Book Review

Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), ***Cyber War: Law and Ethics for Virtual Conflicts*** (Oxford University Press, 2015) 320 pp. $185 (Hardback) ISBN 9780198717492

This is a great book. It is not so common to come across a coherent collection that offers such useful insight and understanding for scholars and students alike, let alone on a topic that is only beginning to take shape. This volume does just that. The editors have brought together leading experts (along with the emerging scholar Nicolò Bussolati whose contribution is worthy of note), to explore the applicability of our international law and norms in the expanding shared environment of cyberspace — specifically, those rules relating to the escalation of conflict. This reviewer picked up the book in the hopes of finding some basic points of entry for students, and has been delighted to find a whole host of chapters that are not only individually valuable, but work well together to provide a lucid view on a complex subject.

The book is launched with a foreword by the director of the Tallinn Manual on the International Law Applicable to Cyber Warfare, Michael Schmitt. As this 2013 document represents the work of a distinguished International Group of Experts invited to produce a non-binding assessment of the application of existing law to cyber warfare, this is indeed a valuable starting point. In addition, two of the chapters have been authored by experts directly involved in this drafting project and the other contributions elucidate what is to be found in the manual while further exploring more specialized terrain. In other words, this book can be said to build upon, and move beyond, the Tallinn Manual.

As a way of illuminating the substantive value of this overall book in a short review, I will focus on one brilliant chapter found at the centre of this work. In Chapter 7, Duncan B. Hollis provides a keen and edifying analysis of the conceptual stumbling blocks for regulating the space of cyber. Whether they are territorial, legal or normative, this nebulous ether defies our current understandings of their customary boundaries. As a result, the attempt to construct governance for cyberspace, or even applicable norms, using any of our existing appreciations of boundary lines inevitably raises fundamental and unresolved theoretical questions about what cyberspace 'is'. To demonstrate this elementary difficulty for mapping viable solutions, Hollis presents the two predominant legal methods of *tailor-made law* and *law-by-analogy* to ultimately show the shortcomings of each.

In a veritable effort to tackle this conceptual problem, Hollis provides a thought-provoking alternative proposal for initiating a transfer of our shared principles of humanity and military necessity — the essence of international humanitarian law — into cyberspace. He calls it the 'Duty to Hack', which would require that 'states use cyber operations in their military operations when they are the least harmful means available for achieving military objectives'.[1] At first blush, the idea might strike humanitarian law scholars as an odd requisite, but Hollis' unconventional bottom-up approach certainly merits a careful reading.

While this chapter does contain a few repetitions that could stand to be polished away, and not everyone will subscribe to the proposition, it represents the reflective work that can be found throughout the book. The first section properly begins with debating chapters on whether 'war' — and all of its accompanying laws and norms — should be applied to cyberspace at all. It also includes a fascinating discussion on whether an increased deployment of cyber-weapons should force the laws of war to develop a more nuanced and sophisticated account of causation (now largely absent). The second section then looks into the failings of a specialized 'enemy criminal law' for those who have no loyalty to the society or its rules, the consequences of belligerent political rhetoric

[1] D.B. Hollis, 'Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?' in J.D. Ohlin, K. Govern and C. Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, 2015) 129, at 156.

and media coverage for the application of law, and an astute presentation of the intersection of non-state actors operating in a transnational environment. Next, beyond the contribution described above, the third section surveys the use of espionage for the task of gathering internet-based information in national security operations and the legality of using cyber deception to distort and disrupt manoeuvers of the enemy. Finally, the book closes with valuable investigations of applicable evidentiary issues to consider in a virtual context through current international jurisprudence, and the principle of non-intervention as low-intensity interference into internal affairs becomes markedly less difficult when logistical and cost impediments are significantly diminished in the world of cyber.

Though there are one or two chapters here that might slow or disrupt a reader's journey through this volume from start to finish, most will not be so linear in their movement through the volume, and some might even come looking for those points of enquiry specifically. In addition, there are some further subjects that could have been interesting to treat here — for example, a chapter on the work of the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (admittedly the fourth group report was only released after this publication), an exploration of the precise distinction between offensive and defensive operations, or perhaps a chapter on what multi-state cooperation for mass collection of personal data from cyberspace might mean to the boundaries of nationality and enmity. But, of course, no work of this kind can be fully comprehensive. Consequently, on the whole this book is indeed an excellent starting place for those interested in delving into the law and ethics for virtual conflicts.

Steven J. Barela
LLM, PhD Assistant Professor Global Studies Institute/ Faculty of Law University of Geneva
Steven.Barela@unige.ch
www.LegitimacyasaTarget.com
doi:10.1093/jicj/mqw003