
Contents

Introduction	xi
Sébastien-Yves LAURENT	
Chapter 1. The United States, States and the False Claims of the End of the Global Internet	1
Sébastien-Yves LAURENT	
1.1. Introduction.	1
1.2. The creation of the internet and the development of cyberspace by the United States	2
1.2.1. The first international telecommunications systems developed by all states.	3
1.2.2. The creation and development of the internet by the United States	3
1.2.3. International management controlled by the United States	4
1.2.4. A sociotechnical system bearing a composite American ideology	10
1.2.5. The false recomposition of the global sociotechnical system: the global summits on the information society	11
1.3. Cyberspace transformed by the arrival in force of states	13
1.3.1. State intentions in “national strategies”: a global approach	14
1.3.2. Russian–American structural disagreements on information security and cybersecurity	16
1.3.3. Discussions on cybersecurity: the symbolic international restoration of the coercive state	18

1.4. Praxis of state coercion in cyberspace	20
1.4.1. Intelligence and surveillance activities in the digital environment	21
1.4.2. Non-military cyber operations	24
1.4.3. Interstate digital conflicts, secrecy and coercive diplomacy	26
1.5. The fragmentation of the global internet and the digital sovereignty of states	29
1.5.1. Linguistic balkanization: Digital Babel	29
1.5.2. Political fragmentation: alternative internets	31
1.6. The strong constraint of interstate cooperation for all states	33
1.6.1. Interstate agreements on an embryo of international law	33
1.6.2. State dependence on international cooperation for cybersecurity	34
1.7. Conclusion	35
1.8. References	36
Chapter 2. Cybersecurity in America: The US National Security Apparatus and Cyber Conflict Management	43
Frédéric GAGNON and Alexis RAPIN	
2.1. Introduction	43
2.2. Societal and institutional dynamics	45
2.3. Organizational and bureaucratic dynamics	49
2.4. Individual dynamics	53
2.5. Conclusion	57
2.6. References	58
Chapter 3. Separation of Offensive and Defensive Functions: The Originality of the French Cyberdefense Model Called into Question?	63
Alix DESFORGES	
3.1. Introduction	63
3.2. A model designed and developed in response to the threats and challenges of the early 2010s	66
3.2.1. An organizational model apparently based on two main actors	66
3.2.2. The commitment to a strict offensive/defensive separation	71
3.3. A strict separation of offensive and defensive functions and missions: an obstacle to better defense?	75
3.3.1. A rapidly changing context: an increasingly significant threat from the most advanced states	76

3.3.2. Limits that have become obstacles to accomplishing cyberdefense missions	78
3.3.3. An institutionalized rapprochement of the actors of defensive and offensive parts in the name of cyberdefense missions: from mitigation to obliteration?	82
3.4. Conclusion	85
3.5. References	86

**Chapter 4. The Boundary Between Cybercrime and Cyberwar:
An Uncertain No-Man’s Land 89**

Marc WATIN-AUGOUARD

4.1. Introduction.	89
4.2. The field of cybercrime up to the limits of the glass ceiling	91
4.2.1. The field of cybercrime: an attempt at delimitation	92
4.2.2. Cybercrime, the “21st century crime”	95
4.2.3. Cyber conflict at the edge of the glass ceiling	95
4.3. War in cyberspace, cyber in war	98
4.3.1. Cyber in war, a daily reality.	98
4.3.2. Autonomous warfare in the cyber world: the test of the law of armed conflict	99
4.3.3. Digital cyber persuasion	102
4.4. Conclusion	104
4.5. References	105

**Chapter 5. Cyberdefense, the Digital Dimension of National
Security 107**

Bertrand WARUSFEL

5.1. Introduction.	107
5.2. Cyberdefense in the political and legal framework of digital security	108
5.2.1. A definition of cyberdefense	108
5.2.2. Linking cyberdefense to national security strategy	109
5.3. The emergence of a coherent legal regime for cyberdefense	111
5.3.1. The legal basis of the permanent cyberdefense posture	111
5.3.2. Exceptional instruments for responding to a crisis	112
5.4. Conclusion	115
5.5. References	116

Chapter 6. Omnipresence Without Omnipotence: The US Campaign Against Huawei in the 5G Era	117
Mark CORCORAL	
6.1. Introduction.	117
6.2. The unilateral American offensive against Huawei: a disruptive campaign causing significant collateral damage	119
6.2.1. Huawei: an “unusual and extraordinary” threat to the United States’ position in the international order	120
6.2.2. A political, legal and economic offensive against Huawei, causing significant collateral damage	122
6.3. The American diplomatic offensive: the limits of American rhetorical coercion of their partners and allies	128
6.3.1. Educating rather than persuading: an attempt to rhetorically coerce partners and allies	129
6.3.2. Successful agenda setting but limited rhetorical coercion	131
6.3.3. American rhetorical coercion in the special relationship.	134
6.4. The anti-Huawei offensive: a barometer of American power?.	137
6.5. References	139
Chapter 7. The Issue of Personal and Sovereign Data in the Light of an Emerging “International Law of Intelligence”	147
Fabien LAFOUASSE	
7.1. Introduction.	147
7.2. The legal rules invoked in the collection of personal and sovereign data	150
7.2.1. Right to privacy versus general communications surveillance	150
7.2.2. Violation of territorial sovereignty versus cyberespionage	153
7.3. Data localization in the light of international intelligence law	156
7.3.1. Data fluidity versus data storage	156
7.3.2. Datasphere versus international intelligence law	159
7.4. Conclusion	163
7.5. Appendix: the quadrants of intelligence law	164
7.6. Sources and references	165
7.6.1. Sources	165
7.6.2. References	166
Chapter 8. International Cybersecurity Cooperation	169
Guillaume POUPARD	
8.1. Current attack trends	169

8.2. The multiple paths of international cooperation 171
 8.3. The issue of attack attribution 175

Chapter 9. Cyberdefense and Cybersecurity Regulations in the United States: From the Failure of the “Comprehensive Policy” to the Success of the Sectoral Approach. 177

Adrien MANNIEZ

9.1. Introduction. 177
 9.2. The identification of a new threat and the impact of cyber on how US security and defense policies are designed. 178
 9.3. From the impact of cyber on policy to the impact of politics on cyber. 181
 9.4. From a comprehensive cyber policy to a sectoral approach: the success of an undeclared regulatory policy. 190
 9.5. Conclusion 195
 9.6. References 196

List of Authors 199

Index 201