

OXFORD

Cyber Operations and the Use of Force in International Law

Marco Roscini



The internet has changed the rules of many industries, and war is no exception. But can a computer virus be classed as an act of war? Does a Denial of Service attack count as an armed attack? And does a state have a right to self-defence when attacked in cyberspace? With the range and sophistication of cyber attacks against states showing a dramatic increase in recent times, this book investigates the traditional concepts of 'use of force', 'armed attack', and 'armed conflict' and asks whether existing laws created for analogue technologies can be applied to new digital developments.

The book provides a comprehensive analysis of primary documents and surrounding literature to establish whether and how existing rules on the use of force in international law apply to cyber operations. In particular, it assesses the rules of the *jus ad bellum*, the *jus in bello*, and the law of neutrality (whether based on treaty or custom), and analyses why each rule applies or does not apply in the context of cyber operations. Those rules which can be seen to apply are then discussed in relation to each specific type of cyber operation. The book addresses the key questions of whether a cyber operation amounts to a use of force and, if so, whether the victim state may exercise its right of self-defence; whether cyber operations trigger the application of international humanitarian law when they are not accompanied by traditional hostilities; what rules must be followed in the conduct of cyber hostilities; how neutrality is affected by cyber operations; and whether those conducting cyber operations are combatants, civilians, or civilians taking direct part in hostilities. The book is essential reading for everyone wanting a better understanding of how international law regulates cyber combat.

Dr Marco Roscini is Reader in International Law at the University of Westminster School of Law.

CYBER OPERATIONS AND THE USE
OF FORCE IN INTERNATIONAL LAW

Cyber Operations and the Use of Force in International Law

MARCO ROSCINI



The Leverhulme Trust

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford, OX2 6DP,
United Kingdom

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries

© Marco Roscini 2014

The moral rights of the author have been asserted

First Edition published in 2014

Impression: 1

All rights reserved. No part of this publication may be reproduced, stored in
a retrieval system, or transmitted, in any form or by any means, without the
prior permission in writing of Oxford University Press, or as expressly permitted
by law, by licence or under terms agreed with the appropriate reprographics
rights organization. Enquiries concerning reproduction outside the scope of the
above should be sent to the Rights Department, Oxford University Press, at the
address above

You must not circulate this work in any other form
and you must impose this same condition on any acquirer

Crown copyright material is reproduced under Class Licence
Number C01P0000148 with the permission of OPSI
and the Queen's Printer for Scotland

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America

British Library Cataloguing in Publication Data
Data available

Library of Congress Control Number: 2013953298

ISBN 978-0-19-965501-4

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

Links to third party websites are provided by Oxford in good faith and
for information only. Oxford disclaims any responsibility for the materials
contained in any third party website referenced in this work.



*For Ludovica, Federico and Margherita,
children of the Information Age*

[E]ach period has had its own peculiar forms of War,
its own restrictive conditions, and its own prejudices.

Carl von Clausewitz, *On War*, Book VIII, Chapter III.B
(London: Kegan Paul, Trench, Trübner & Co, 1940), vol III, p 103

Contents

<i>Table of Cases</i>	xv
<i>Table of Legislation and Other Documents</i>	xix
<i>List of Abbreviations</i>	xxvii
1. Identifying the Problem and the Applicable Law	1
I. The Emergence of the Cyber Threat to International Security	1
II. The Taxonomy of Military Cyber Operations: Definitions and Classification	10
III. The Applicable Law: <i>Inter (Cyber) Arma Enim Silent Leges?</i>	19
IV. Identification and Attribution Problems	33
V. The Book's Scope and Purpose	40
2. Cyber Operations and the <i>jus ad bellum</i>	43
I. Introduction	43
II. Cyber Operations and the Prohibition of the Threat and Use of Force in International Relations	44
III. Cyber Operations and the Law of Self-Defence	69
IV. Remedies Against Cyber Operations Short of Armed Attack	104
V. Chapter VII of the United Nations Charter and the Role of the Security Council	110
VI. Conclusions	115
3. The Applicability of the <i>jus in bello</i> to Cyber Operations	117
I. Introduction	117
II. Cyber Operations in and as International Armed Conflicts	119
III. Cyber Operations During Partial or Total Belligerent Occupation	141
IV. Cyber Operations in and as Non-International Armed Conflicts	148
V. Cyber Operations as 'Internal Disturbances and Tensions'	159
VI. Conclusions	161
4. Cyber Operations and the Conduct of Hostilities	164
I. Introduction	164
II. The Legality of Means and Methods of Cyber Warfare	168
III. The Law of Targeting	176
IV. Cyber Operations Short of 'Attack'	239
V. Cyber Operations as Remedies Against Violations of the Law of Armed Conflict	242
VI. Conclusions	245

5. Cyber Operations and the Law of Neutrality	246
I. Introduction	246
II. When Does the Law of Neutrality Apply?	248
III. The Law of Neutrality and its Consequences on the Conduct of Cyber Operations	253
IV. Non-Belligerency	267
V. The Law of Neutrality and the UN Charter	269
VI. Remedies Against the Violations of the Law of Neutrality	272
VII. Conclusions	277
General Conclusions	280
<i>Select Bibliography</i>	289
<i>Index</i>	301

Biblioteka Główna
Akademii Obrony Narodowej

21314/III



03-021314-000-0

Czyt.
004, 056

'Land, sea, and air are no more the only domains where hostilities can be conducted. Cyberspace has now become the fourth dimension. Marco Roscini's *Cyber Operations and the Use of Force in International Law* is a challenging subject. Taking into account recent state practice, traditional customary and treaty law to construe rules applicable to cyber operations.

He examines all the main chapters of the law of armed conflict: *jus ad bellum* and the law of neutrality. A sound knowledge of the law of armed conflict enables the author to formulate a complete set of rules for cyber operations in a realistic mode. Dr Roscini's book is to be recommended to the attention of legal advisors and to all concerned with planning defence operations.

Natalino Ronzitti, Professor Emeritus of International Law, LUISS University, Rome

'The present volume by Dr Marco Roscini is a systematic, up-to-date and well-informed analysis of the legal discourse that has taken place thus far. The author identifies the issues that have given rise to much discussion, marshals the evidence and provides a clear picture of where cyber operations stand in the overall scheme of the international law of armed conflict. This gives him an opportunity to delve into many controversial aspects of that law, irrespective of their kinetic/cyber application... The book surely sets the stage for the future encounter between law and reality.'

Yoram Dinstein, Professor Emeritus of International Law, Tel Aviv University, from the Foreword

'The increasing amount of cyber attacks and cyber exploitation operations by states and non-state actors calls for a comprehensive review of the current legal framework and its loopholes. Marco Roscini's admirable study of pertinent rules of international law, whether based on treaty or custom, underlines the applicability of existing law to new technological developments. His convincing examination of relevant rules of the *jus ad bellum*, the *jus in bello* and the law of neutrality will facilitate implementation of the law in a particularly complex environment and may also help to inform peacetime cooperation on cyber security for which sustainable efforts and effective new regulation are urgently required.'

Dieter Fleck, Former Director, International Agreements and Policy, German Ministry of Defence

Jacket image: © Fuse / Gettyimages.com

OXFORD
UNIVERSITY PRESS

www.oup.com

ISBN 978-0-19-965501-4



9 780199 655014