Leiden Journal of International Law (2019), **32**, pp. 883–885
doi:10.1017/S0922156519000359

BOOK REVIEW

Russell Buchan, *Cyber Espionage and International Law*, Hart Publishing, 2018, 248pp, ISBN 9781782257363, £75.60
doi:10.1017/S0922156519000359

There are certain matters that international lawyers do not like discussing in polite company. Close to the top of any list is likely to be peacetime espionage. Whether one views it as falling within the mystical 'grey zone' of state activities un- (or under-)regulated by international law, an example of the now popular trope of 'illegal but legitimate', an instance of the reserved domain, or falling back on the positivist nostalgia of *The Lotus* presumption, peacetime espionage is not well understood in mainstream international law. And, to a large extent, you often get a sense most international lawyers are content to leave it that way.

On the other hand, espionage is often a matter of great importance to scholars of certain schools of international relations and realist international lawyers. In contrast to the timidity of approach of some, they see espionage as a fundamental feature of national security, that often – though not invariably – should be treated as a legitimate *and* legal state function. State practice, on the other hand, is more equivocal than theory, and the practice that does exist (and is publically recorded) seems to slide towards illegality, though most discourses would focus on violations of domestic law than international law *per se*.

It is within this general context that Russell Buchan in this new monograph, *Cyber Espionage and International Law*, an ambitious and original work, seeks to place these general questions within the more specific phenomenon of cyberspace. Buchan defines cyber espionage as 'the non-consensual use of cyber operations to penetrate computer networks and systems with the objective of copying confidential data that is under the control of another actor'.[1] Such a definition is unlikely to withstand significant scrutiny from experts in the technological field, and it raises several normative questions – some of which are identified below. But, as a means of demarcating the scope of his study, and providing necessary precision within the study of an invariably secretive practice in a forever changing world, it has much to commend it. Indeed, Buchan has recognized, be it implicitly, that, for a study on cyber espionage to be useful to international lawyers it must not fall within the trap of technical-ese, where the jargon of the specific excludes the generalist from engaging in the debate.

The central thesis of the book is one of simplicity; simplicity not used here in a pejorative sense but one that is essential to public international law. Namely, that matters such as espionage and cyberspace – in this monograph brought together – despite their innate political, technological, and security implications are capable of robust, simple analysis. In other words, that it is possible to identify the legal framework in which such matters exist; that complexity does not *per se* obfuscate against normative precision. Buchan argues that indeed peacetime espionage – through the

[1] R. Buchan, *Cyber Espionage and International Law* (2018), at 27.

underlying acts that constitute it – is a matter regulated by international law, and that notwithstanding the absence of a universal regime against such espionage, general rules and principles do exist which provide the legal context in which states operate. And – importantly – such rules and principles transcend the media in which such espionage occurs, thus, by merely making it more technical to understand, do not in any way transform the illegality or otherwise of such activity. This is a simple proposition in one sense; but as I said simplicity in an almost Kelsenian manner, rather than based on the naivety of a generalist.

In fact, one of the biggest strengths of Buchan's study is his systematic attempt to interrogate cyber espionage against traditional, and doctrinal, norms of international law. Though there are important chapters on cyber espionage and diplomatic and consular law, international economic law, and human rights *inter alia*, it is his attempt to examine cyber espionage against the rules of territorial sovereignty and non-intervention that gives this book its strongest appeal. Buchan takes standard customary norms and seeks to apply them in a wholly modern context. More significantly, as he is not fixated on Articles 39 and 51 of the UN Charter on peace and security, he is able to (almost entirely) escape the rather tired debate of use of force and self-defence, though he does include sufficient examination of these matters not to be accused of ignoring them.

But the book's biggest strength, perhaps, is also its most challenging weakness. Buchan is very careful in how he demarcates his study. He makes a number of methodological and doctrinal choices that invariably allow him to expertly grasp this most challenging of topics. However, the choice itself leaves questions unanswered. For instance, he excludes cyber espionage in times of war and thus, *a priori*, ignores the application of international humanitarian law. As the law of peace and the law of wars remain distinct, this is a rational choice. By focusing on espionage as he defines it, and which mirrors its counterpart in international humanitarian law: 'gathering or attempting to gather information in territory controlled by an adverse party through an act undertaken on false pretences or deliberately in a clandestine manner',[2] he can navigate a complex field.

Nevertheless, by defining cyber espionage in this way it also prevents a wider, perhaps more contemporary, discussion. I am not talking here about cyber-attacks, or more aggressive cyber hacking, both of which Buchan briefly mentions (to exclude from his study),[3] and both of which, certainly the former, enters what involves an important – but personally I think a rather sterile and self-referential – debate on armed attack and (pre-emptive) self-defence. Rather, I am reflecting on the coercive element of cyber espionage, as principally illustrated by alleged Russian actions against several western states, namely the use of the medium of the internet, *inter alia*, to influence other states' internal (and democratic) processes, as well as public opinion and perhaps national security more generally. Buchan mentions such coercive cyber activity but feels it falls outwith the scope of his study. It certainly falls outside his definition of cyber espionage. To make the manuscript manageable this both seems entirely reasonable and on the whole justifiable. However, it does have certain important normative consequences. First, Buchan views cyber espionage (as he defines it[4]) as violating the rule of territorial sovereignty, but not non-intervention.[5] His analysis is important, and challenging, for he questions other key writers who view cyber space as external to (or at best tangential to) the territorial sphere. Buchan refuses to accept such an argument; the general principle is universal enough to cope with modern phenomena.

However, as regards the rule against non-intervention, he finds coercion as a key element of that rule (as set out in *Nicaragua*);[6] and the mere copying of data is not coercive in that sense. What, of course, is done with that data is an altogether different matter, but the espionage itself is

[2]ICRC Customary Rule 107.

[3]Buchan, *supra* note 1, at 2, 18.

[4]Ibid., at 27.

[5]Ibid., at 69.

[6]*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment of 27 June 1986, [1986] ICJ Rep. 14, para. 205.

https://doi.org/10.1017/S0922156519000359 Published online by Cambridge University Press

non-coercive. Likely to be very true. But if one considers the present debates around recent state practice including alleged interference in the 2016 US presidential election, whether cyber 'espionage' can be so narrowly demarcated is surely arguable? Coercion would seem to be very much an element in such matters, and therefore non-intervention consequently equally engaged. Perhaps such activity is not espionage *stricto sensu*, but then where does it fall? Just as Buchan is right to challenge those realists who would discount the illegality of (cyber-)espionage, recourse to formalism to exclude other tributaries in a normative stream is methodologically tidy but somewhat artificial in the real world. As the International Court noted in *Nicaragua*, 'Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones'.[7] Buchan would, as this book shows, be the first to apply traditional rules and principles to the modern context.

There is much of interest and a wealth of material here. As I mentioned above, Buchan devotes separate chapters to the human rights implications of cyber espionage, the international economic angle, and diplomatic consequences thereof. He also tackles the argument that even if there are primary rules of international law which would seem to prohibit (cyber-)espionage, there is either a customary rule exception to it, or the defence of necessity excludes it. In both cases, his argument is squarely based in mainstream international law argument to discount such propositions. In the first, on the generally accepted principles of customary international law (including for a rule (or exception) to exist it must be publically made, and not be done in secret) and for states to accept or acquiesce in such practice, thus requiring the necessary *opinio juris*; and in the second, on the ILC exacting requirements for necessity, as endorsed by the International Court.[8] The chapter on a customary international law exception is particularly strong in revealing how Buchan's work is distinctive from much of the literature in the field. That in itself is very telling as to how far international law has been too submissive on this topic for too long.

On all these, and other matters, such as extraterritoriality and the right to privacy, Buchan places cyber-operations within the context of general international law. That is not to say he cannot see a place for *lex specialis* – a legal regime placing cyber espionage within a clearer legal framework – but he does so as *desideratum*, and not in despondency as to what general international law already provides. Cyber-espionage as a topic, however much avoided in polite company in the past, now more than ever needs to be subject to proper analytical discourse. This book provides a significant and rigorous contribution to that intellectual debate.

*Duncan French**

[7]Ibid.

[8]*Gabčíkovo-Nagymaros Project (Hungary/Slovakia)*, Judgment of 25 September 1997, [1997] ICJ Rep. 7, para. 51; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, [2004] ICJ Rep. 136, para. 140.

*Professor, College of Social Science, University of Lincoln, LN6 7TS UK, +44 1522 835567 [dfrench@lincoln.ac.uk].

https://doi.org/10.1017/S0922156519000359 Published online by Cambridge University Press