OXFORD

CYBERWAR

Law and Ethics for Virtual Conflicts

EDITED BY
Jens David Ohlin, Kevin Govern, and Claire Finkelstein

CYBERWAR

Law and Ethics for Virtual Conflicts

Cyberwar

Law and Ethics for Virtual Conflicts

Edited by
JENS DAVID OHLIN
KEVIN GOVERN
CLAIRE FINKELSTEIN

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

First Edition published in 2015

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 Cataloging in Publication Data
Data available

ISBN 978–0–19–871750–8

Foreword

In 2013, the Group of Governmental Experts (GGE), a collection of cyber experts from fifteen states, concluded that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [information and communications technology] environment."[1] Although drawing world-wide attention, the statement hardly represented a jurisprudential epiphany. Earlier the same year, the International Group of Experts (IGE) that produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare* agreed unanimously "both the *jus ad bellum* and the *jus in bello* apply to cyber operations."[2] Indeed, it is unfortunate that the GGE failed to explicitly pronounce on the applicability of the jus in bello (international humanitarian law (IHL)) to cyber operations occurring during an armed conflict.

Claims that cyberspace is a new domain to which international law is inapplicable (or inapplicable in part) persist but are steadily diminishing. The logic underlying the premise of international law's applicability to cyberspace is simply too compelling for such assertions to gain meaningful traction. For instance, in its *Nuclear Weapons Advisory Opinion*, the International Court of Justice confirmed that the UN Charter's Article 2(4) prohibition on the use of force and Article 51 acknowledgment of the "inherent" right of self-defense apply "regardless of the weapon used."[3] Today experts in the field universally accept this pronouncement as accurate. It is, therefore, difficult to sustain an argument that cyberweapons do not fall within its ambit. This is so despite occasional arguments that cyber operations do not involve the use of weapons. Such arguments, which tend to be advanced by those with little expertise in the jus ad bellum, were rejected by both the GGE and IGE.

Similarly, it is spurious to assert that IHL does not govern cyber operations during an armed conflict. Consider Article 36 of the 1977 Additional Protocol to the 1949 Geneva Conventions: "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."[4] This provision generally reflects customary law, and thus binds

[1] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para 19, UN Doc A/68/98, June 24, 2013, at <http://undocs.org/A/68/98>. The experts came from Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

[2] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013) 5.

[3] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226, para 39 (July 8).

[4] Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, art 36, June 8, 1977, 1125 UNTS 3.

all states irrespective of party status.[5] Since cyber operations involve "new weapon[s], means or method[s] of warfare," they, therefore, require review for compliance with the extant IHL. The Article unambiguously demonstrates that IHL was intended to continue to apply as the nature and instruments of warfare evolved. This is the position that has been taken by the International Committee of the Red Cross;[6] it is one that is, quite frankly, indisputable.

Although less studied, the applicability of international law to "below the threshold" cyber operations, that is, those that neither constitute a "use of force" nor an "armed conflict," would likewise appear certain. For instance, although it may sometimes be difficult to attribute cyber operations to a particular state, non-state actor, or individual as a matter of *fact*, there is no reason to exclude application of the *law* of state responsibility's attribution principles to them.[7] Similarly, on what basis would cyber operations conducted from land, sea, air, and space escape the reach, for instance, of the law of sovereignty, the law of the sea, air law, or space law? On the contrary—the risks associated with cyber operations to states, economies, societal functions, and individuals, make the argument for application of existing law especially compelling. As examples, the principle of due diligence can act to impede malicious cyber operations mounted from other states' territories by third parties,[8] while the plea of necessity affords a meaningful basis for responding to cyber operations against critical infrastructure in situations where even the originator of the cyber operation cannot be determined.[9]

Acknowledging that international law is applicable to cyber operations is only, however, the initial step in the process of articulating and implementing the normative architecture. Two more are necessary.

First, it is obviously essential to identify *how* that law applies. For instance, while it is clear that pursuant to the UN Charter and customary law, cyber uses of force are prohibited and forceful responses are only available once a cyber operation rises to the level of an armed attack, it remains unclear when a cyber operation qualifies as either a use of force or armed attack if it causes no physical damage or injury. The most oft-cited case is a massive cyber operation directed against a state economic infrastructure. Would the operation be unlawful as a prohibited use of force and would it qualify as an armed attack that allowed the target state to respond with its own forceful kinetic or cyber operations? Opinions vary.[10] Similarly, although the due diligence principle requires all states to take feasible measures to stop ongoing malicious cyber operations emanating from their territory that harm other states, what obligations does

[5] Tallinn Manual, Rule 48 and accompanying commentary. Although some states do not acknowledge the customary nature of the norm vis-à-vis methods of warfare, this minor deviation from the text of Article 36 has little bearing on the general applicability of IHL to cyber operations.

[6] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 31st International Conference of the Red Cross and Red Crescent, November 28–December 1, 2011, Doc 31IC/11/5.1.2, 36–7.

[7] UN International Law Commission, Report of the International Law Commission, Draft Articles of State Responsibility, Articles 4–11, U.N. GAOR, 53rd Session, Supp. No 10, U.N. Doc. A/56/10 (2001).

[8] Tallinn Manual, Rules 6–8 and accompanying commentary.

[9] Draft Articles of State Responsibility, Article 25.

[10] See discussion in commentary accompanying *Tallinn Manual* Rules 11 and 13.

that principle impose on a transit state in light of the difficulty of identifying malicious packets of data transiting their cyber infrastructure and the fact that a blocked transmission will often simply traverse a different route to the intended target?[11] And in the field of IHL, it is clear that attacks, including cyber attacks, against civilians and civilian infrastructure, are prohibited.[12] But when does a cyber operation qualify as an "attack" in the meaning of Article 49 of Additional Protocol I such that it is unlawful? Must it cause physical damage or injury? Or does interference with functionality qualify as damage? If so, what degree of interference?[13]

Second, the exercise of applying international law in the cyber context will reveal lacunae in the law that may need to be addressed directly through treaty action or that will inevitably become the subject of state practice that will in turn contribute to the crystallization of either responsive interpretations of existing law or new customary norms. To illustrate, IHL protects civilian objects against direct attack. The majority of the IGE concluded that data did not constitute a civilian object since they were intangible.[14] While this conclusion may be sound as a matter of legal interpretation, the consequences of the interpretation were seen as problematic even by some of the experts who took the position. Some data are plainly of great significance both to the orderly functioning of societies during an armed conflict and the general well-being of individuals. It would accordingly appear likely that over time a broader interpretation of the notion of objects in IHL will, and should, gain traction. The process of identifying such lacunae is essential if law is to adapt itself to the new realities of cyberspace.

Moreover, legal norms are but one facet of the normative universe. They merely articulate the outer limits of permissible cyber operations. Once these boundaries are defined, policy-makers craft ethical, political, and operational norms that further refine the permissible scope of cyber activities. The norms will find expression in domestic law or policy. They may also evolve into regional or global prescriptive norms. Thus, the work in these fields is no less important than that which is ongoing in the legal field. On the contrary, ethical, political, and operational norms may prove to have greater influence on restricting the conduct of cyber operations since legal norms sometimes allow states and other actors in cyberspace great leeway.

Unfortunately, non-legal cyber norms are too often conflated with legal ones. For example, ethicists speaking at the last two global CyCon conferences convened by the NATO Cooperative Cyber Defence Centre of Excellence, a leader in the field of cyber law and policy, repeatedly proffered ethical standards as binding international law. In doing so, they badly mangled the law. As the normative tapestry of cyber operations develops, it is essential that the various bodies of normative strictures be defined with precision. The process begins with international law boundaries for cyber operations and then those boundaries contract based on other concerns.

Cyberwar: Law and Ethics for Virtual Conflict measurably contributes to the process. It contains highly sophisticated legal analyses that not only apply extant international

[11] *Tallinn Manual* Rule 8 and accompanying commentary.
[12] Additional Protocol I, Article 52(1); *Tallinn Manual*, Rule 37.
[13] See discussion in commentary accompanying *Tallinn Manual*, Rule 30.
[14] *Tallinn Manual*, 127.

law in such areas as cyber deception and criminal law, but also tease loose such interpretive dilemmas as the classification of cyber armed conflict, the meaning of the term "attack," and the application of legal causality principles to cyber operations. The book also focuses on cyber activities that do not lend themselves well to the simple application by analogy of legal principles and rules developed in the non-cyber context. These topics include how the law responds to cyber operations mounted by individuals or non-state groups, including cyber terrorists, and whether traditional understandings of borders in international law are suited to application in cyberspace.

Recognizing that normative constraints are not exclusively juridical in nature, the book also explores the nature of cyberwar and its unique ethical status. Additionally, it usefully places cyber activities into a technical context, for norms, whether legal or not, must take cognizance of the distinctive technical environment to which they have to respond.

In this book, Jens Ohlin, Kevin Govern, and Claire Finkelstein have gatherd a distinguished and diverse group of contributors. They include accomplished scholars from different disciplines, as well as experienced practitioners. All have offered an especially perceptive perspective on their respective topics. Together their contributions take the discourse, which is too often counter-normative and usually stovepiped, to a new level. I congratulate the distinguished editors and contributors on their role in producing this fascinating and useful work.

Michael N Schmitt
Director, Stockton Center, United States Naval War College
Chair of International Law, Exeter University
Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence

Table of Contents

PART IV: RESPONSIBILITY AND ATTRIBUTION IN CYBER ATTACKS

Cyber warfare is fast becom
nations face. Cyberattacks
in a single act, making the
law of armed conflict applie
national security, supplying
traditional military conflict. Under what conditions does a cyberattack amount to an act of war? What is a proportional response to a cyberattack? Is it permissible to pre-empt a cyberattack with the use of kinetic force? If so, when would the use of pre-emptive force violate third party sovereignty?

This collection of essays, written by a group of interdisciplinary scholars and practitioners, addresses the ethical and legal issues that surround cyber warfare. It considers whether the Laws of Armed Conflict apply to cyberspace, as well as the ethical position of cyber warfare against the background of generally recognized moral traditions in armed conflict.

Cyberwar is essential reading for anyone interested in the impact of cyber warfare on international law and the laws of war.

Jens David Ohlin is Professor of Law at Cornell Law School.

Kevin Govern is Associate Professor of Law at Ave Maria School of Law.

Claire Finkelstein is the Algernon Biddle Professor of Law, and Professor of Philosophy, at the University of Pennsylvania.

ISBN 978-0-19-871750-8

OXFORD
UNIVERSITY PRESS

www.oup.com