

**WestminsterResearch**

<http://www.westminster.ac.uk/westminsterresearch>

**Book Review: Cyber Espionage and International Law (2018) by  
Russell Buchan  
Longobardo, M.**

This book review has been accepted for publication and will appear in a revised form, subsequent to peer review and/or editorial input by Cambridge University Press in the Israel Law Review. This version is free to view and download for private research and study only. Not for re-distribution, re-sale or use in derivative works.

© Cambridge University Press, 2020

The final definitive version in the online edition of the book review at Cambridge Journals Online is available at:

<https://doi.org/10.1017/S0021223720000011>

The WestminsterResearch online digital archive at the University of Westminster aims to make the research output of the University available to a wider audience. Copyright and Moral Rights remain with the authors and/or copyright owners.

*Cyber Espionage and International Law* by Russell Buchan [Hart, 2018,  
ISBN: 9781782257363, 248pp, £75, h/bk]

*Cyber Espionage and International Law* by Russell Buchan is a clever and well-argued book that tackles a dramatically important issue of current international affairs: the international legal regulation of cyber espionage. Clearly, the very issue is topical in its own right because of the current massive use of cyber means to collect and store reserved data, which is becoming commonplace thanks to the increased availability of the relevant sophisticated technology. So far, no significant monograph has been published on this topic, although the author of the book under review<sup>1</sup> and other scholars have offered some shorter reflections.<sup>2</sup> The book offers an engaging overview of the international legal framework applicable to espionage *tout court*, beside the specific realm of cyber espionage, which will last irrespective of the future evolution of espionage and of scholarship on this subject matter.

The analysis is divided into an introduction and eight chapters. The introduction puts forth the scope of the book and its main argument, according to which although international law does not prohibit political and economic cyber espionage, it significantly constrains the way in which cyber espionage may be lawfully conducted. The author argues that the traditional view on the neutrality of international law towards

---

<sup>1</sup> Russell Buchan, 'Cyber Espionage and International Law' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015) 168.

<sup>2</sup> See, eg, Ashley Deeks, 'An International Legal Framework for Surveillance' (2015) 55 *Virginia Journal of International Law* 291; Asaf Lubin, "'We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance' (2018) 18 *Chicago Journal of International Law* 502.

cyber espionage<sup>3</sup> is an illusion since cyber espionage is a state activity that must comply with a variety of customary and treaty international rules (pp 4-8). Accordingly, the author's argument implies a rejection of the opinion that states have a right to spy under international law.<sup>4</sup>

The author's argument is demonstrated over the eight thematic chapters, which explore the definition of cyber espionage (Chapter 1), the role of cyber espionage as a threat for international peace and security (Chapter 2), and the legality of cyber espionage in relation of some international law rules and regimes. In particular, Chapter 3 addresses the relevance of the rules on territorial sovereignty, non-intervention, and non-use of force, Chapter 4 focuses on diplomatic and consular law, Chapter 5 explores international human rights law (with a specific focus on the extraterritorial application of human rights instruments and the right to privacy), and Chapter 6 engages with World Trade Organization rules. The book closes with two chapters on the existence of rules allowing states to conduct cyber espionage notwithstanding the legal constraints addressed in the previous chapters, both as customary exceptions (Chapter 7) and defences based on self-defence and necessity (Chapter 8). A general Conclusion summarises the main results achieved through the book.

Since it is unfeasible to address here all the arguments presented by Buchan's book, this review will focus only on the points that have most caught my attention. The first notation is on methodology. Buchan addresses the fact that cyber espionage may violate some customary and treaty international rules through a persuasive deductive reasoning:

---

<sup>3</sup> The view is grounded in the idea the peacetime espionage is not directly regulated by international law. See, eg, Roger D Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 *Air Force Law Review* 217, at 223; Geoffrey B Demarest, 'Espionage in International Law' (1996) 24 *Denver Journal of International Law and Policy* 321.

<sup>4</sup> See Asaf Lubin, 'Espionage as a Sovereign Right under International Law and Its Limits' (2016) 24(3) *ILSA Quarterly* 22.

the author first analyses a specific legal framework and the competing views of other scholars, then suggests his interpretation and finds in state practice and judicial decisions confirmation of his conclusions (eg at pp 51-55, 56-59, and 99-101, just to mention few examples). This method rests on the author's impressive knowledge of a variety of international law issues so that, at the end of the book, the reader has the satisfying feeling of having read an excellent work on general international law occasioned by a discussion on cyber espionage, rather than a monograph on a specific and narrow topic. This is a very positive feature, especially if compared to the ongoing trend of high specialisation in the study of just one specific area of international law.

Moreover, the author deserves praise for his courage to challenge the mainstream view according to which cyber espionage does not constitute in itself a violation of territorial sovereignty. Contrary to the finding of the Tallinn Manual,<sup>5</sup> Buchan argues that cyber espionage violates territorial sovereignty even in the absence of any 'real-world physical damage' or 'destructive effects in cyberspace' (p 53). Compellingly, the author argues that the exercise of territorial sovereignty over cyber infrastructures should be assessed in the same way as the exercise of territorial sovereignty over physical territory, which is violated every time there is an intrusion with the aim of undertaking espionage activities (p 54). In this regard, the book offers an alternative view that must be kept at the centre of the legal debate along with the contrary views suggested by other scholarly works.

The familiarity of the author with broader issues of international law, and his capacity to apply them to the context of cyber espionage, is demonstrated also by his analysis of alleged customary exceptions allowing states to conduct cyber espionage. The author shows that covert actions cannot be taken into account in the assessment of the state

---

<sup>5</sup> Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) at 20-21.

practice that is relevant for the emergence of customary international law (p 154), demonstrating that the existence of such exceptions is not supported by a sufficiently uniform state practice (pp 155-159) and *opinio juris* (pp 160-163). This conclusion is in line with past scholarship<sup>6</sup> and the assumption that international customary rules cannot be altered by violations of international law.<sup>7</sup>

All in all, the book under review is an excellent monograph, which addresses a very topical issue through the lens of a variety of international law rules. The conclusions of the author are always reached after a careful examination of international scholarship and take into account a wealth of domestic and international decisions, as well as episodes of state practice. As mentioned, the book does not hesitate to engage with the mainstream views, discussing them and offering original solutions that will be relevant to future studies of cyber espionage under international law. The book is written in such a frank and honest style that the author does not hesitate to acknowledge that his view on the relationship between cyber espionage and the principle of non-intervention has evolved (p 65, note 81, referring to a previous chapter written by the author).

This very well-argued book presents only very marginal shortcomings related to the fact that the reader, at times, may have the impression that there is something missing. For instance, as a matter of content, it would have been interesting to read the author's opinion on cyber espionage in times of armed conflict (outside the scope of the book, see p 26), especially because Buchan is a proficient international humanitarian lawyer in his own right.<sup>8</sup> Indeed, the regulation of espionage in armed conflict is different from that

---

<sup>6</sup> See eg Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs' in Roland Stanger (ed), *Essays on Espionage and International Law* (Ohio State University Press 1962) 3, at 17.

<sup>7</sup> *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA)*, Judgment, 27 June 1986, ICJ Reports (1986) 14, at para 186.

<sup>8</sup> See, eg, his works on 'International Community and the Occupation of Iraq' (2007) 12 *Journal of Conflict & Security Law* 37; 'The International Law of Naval Blockade and Israel's Interception of the *Mavi*

conducted in peacetime: international humanitarian law allows intelligence collection<sup>9</sup> but punishes the spy caught in the enemy territory with the denial of the prisoner of war status.<sup>10</sup> It would have been interesting to read Buchan's view on the application of these rules to cyber espionage, where the operator is usually located far from the theatre of the conflict.<sup>11</sup>

Moreover, the analysis of international human rights law instruments is limited to the International Covenant on Civil and Political Rights and the European Convention on Human Rights (pp 97-105). The book could have benefitted from an engagement with the protection to right to privacy provided by the Inter-American system, especially in light of the very progressive stance adopted by the Inter-American Commission on Human Rights and the Inter-American Court of Human Rights.

Finally, the bibliography cites only one piece of scholarship that is not written in English,<sup>12</sup> in line with the mainstream, and nonetheless regrettable, trend to ignore largely works written in other languages. Works on espionage that Buchan could have taken into account in his analysis of cyber espionage have been written in French and German.<sup>13</sup>

---

*Marmara*' (2011) 58 *Netherlands International Law Review* 209; 'The Rule of Surrender in International Humanitarian Law' (2018) 51 *Israel Law Review* 3.

<sup>9</sup> See Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No IV Respecting the Laws and Customs of War on Land, 18 October 1907, 36 Stat 2227, Art 24 (hereinafter: HR).

<sup>10</sup> See, eg, Art 31 of the HR.

<sup>11</sup> For some remarks on this, see Marco Longobardo, '(New) Cyber Exploitation and (Old) International Humanitarian Law' (2017) 77 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 809.

<sup>12</sup> Iñaki Navarrete, 'L'espionnage en temps de paix en droit international public' (2016) 63 *Canadian Yearbook of International Law* 1. The book by François Gény, *Méthode d'interprétation et sources en droit privé positif: essai critique* (Libr Marescq Ainé 1899) is referred to only as quoted by Antony D'Amato, *The Concept of Custom in International Law* (Cornell University Press 1971) 49.

<sup>13</sup> See eg Fabien Lafouasse, 'L'espionnage en droit international' (2001) 47 *Annuaire Français de Droit International* 63; Helmut Philipp Aust, 'Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht' (2014) 52 *Archiv des Völkerrechts* 375.

Notwithstanding these remarks, it is irrefutable that Russel Buchan's *Cyber Espionage and International Law* is one of the most important and complete works on cyber espionage in international scholarship, and it will be studied and analysed for many years in the future to understand the complex relationship between cyber espionage and a number of international law rules. The book's compelling arguments, its fresh and frank style, and its sound knowledge of international law rules make this monograph a fascinating and pleasant reading.

Dr Marco Longobardo  
Lecturer in International Law  
University of Westminster  
m.longobardo1@westminster.ac.uk