryptography
A Role for Firewalls?
The Role of Air-Gapping
Relationships among Machines, Systems, and Engineering
Cybersecurity as a Business Process Problem
Measures and Countermeasures
Lessons from the OPM Hack

CHAPTER 5. DEFENDING AGAINST DEEP AND WIDE ATTACKS

Deep Attacks
Identifying Near-Catastrophes to Get Ahead of Catastrophes
Hedging to Deal with Exceptions to the Power-Law Rule
Attacks of Broad Consequence
Scalability Influences How Well a Near-Catastrophe Predicts a Catastrophe
Implications for Learning
Is Information Sharing a Panacea?

CHAPTER 6. DETERRENCE BY DENIAL

What Is Being Discouraged?
Complicating Psychological Factors
Dissuading Cyberattack by Defeating Its Strategy
Is Deterrence by Denial Transferable?

PART II. OPERATIONS

CHAPTER 7. TACTICAL CYBERWAR

Possible Effects
Timing Cyberattacks
The Role of Surprise

A Tactical Cyberwar Scenario
Would China Use Tactical Cyberwar the Same Way?
Why Supremacy Is Meaningless and Superiority Unnecessary
Conclusions

CHAPTER 8. ORGANIZING A CYBERWAR CAMPAIGN

Why a Campaign?
Whose Campaign?
The Challenge of Skepticism over the Potential of Tactical Cyberwar
The Insertion of Tactical Cyberwar into Kinetic Operations
Escalation and Tactical Cyberwar

CHAPTER 9. PROFESSIONALIZING CYBERWAR

Battle Damage Assessment
Collateral Damage
Other Weaponization Parameters
Should Cyberwar Authority Be Predelegated?
A Hacker Way of Warfare
Programming and Budgeting for Cyberwar

CHAPTER 10. IS CYBERSPACE A WARFIGHTING DOMAIN?

Cyberwar Operations Are about Usurping Command and Control
Cyberspace as Multiple Media
Defend the Domain or Ensure Missions?
Offensive Operations
Cyberspace as a Warfighting Domain and DDOS Attacks
Other Errors from Calling Cyberspace a Warfighting Domain
No Domain, No Cyber Equivalent of Billy Mitchell
Conclusions

CHAPTER 11. STRATEGIC IMPLICATIONS OF TACTICAL CYBERWAR

Influencing Others against Digitization
Cyberattacks and the Correlation of Forces

The Challenge of Alliance Defense in Cyberspace

CHAPTER 12. STABILITY IMPLICATIONS OF TACTICAL CYBERWAR

Attack Wins

Getting the Jump Wins

The Risks of Acting Are Reduced

The Risks of Not Acting Are Increased

A Missing Element of Caution

A Quick Comparison to Nuclear Weapons

Do Cyberattack Options Reduce Violence?

Conclusions

PART III. STRATEGIES

CHAPTER 13. STRATEGIC CYBERWAR

Strategic Cyberwar May Focus on Power Grids and Banks

How Coercive Can a Strategic Cyberwar Campaign Be?

The Conduct of Strategic Cyberwar

Indications and Warnings

A Cyber SIOP?

Keeping Targets in Reserve

Terminating Cyberwar

Conclusions

CHAPTER 14. CYBERWAR THREATS AS DETERRENCE AND COMPULSION

The Anger/Fear Balance

The Difficulty of Evaluating a Coercive Campaign

A Stalling Strategy for Compulsion

A Deterrence Response Window

CHAPTER 15. THE UNEXPECTED ASYMMETRY OF CYBERWAR

The Third World Disadvantage

The Particular U.S. Advantage

Was This All an Exercise in Nostalgia?
A Silver Lining Arising from Kerckhoffs's Principle
The Influence of Third Parties on the Balance of Power in
Cyberspace

CHAPTER 16. RESPONDING TO CYBERATTACK

First-Strike Cyberattacks May Have a Variety of Motives
What Looks like an Unprovoked Cyberattack May Not Be
Should the Target Reveal the Cyberattack—and When?
A Delayed Response
Responding without Force
Economic Responses
Sanctions until the Behavior Ends
The Perils of an Easy Response
Sub-Rosa Cyberwar
A Drawback to Any Response
How Will the Attacker Respond to Retaliation?
Conclusions

CHAPTER 17. DETERRENCE FUNDAMENTALS

Cyberdeterrence Differs from Nuclear and Criminal Deterrence
The Rationale for Deterrence
What Makes Deterrence Work?
The Core Message of Deterrence
Tailored Deterrence
The Problematic Nature of Cyberdeterrence

CHAPTER 18. THE WILL TO RETALIATE

The Risks of Reprisals
Third-Party Cyberattacks
Retaliation May Be Stymied by Bigger Issues on the Table
Credibility May Not Be Easy to Establish
The Signals Associated with Carrying Out Reprisals May Get
Lost in the Noise
The Impact of Good Defenses on Credibility Is Mixed
Can Extended Deterrence Work in Cyberspace?

A Baltic Cyberspace Alliance?
Conclusions

CHAPTER 19. ATTRIBUTION

What Will Convince Others of Your Attribution?
How Good Would Attribution Be?
What Could Make Attribution So Hard?
When Attribution Seems to Work
When Can Countries Be Blamed for What Starts within Their Borders?
Why Credibility Makes Attribution an Issue
Will the Attacker Always Avoid Attribution?
Why an Attacker May Favor Ambiguous Attribution over None at All
What Should Be Revealed about Attribution?
Attribution in a Post-Truth World
Conclusion

CHAPTER 20. WHAT THRESHOLD FOR RESPONSE?

A Zero-Tolerance Policy?
Non-Zero Thresholds
Did NotPetya Cross What Would Be a Reasonable Threshold?
Should Pulled or Failed Punches Merit Retaliation?
Compulsion versus Deterrence
Threshold Issues Complicate Retaliating against Cyberespionage

CHAPTER 21. A DETERMINISTIC POSTURE

Advantages of Determinism
Advantages of a Probabilistic Deterrence Posture
The Choice to Retaliate under Uncertainty

CHAPTER 22. PUNISHMENT AND HOLDING TARGETS AT RISK

The Lack of Good Targets for Intradomain Deterrence
The Temptations of Cross-Domain Deterrence
Will Targets Actually Hit Back at All?

Can Secondary Deterrence Address the Problems of Primary Deterrence?

Persistent Engagement qua Deterrence

Summary Observations on Cyberdeterrence

CHAPTER 23. CYBERWAR ESCALATION

The Purpose and Risks of Escalation

Escalation in Strategic Cyberwar

The Difficulties of Tit-for-Tat Management

Escalation into Kinetic Warfare

Escalation Risks from Proxy Cyberwar

Proxy Cyberattacks

Conclusions

CHAPTER 24. BRANDISHING CYBERATTACK CAPABILITIES

What Brandishing Is

Your Power or Their Powerlessness?

How to Brandish Cyberattack Capabilities

Brandishing Implants

Escalation Dominance and Brandishing

Counter-Brandishing

Caveats and Cautions

CHAPTER 25. NARRATIVES AND SIGNALS

Narratives to Facilitate Crisis Control

A Narrative Framework for Cyberspace

Narratives as Morality Plays

Narratives to Walk Back a Crisis

Narrative, Attribution, and Response

Signaling

What Can We Say with Signals That Would Come as News to Others?

Ambiguity in Signaling

Why Narratives Matter to Signals

CHAPTER 26. CYBERATTACK INFERENCES FROM CYBERESPIONAGE

- Inferring Cyberattacks from Cyberespionage
- Inferences from the Fact of Cyberespionage Alone
- How to Continue with Cyberespionage with Less Risk
- Stick with Attacks on Offensive Systems?
- The Defender's Options
- Deliberate Signaling, Both Friendly and Hostile
- Conclusions

CHAPTER 27. STRATEGIC STABILITY

- Would Nuclear Dilemmas Echo in Cyberspace?
- Misperception as a Source of Crisis
- Excessive Confidence in Attribution or Preemption
- Can There Be a Cuban Missile Crisis in Cyberspace?
- Conclusions

PART IV. NORMS

CHAPTER 28. NORMS FOR CYBERSPACE

- Unilateral Red Lines and Multilateral Norms
- Red Lines versus Norms
- The Criminalization of Hacking
- Norms on Attribution
- Arms Control
- Normalization
- Law of Armed Conflict: Jus in bello
- Law of Armed Conflict: Jus ad bellum
- From the Tallinn Manual to Las Vegas Rules
- What the Tallinn Manual Says
- Viva Las Vegas
- But Not So Fast
- Why Not Las Vegas Rules for Outer Space as Well?
- Conclusions

CHAPTER 29. THE ROCKY ROAD TO CYBERESPIONAGE NORMS

Norms against Economically Motivated Cyberespionage
The Cybercrime Markets Norm
The No-Political-Doxing Norm
Prohibiting Certain Targets to Prohibit Unwelcome Uses of Purloined Information
Cyberespionage against Critical Infrastructure
Getting to Norms

CHAPTER 30. SINO-AMERICAN RELATIONS AND NORMS IN CYBERSPACE

The United States Advocates Its Norms
Can We Trade?
The Deal That Was Struck

CHAPTER 31. THE ENIGMA OF RUSSIAN BEHAVIOR IN CYBERSPACE

The Early Years
After Maidan
What Happened to Cyberwar in the Russo–Ukraine Conflict?
Cyberattacks to Support Narratives
Conclusions

CHAPTER 32. CYBERSECURITY FUTURES

Better Offense
A Larger Attack Surface
Better Defense
Artificial Intelligence
A Three Mile Island in Cyberspace

CHAPTER 33. CYBERWAR: WHAT IS IT GOOD FOR?

Notes

Bibliography

Index

Illustrations

TABLES

- 1.1 Noteworthy Incidents in Cyberspace
- 12.1 Kinetic/Cyber Preferences and Outcomes

FIGURES

- 2.1 Hierarchical Decomposition of Unwanted Cyberspace Events
- 17.1 Cost-Effective Curves for Cyberattacks
- 22.1 Various Types of Deterrence-by-Punishment
- 23.1 An Inadvertent Path to Mutual Escalation