

Contents

<i>List of figures</i>	ix
<i>List of tables</i>	x
<i>About the author</i>	xi
<i>Preface</i>	xiii
<i>Post script</i>	xvi
<i>List of abbreviations</i>	xvii

PART I BACKGROUND FOR CYBERSECURITY LAW

1	Introduction: Cybersecurity and cybersecurity law	2
1.1	Defining cybersecurity	2
1.2	Cybersecurity law: Overview of the book	6
2	Cyberspace, security, and law	11
2.1	What is ‘security’ in ‘cyberspace’?	11
2.1.1	What is the ‘internet’?	11
2.1.2	What is ‘cyberspace’?	13
2.1.3	What is ‘security’?	14
2.2	What is internet governance?	17
2.3	What is cybersecurity governance?	21
2.4	What is the role of law in cybersecurity governance?	23
2.4.1	The functions of law and technological change	23
2.4.2	Domestic law and cybersecurity governance	24
2.4.3	International law and cybersecurity governance	25

PART II CYBERSECURITY AND NON-STATE ACTORS: CRIME AND TERRORISM IN CYBERSPACE

3	Cybercrime	30
3.1	The cybercrime problem	30
3.2	Cybercrime and domestic law	32
3.2.1	Jurisdictional issues	33
3.2.2	Substantive criminal law	34
3.2.3	Criminal procedure and law-enforcement access to electronic data and communications	36
3.2.4	Law enforcement, encryption, and ‘going dark’	37
3.2.5	‘Harden the target’ and ‘hacking back’: Cyber defence and cyber deterrence	39
3.3	Cybercrime and international law	41
3.3.1	Sovereignty, non-intervention, and jurisdiction to prescribe and enforce law	41
3.3.2	Extradition and mutual legal assistance treaties	42
3.3.3	Harmonizing domestic law and facilitating law-enforcement cooperation through cybercrime treaties	45
3.3.4	International law and cybercrime: Cyber defence and cyber deterrence	49
4	Cyber terrorism	55
4.1	The cyber terrorism problem	55
4.2	Cyber terrorism and criminal law	57
4.2.1	Criminalizing acts of, support for, and glorification and incitement of terrorism	57
4.2.2	International law and the criminalization of terrorism	60
4.2.3	Criminal law, terrorism, and cyber terrorism	65
4.3	Protecting critical infrastructure from terrorism	66
4.3.1	Critical-infrastructure protection and domestic law	66
4.3.2	Critical-infrastructure protection and international law	67
4.4	Counterterrorism, electronic surveillance, and cybersecurity	69

4.4.1	Counterterrorism, electronic surveillance, and domestic law	69
4.4.2	Counterterrorism, electronic surveillance, and international law	72
4.5	International law and state responsibility for combating terrorism	74

PART III CYBERSECURITY AND STATE ACTORS: ESPIONAGE AND WAR IN CYBERSPACE

5	Cyber espionage	78
5.1	The cyber espionage problem	79
5.2	Cyber espionage and international law	81
5.2.1	The traditional approach to espionage under international law	81
5.2.2	Cyber espionage and rethinking the traditional approach to espionage under international law	82
5.2.3	Cyber espionage, economic cyber espionage, and the extraterritorial application of international law	84
5.3	Domestic law and cyber espionage	90
5.3.1	Conducting cyber espionage	91
5.3.2	Defending against cyber espionage	93
5.3.3	Balancing cyber offence and defence: The zero-day vulnerability problem	98
5.4	Beyond cyber espionage: Covert cyber operations	101
6	Cyber war	104
6.1	The cyber war problem	105
6.2	Going to war in cyberspace: Domestic law and war powers	108
6.2.1	Stuxnet as a case study	109
6.2.2	War powers in domestic law	110
6.3	Going to war in cyberspace: International law on the use of force	112

6.3.1	The prohibition of the use of force and the right to use force in self-defence	112
6.3.2	Determining what is a 'use of force' and an 'armed attack'	114
6.3.3	Responding to a use of force or an armed attack	116
6.3.4	Anticipatory self-defence	117
6.3.5	The principles on state responsibility	119
6.3.6	The act and crime of aggression	120
6.3.7	Security Council authorization of the use of force	121
6.3.8	Humanitarian intervention	122
6.3.9	Cyber operations not constituting uses of force	122
6.4	Fighting armed conflict in cyberspace	127
6.4.1	Background on international humanitarian law	127
6.4.2	Cyber operations and armed conflict	129
6.4.3	Cyber operations during international armed conflict	136
6.4.4	Cyber operations during non-international armed conflict	137
6.5	Arms control and cyber weapons	138
6.5.1	Arms control strategies	139
6.5.2	Confidence-building measures	140
6.5.3	Export control strategies	140
7	Conclusion: Cybersecurity law in a divided world	142
7.1	Taking stock of cybersecurity law	142
7.1.1	Cybersecurity and non-state actors: Cybercrime and cyber terrorism	142
7.1.2	Cybersecurity and state actors: Cyber espionage and cyber war	144
7.2	Cybersecurity's 20 years' crisis	145
7.3	The next decade in cybersecurity law	148
7.3.1	International law	148
7.3.2	Domestic law	149
7.4	Final thoughts	150
	<i>Index</i>	152