

Russell Buchan



# Cyber Espionage

and International Law

# Cyber Espionage

## and International Law

Russell Buchan

The advent of cyberspace has led to a dramatic increase in state-sponsored political and economic espionage. This monograph argues that these practices represent a threat to the maintenance of international peace and security and assesses the extent to which international law regulates this conduct. The traditional view among international legal scholars is that, in the absence of direct and specific international law on the topic of espionage, cyber espionage constitutes an extra-legal activity that is unconstrained by international law. This monograph challenges that assumption and reveals that there are general principles of international law as well as specialised international legal regimes that indirectly regulate cyber espionage. In terms of general principles of international law, this monograph explores how the rules of territorial sovereignty, non-intervention and the non-use of force apply to cyber espionage. In relation to specialised regimes, this monograph investigates the role of diplomatic and consular law, international human rights law and the law of the World Trade Organization in addressing cyber espionage. This monograph also examines whether developments in customary international law have carved out espionage exceptions to those international legal rules that otherwise prohibit cyber espionage as well as considering whether the doctrines of self-defence and necessity can be invoked to justify cyber espionage. Notwithstanding the applicability of international law, this monograph concludes that policymakers should nevertheless devise an international law of espionage which, as *lex specialis*, contains rules that are specifically designed to confront the growing threat posed by cyber espionage.





## CYBER ESPIONAGE AND INTERNATIONAL LAW

The advent of cyberspace has led to a dramatic increase in state-sponsored political and economic espionage. This monograph argues that these practices represent a threat to the maintenance of international peace and security and assesses the extent to which international law regulates this conduct. The traditional view among international legal scholars is that, in the absence of direct and specific international law on the topic of espionage, cyber espionage constitutes an extra-legal activity that is unconstrained by international law. This monograph challenges that assumption and reveals that there are general principles of international law as well as specialised international legal regimes that indirectly regulate cyber espionage. In terms of general principles of international law, this monograph explores how the rules of territorial sovereignty, non-intervention and the non-use of force apply to cyber espionage. In relation to specialised regimes, this monograph investigates the role of diplomatic and consular law, international human rights law and the law of the World Trade Organization in addressing cyber espionage. This monograph also examines whether developments in customary international law have carved out espionage exceptions to those international legal rules that otherwise prohibit cyber espionage as well as considering whether the doctrines of self-defence and necessity can be invoked to justify cyber espionage. Notwithstanding the applicability of international law, this monograph concludes that policymakers should nevertheless devise an international law of espionage which, as *lex specialis*, contains rules that are specifically designed to confront the growing threat posed by cyber espionage.



# Cyber Espionage and International Law

Russell Buchan



• HART •

OXFORD • LONDON • NEW YORK • NEW DELHI • SYDNEY

HART PUBLISHING

Bloomsbury Publishing Plc

Kemp House, Chawley Park, Cumnor Hill, Oxford, OX2 9PH, UK

HART PUBLISHING, the Hart/Stag logo, BLOOMSBURY and the Diana logo are trademarks of Bloomsbury Publishing Plc

First published in Great Britain 2019

Reprinted 2019

Copyright © Russell Buchan, 2019

Russell Buchan has asserted his right under the Copyright, Designs and Patents Act 1988 to be identified as Author of this work.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage or retrieval system, without prior permission in writing from the publishers.

While every care has been taken to ensure the accuracy of this work, no responsibility for loss or damage occasioned to any person acting or refraining from action as a result of any statement in it can be accepted by the authors, editors or publishers.

All UK Government legislation and other public sector information used in the work is Crown Copyright ©. All House of Lords and House of Commons information used in the work is Parliamentary Copyright ©. This information is reused under the terms of the Open Government Licence v3.0 (<http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3>) except where otherwise stated.

All Eur-lex material used in the work is © European Union,  
<http://eur-lex.europa.eu/>, 1998–2019.

A catalogue record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication data

Names: Buchan, Russell, 1983- author.

Title: Cyber espionage and international law / Russell Buchan.

Description: Oxford, UK ; Portland, Oregon : Hart, an imprint of Bloomsbury, 2019. | Includes bibliographical references and index.

Identifiers: LCCN 2018034245 | ISBN 9781782257349 (hardback : alk. paper)

Subjects: LCSH: Espionage—Law and legislation. | Internet in espionage.

Classification: LCC KZ4079 .B83 2018 | DDC 341.3—dc23 LC record available at <https://lcn.loc.gov/2018034245>

ISBN: HB: 978-1-78225-734-9

ePDF: 978-1-78225-735-6

ePub: 978-1-78225-736-3

Typeset by Compuscript Ltd, Shannon

Printed and bound by CPI Group (UK) Ltd, Croydon CR0 4YY

To find out more about our authors and books visit [www.hartpublishing.co.uk](http://www.hartpublishing.co.uk). Here you will find extracts, author information, details of forthcoming events and the option to sign up for our newsletters.

---

## ACKNOWLEDGEMENTS

---

This project would not have been completed without the support and assistance of a number of institutions and individuals. I thank the University of Sheffield School of Law for providing me with the necessary resources to produce this monograph. I also extend my gratitude to the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, for hosting me during my sabbatical in late 2016. The Centre provided me with a warm and intellectually rich environment to pursue my research. This monograph has benefited from the many deep and stimulating conversations that I have had with Iñaki Navarrete on the topic of international law and espionage, which I enjoyed immensely. I thank Iñaki for assisting me with the research for chapter 5 of this monograph and I also thank Adam Keenaghan for meticulously editing the final manuscript. I am indebted to Cormac Behan, Patrick Capps, David Hayes, Clair Gammage, Tarcisio Gazzini, Gregory Messenger and Nicholas Tsagourias for reading through various chapters of this monograph and providing useful comments. On a personal level, I am grateful for the love and support of my husband, Shane, and I apologise once again for the many early mornings, late nights and lost weekends that you had to withstand during the course of this project. Finally, this monograph is dedicated to Juanita Patrick: your love, humour and happiness are dearly missed and we think about you every day.

Russell Buchan  
*June 2018*



---

# TABLE OF CONTENTS

---

<i>Acknowledgements</i> .....	v
<i>Table of Cases</i> .....	xi
<i>Table of Instruments</i> .....	xxi
Introduction .....	1
1. Background .....	1
2. The Argument .....	4
3. Chapter Overview .....	9
1. Defining Cyber Espionage .....	13
1. Introduction .....	13
2. The Intelligence Community .....	14
2.1. Sources of Information Collection .....	15
2.2. Open and Closed Sources .....	16
3. Cyber Espionage: The Copying of Confidential Data .....	17
4. Close and Remote Access Cyber Espionage .....	18
5. Secrecy and Cyber Espionage .....	19
6. Non-Consensual Information Gathering .....	20
7. Political and Economic Cyber Espionage and the Role of State and Non-State Actors .....	21
8. Cyber Espionage and International Law .....	25
9. Peacetime Cyber Espionage .....	26
10. Conclusion .....	27
2. Cyber Espionage and International Peace and Security .....	28
1. Introduction .....	28
2. Political Cyber Espionage .....	28
2.1. Realism .....	28
2.2. The International Society .....	31
2.3. Espionage and International Cooperation .....	36
3. Economic Cyber Espionage .....	41
4. Conclusion .....	46
3. Cyber Espionage and the Rules of Territorial Sovereignty, Non-Intervention and the Non-Use of Force .....	48
1. Introduction .....	48
2. The Rule of Territorial Sovereignty .....	49
2.1. Cyber Espionage and Control Over Cyber Infrastructure .....	51

2.2.	Cyber Espionage and the Performance of Inherently Governmental Functions.....	56
3.	The Rule of Non-Intervention .....	61
3.1.	<i>Domaine Réservé</i> .....	62
3.2.	Coercion.....	63
4.	The Prohibition on the Use of Force .....	65
5.	Conclusion.....	68
4.	Cyber Espionage and Diplomatic and Consular Law .....	70
1.	Introduction .....	70
2.	Cyber Espionage Against Diplomatic Missions and Consular Posts.....	71
2.1.	The Inviolability of Diplomatic and Consular Premises.....	72
2.1.1.	Premises.....	72
2.1.2.	The 'Special Duty' to Protect Premises.....	77
2.1.3.	Furnishings, Property and Means of Transport .....	80
2.2.	The Inviolability of Archives and Documents .....	83
2.3.	Freedom of Communication.....	86
3.	The Use of Diplomatic Missions and Consular Posts for Cyber Espionage.....	89
3.1.	Immunities for Diplomatic and Consular Officials.....	92
4.	Conclusion.....	94
5.	Cyber Espionage and International Human Rights Law .....	95
1.	Introduction .....	95
2.	The Extraterritorial Application of Human Rights Treaties .....	96
2.1.	ICCPR .....	97
2.2.	ECHR .....	101
3.	The Right to Privacy.....	105
4.	Restricting the Right to Privacy.....	109
4.1.	In Accordance with the Law.....	109
4.1.1.	Accessible .....	110
4.1.2.	Foreseeable .....	110
4.1.3.	Oversight .....	114
4.2.	Legitimate Aim.....	116
4.3.	Proportionality.....	119
5.	Conclusion.....	121
6.	Economic Cyber Espionage and the World Trade Organization .....	122
1.	Introduction .....	122
2.	Economic Cyber Espionage as a WTO 'Measure' .....	125
2.1.	'As Applied' Challenge.....	125
2.2.	'As Such' Challenge .....	127

3.	Nullification or Impairment of a Benefit.....	129
4.	Substantive Obligations under WTO Law .....	130
4.1.	Article 10 <i>bis</i> Paris Convention 1967 .....	130
4.1.1.	Who Qualifies as a National?.....	131
4.1.2.	What Amounts to Unfair Competition? .....	132
4.1.3.	What Measures Must Members Adopt to 'Assure to Nationals' of Other Members 'Effective Protection' Against Unfair Competition? .....	135
4.2.	Article 39.2 TRIPS 1994.....	137
4.2.1.	Who Qualifies as a National?.....	137
4.2.2.	Article 39.2 and Trade Secrets .....	138
4.2.3.	The Nature of the Obligation Imposed by Article 39.2 TRIPS.....	139
4.2.4.	Extraterritoriality.....	140
5.	Non-Violation Complaints.....	141
6.	Conclusion.....	143
7.	Cyber Espionage and the Existence of Customary International Law Exceptions.....	145
1.	Introduction .....	145
2.	Customary International Law .....	148
3.	State Practice .....	149
3.1.	Duration.....	150
3.2.	Generality .....	150
3.3.	Uniformity .....	151
3.4.	Public Acknowledgment.....	152
3.5.	Assessment.....	155
4.	<i>Opinio Juris</i> .....	160
4.1.	Acquiescence and Protest .....	163
4.2.	National Legislation.....	167
5.	Conclusion.....	168
8.	Cyber Espionage and the Doctrines of Self-Defence and Necessity .....	170
1.	Introduction .....	170
2.	The Doctrine of Self-Defence .....	171
2.1.	Armed Attack.....	173
2.2.	Necessity .....	175
2.3.	Proportionality.....	177
3.	The Doctrine of Necessity .....	179
3.1.	Essential Interest .....	180
3.2.	A Grave and Imminent Peril .....	182
3.3.	No Other Means to Safeguard an Essential Interest.....	184

x *Table of Contents*

3.4. Non-Contribution .....	185
3.5. Balancing of Interests .....	187
4. Conclusion.....	190
Conclusion .....	191
<i>Bibliography</i> .....	196
<i>Index</i> .....	205

'*Cyber Espionage and Intelligence* is a thorough examination of the practice of espionage. Grounding the analysis in the history of the foundational principles of espionage, it offers a superb job both in illustrating the case for their unique operation in addressing the contemporary challenges posed by new surveillance technologies.'

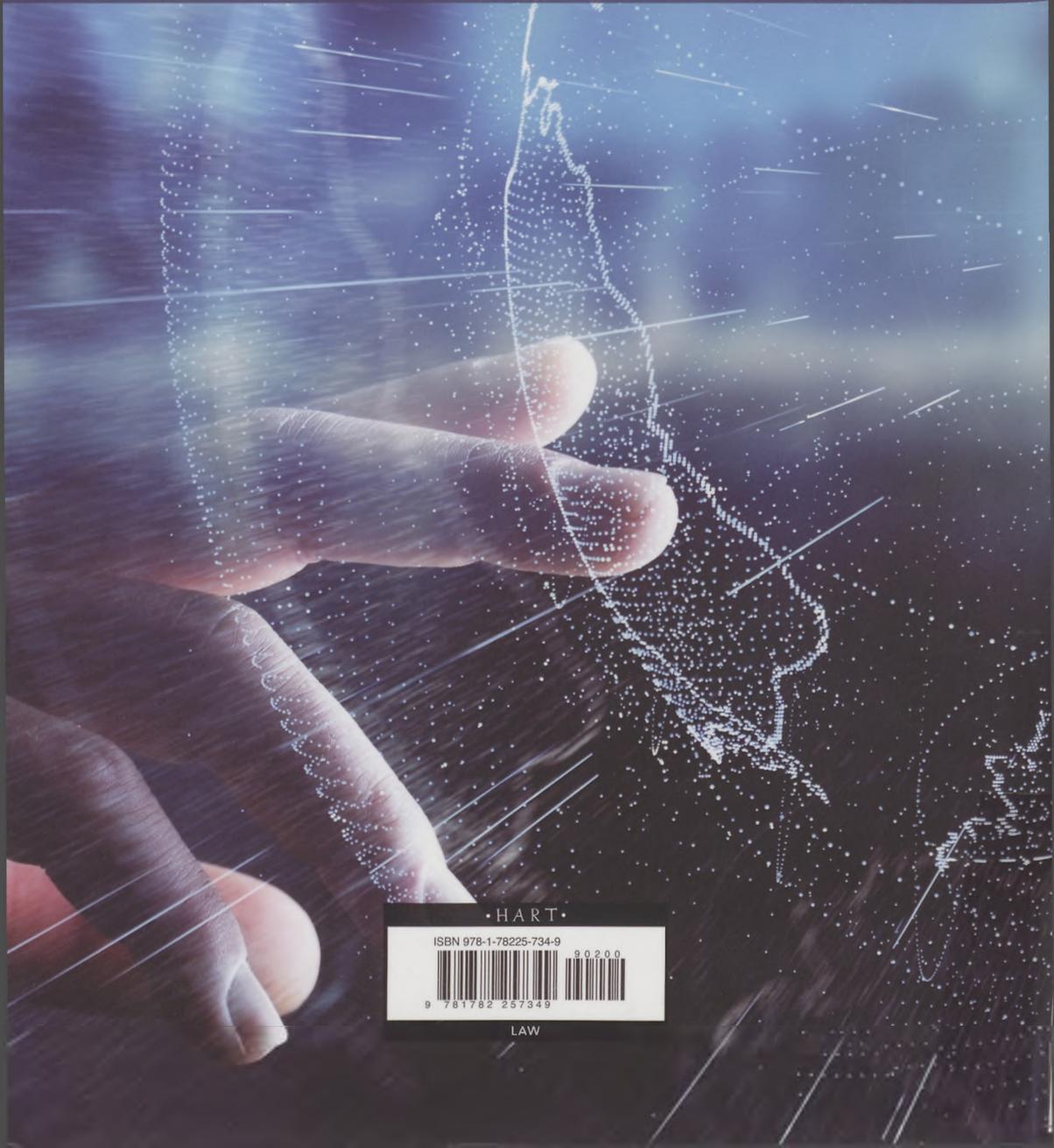
**Dr Asaf Lubin, Yale University**

Biblioteka Główna  
Akademii Sztuki Wojennej

26793/III (CB)



03-026793-000-0



• HART •

ISBN 978-1-78225-734-9



9 781782 257349

LAW