

Table of Contents

<i>List of Contributors</i>	xxiii
<i>Table of Cases</i>	xxvi
<i>Table of Legislation and Executive Orders</i>	xxviii
<i>Table of Treaties and Conventions</i>	xxix
<i>List of Abbreviations</i>	xxxi

PART I: FOUNDATIONAL QUESTIONS OF CYBERWAR

1. The Nature of War and the Idea of “Cyberwar”	3
<i>Larry May</i>	
2. Is There Anything Morally Special about Cyberwar?	16
<i>James L Cook</i>	
3. Cyber Causation	37
<i>Jens David Ohlin</i>	

PART II: CONCEPTUALIZING CYBER ATTACKS: THE CIVIL-MILITARY DIVIDE

4. Cyberterrorism and Enemy Criminal Law	57
<i>Stuart Macdonald</i>	
5. Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace	76
<i>Laurie R Blank</i>	
6. The Rise of Non-State Actors in Cyberwarfare	102
<i>Nicolò Bussolati</i>	

PART III: CYBERSECURITY AND INTERNATIONAL HUMANITARIAN LAW: THE ETHICS OF HACKING AND SPYING

7. Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?	129
<i>Duncan B Hollis</i>	
8. Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures	175
<i>Christopher S Yoo</i>	
9. Deception in the Modern, Cyber Battlespace	195
<i>William H Boothby</i>	

PART IV: RESPONSIBILITY AND ATTRIBUTION IN
CYBER ATTACKS

10. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations <i>Marco Roscini</i>	215
11. Low-Intensity Cyber Operations and the Principle of Non-Intervention <i>Sean Watts</i>	249
<i>Index</i>	271