Law, Governance and Technology Series 32

Kriangsak Kittichaisaree

Public International Law of Cyberspace

Springer

Law, Governance and Technology Series

Volume 32

The *Law-Governance and Technology Series* is intended to attract manuscripts arising from an interdisciplinary approach in law, artificial intelligence and information technologies. The idea is to bridge the gap between research in IT law and IT applications for lawyers developing a unifying techno-legal perspective. The series will welcome proposals that have a fairly specific focus on problems or projects that will lead to innovative research charting the course for new interdisciplinary developments in law, legal theory, and law and society research as well as in computer technologies, artificial intelligence and cognitive sciences. In broad strokes, manuscripts for this series may be mainly located in the fields of the Internet law (data protection, intellectual property, Internet rights, etc.), Computational models of the legal contents and legal reasoning, Legal Information Retrieval, Electronic Data Discovery, CollaborativeTools (e.g. Online Dispute Resolution platforms), Metadata and XML Technologies (for Semantic Web Services), Technologies in Courtrooms and Judicial Offices (E-Court), Technologies for Governments and Administrations (E-Government), Legal Multimedia, and Legal Electronic Institutions (Multi-Agent Systems and Artificial Societies).

More information about this series at http://www.springer.com/series/8808

Kriangsak Kittichaisaree

Public International Law of Cyberspace

Springer

Kriangsak Kittichaisaree
Royal Thai Embassy
Moscow, Russia

ISSN 2352-1902 ISSN 2352-1910 (electronic)
Law, Governance and Technology Series
ISBN 978-3-319-85446-5 ISBN 978-3-319-54657-5 (eBook)
DOI 10.1007/978-3-319-54657-5

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

After finishing my mandate as chairman of the United Nations International Law Commission's Open-Ended Working Group on the topic *obligation to extradite or prosecute* (aut dedere aut judicare) in 2014, I was interested in taking up the topic *protection of personal data in transborder flow of information*, which had been put on the International Law Commission's long-term programme of work since 2006. However, I have eventually concluded that this latter topic is too narrow in its scope to meet the pressing needs of the international community.

Cyberspace has become one of the domains for everyday human interaction in almost all corners of the earth. Clandestine cyber surveillance, cyber crimes, and cyber espionage are now common phenomenons. While cyber warfare resulting in large-scale catastrophes and cyber terrorism may seem remote possibilities, in the age of fast-developing cyber innovations there is no reason for complacency and international law must be ready to meet any present and future challenge.

At international meetings both inside and outside of the United Nations system, States have expressed their positions on cyber activities and sought international legal bases to support their respective positions. Most international lawyers and governments also agree that the relevant rules of existing international law regulate cyberspace. Opinions diverge, though, on which rules are to be applied and how. This book will endeavour to provide practical and objective answers to the cyber-related international legal issues considered to be of importance by States, international organizations, individuals, and corporations, as well as other actors.

Being one of the 19 members of the International Group of Experts of the NATO Cooperative Cyber Defence Centre of Excellence entrusted with writing *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, or *Tallinn Manual 2.0*, has immensely enriched my knowledge about the international law governing cyberspace. Although this book of mine is intended for different readers and focuses on broader issues than the *Tallinn Manual 2.0*, I am beholden to all my colleagues in the Group since our brainstorming sessions have clarified so many aspects of the law.

I am grateful to the valuable comments of the two anonymous reviewers and to the efficient editorial and production teams at Springer. The research for this book

would not have been possible without the excellent facilities and support of the United Nations Office at Geneva Library, especially its law librarians. I am also appreciative of the assistance of Margaux V. Roussel (JD candidate 2017, The George Washington University Law School) and Francesca Dal Poggetto (Master in International Law candidate 2017, Graduate Institute of International and Development Studies, Geneva), who helped me with American and European case references, respectively. The views in this book are my personal views and, unless otherwise indicated, do not necessarily reflect those of the institutions to which I belong or used to belong.

Royal Thai Embassy
Moscow, Russia
9 January 2017

Kriangsak Kittichaisaree

Contents

1 Introduction: Perspectives of Various Stakeholders and Challenges for International Law 1
1.1 Perspectives of Stakeholders 1
1.2 General Introduction to Public International Law 15
1.3 Food for Thought 21

2 Jurisdiction and Attribution of State Responsibility in Cyberspace 23
2.1 Jurisdiction 23
2.2 Attribution of State Responsibility 32
2.2.1 ILC's Draft Articles on State Responsibility 36
2.2.2 Standard(s) of Proof 40
2.2.3 Attribution and International Organizations, Such As NATO 43

3 Regulation of Cyberspace and Human Rights 45
3.1 General Background 45
3.2 Human Rights in Cyberspace 53
3.2.1 Privacy and Related Rights 54
3.2.2 Right to the Freedom of Expression 84
3.2.3 Anonymity and the Right to Be Forgotten 87
3.3 Exceptions 94
3.3.1 European Practice 101
3.3.2 US Practice 111
3.3.3 Some Examples of Practice in Other Global Regions 128
3.4 Territorial Scope of Human Rights Protection and Extraterritorial Jurisdiction Regarding Search Warrants and Other Law Enforcement Measures 132
3.5 Food for Thought 150

4 Cyber Warfare 153
4.1 Cyberattack 153
4.2 Cyber Warfare 158
4.3 Cyber Weapons 160
4.4 Use of Force Under International Law 161
4.5 Armed Attack and the Right of Self-Defence 166
4.6 Self-Defence Against Non-State Actors 175
4.7 Countermeasures 191
4.8 Necessity 192
4.9 Reprisals 193
4.10 Retorsion 194
4.11 Neutrality in Cyberspace 195
4.12 Cyber Disarmament 196

5 Application of the Law of Armed Conflict, Including International Humanitarian Law, In Cyberspace 201
5.1 The Law of Armed Conflict/International Humanitarian Law 202
5.2 International Armed Conflict 208
5.3 Non-international Armed Conflict 224
5.4 War Crime of Terrorism 228
5.5 Food for Thought 229

6 Cyber Espionage 233
6.1 Modus Operandi 234
6.2 Targets 236
6.3 International Law on Espionage 241
6.4 Food for Thought 260

7 Cyber Crimes 263
7.1 Cyber Crimes: The Challenges 263
7.2 Budapest Convention: Model for Universal Suppression of Cyber Crimes 270
7.3 Beyond the Budapest Convention 292

8 Cyber Terrorism 295
8.1 Acts of Terrorism Against Civil Aviation 299
8.2 Acts of Terrorism Against Potential Victims 308
8.3 Acts of Terrorism at Sea 310
8.4 Acts of Terrorism Relating to Dangerous Materials 313
8.5 Terrorist Financing 318
8.6 Developments Beyond the Sectoral Conventions 322
8.7 National Laws 324

9 Future Prospects of Public International Law of Cyberspace 335
9.1 Stocktaking 335
9.2 Cybersecurity 343
9.3 Cyber Deterrence 343
9.4 Cyberspace Governance 347
9.5 Cyber Sovereignty 352

Glossary 357

Bibliography 359

Law, Governance an

Kriangsak Kittichaisa

Public Internat

This compact, hig
the conduct of Sta
to the use of cyberspace. Chapters introduce the perspectives of various stakeholders and the challenges for international law. The author discusses State responsibility and key cyberspace rights issues, and takes a detailed look at cyber warfare, espionage, crime and terrorism. The work also covers the situation of non-State actors and quasi-State actors (such as IS, or ISIS, or ISIL) and concludes with a consideration of future prospects for the international law of cyberspace.

Readers may explore international rules in the areas of jurisdiction of States in cyberspace, responsibility of States for cyber activities, human rights in the cyber world, permissible responses to cyber attacks, and more. Other topics addressed include the rules of engagement in cyber warfare, suppression of cyber crimes, permissible limits of cyber espionage, and suppression of cyber-related terrorism. Chapters feature explanations of case law from various jurisdictions, against the background of real-life cyber-related incidents across the globe. Written by an internationally recognized practitioner in the field, the book objectively guides readers through on-going debates on cyber-related issues against the background of international law.

This book is very accessibly written and is an enlightening read. It will appeal to a wide audience, from international lawyers to students of international law, military strategists, law enforcement officers, policy makers and the lay person.

Law

ISBN 978-3-319-85446-5
9 "783319"854465"

▶ springer.com