

TABLE OF CONTENTS

Introduction	1
<i>Retorsion as a Response to Ongoing Malign Cyber Operations</i> Jeff Kosseff	9
<i>Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?</i> Przemysław Roguski	25
<i>Up in the Air: Ensuring Government Data Sovereignty in the Cloud</i> Neal Kushwaha, Przemysław Roguski and Bruce W. Watson	43
<i>Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection</i> Livinus Nweke and Stephen Wolthusen	63
<i>Making the Cyber Mercenary – Autonomous Weapons Systems and Common Article 1 of the Geneva Conventions</i> Aleksi Kajander, Agnes Kasper and Evhen Tsybulenko	79
<i>Cyber Weapons Review in Situations Below the Threshold of Armed Conflict</i> Ivana Kudláčková, David Wallace and Jakub Harašta	97
<i>R2P & Cyberspace: Sovereignty as a Responsibility</i> Tina J. Park and Michael Switzer	113
<i>The Past, Present, and Future of Russia's Cyber Strategy and Forces</i> Bilyana Lilly and Joe Cheravitch	129
<i>Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) During the Ukrainian Crisis</i> Frédéric Douzet, Louis Pétiñiaud, Loqman Salamatian, Kevin Limonier, Kavé Salamatian and Thibaut Alchus	157

<i>Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations</i> Matthias Schulze	183
<i>Correlations Between Cyberspace Attacks and Kinetic Attacks</i> Martin C. Libicki	199
<i>Problems of Poison: New Paradigms and “Agreed” Competition in the Era of AI-Enabled Cyber Operations</i> Christopher Whyte	215
<i>The Next Generation of Cyber-Enabled Information Warfare</i> Kim Hartmann and Keir Giles	233
<i>Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations</i> Jason Healey, Neil Jenkins and JD Work	251
<i>Using Global Honeypot Networks to Detect Targeted ICS Attacks</i> Michael Dodson, Alastair R. Beresford and Mikael Vingaard	275
<i>Addressing the Cybersecurity Challenges of Electrical Power Systems of the Future</i> Gilberto Pires de Azevedo, Maxli Barroso Campos and Paulo César Pellanda	293
<i>Towards Classifying Devices on the Internet Using Artificial Intelligence</i> Artūrs Lavrenovs, Roman Graf and Kimmo Heinäaro	309
<i>Hacking the AI – The Next Generation of Hijacked Systems</i> Kim Hartmann and Christoph Steup	327
<i>Recent Developments in Cryptography</i> Lubjana Beshaj and Andrew O. Hall	351
Biographies	369