Russell Buchan, ***Cyber Espionage and International Law***. Hard Publishing, 2019, 195 pp., ISBN 9781782257349.

Peacetime espionage as a method for states' gathering military, political, commercial or other secret information by means of spies, secret agents, or monitoring devices has a long and well documented history. It has and continues to be an indispensable part of the activities that most governments undertake, but characteristically it is shrouded in secrecy and usually denied. The international law's stance regarding peacetime espionage has traditionally been and remains rather ambivalent. Some commentators argue that it exists in the twilight of international law, whilst others contend that the rules of *lex lata* have little role to play as they neither prohibit nor allow states to engage in this method of gathering information. Nevertheless, to assert that international law does not apply to these activities would be misguided, as there is a substantial body of existing rules, which indirectly regulate espionage, such as the principles of territorial sovereignty, non-intervention and the law on diplomatic relations, to name but a few.

The dawn of the internet and the prolific use of cyberspace by states, corporations, terrorists, criminals and individuals alike added not only an additional and much utilised avenue through which states can nowadays conduct their espionage activities, but also an auxiliary layer of uncertainty regarding both the applicability and the utility of international law in the context of state cyber espionage. This complexity and therefore the challenges that such intelligence gathering poses to international law is the subject matter of the inquiry by Dr Russell Buchan in this book titled, *Cyber Espionage and International Law.* The monograph's contention that cyber espionage does not exist in an international legal vacuum serves as the basic premise to a comprehensive and well-argued overview of the applicable law, namely the rules of territorial sovereignty and non-intervention, diplomatic and consular law, international human rights law and the rules of the World Trade Organization (WTO). In addition, consideration has been given to whether cyber espionage could be said to be lawful on the basis of customary international law, in other words if this form of spying could be considered as an exception to international law rules that prohibit it. Furthermore, the monograph grapples with the issue as to whether the doctrines of self-defence and necessity could justify deploying such methods of intelligence collection from afar. Having defined cyber espionage as 'non-consensual copying of confidential information that is resident in or transiting through cyberspace' the book clearly articulates its main objective, namely 'to identify the international rules applicable to cyber espionage and to assess the extent to which they prohibit or constrain this activity' (p 13). That this goal has been achieved is abundantly clear.

To begin with, the monograph makes an explicit distinction between political and economic cyber espionage and effectively interweaves these two strands of state activity by applying pertinent rules of international law to each of these methods of intelligence collection, thus presenting a comprehensive and well-constructed taxonomy of norms applicable in each context. To that end, having posited cyber espionage within the broader lexicon of international relations theories, the book in chapter 2 postulates that political espionage threatens the maintenance of international peace and security because not only

does it violate the principles of sovereign equality of states and human dignity, but also undermines trust and confidence among the international community of states 'thereby preventing them from effectively addressing the threats and dangers that proliferate within international society' (p. 46). A similarly uncompromising stance is taken with respect to economic cyber espionage, which poses the same danger, as according to the author 'stealing a company's trade secretes compromises its financial success [which] has a negative knock-on effect upon the economic wellbeing of the host state' (p. 45). This argument is justified on the basis that 'the maintenance of a state's economic security and the preservation of peace and security' are inextricably linked and therefore for the latter to be achieved 'it is essential that international law clearly prohibits […] cyber-enabled economic espionage' (p. 46). Having justifiably called on the international community to 'implement international legal rules that expressly and unequivocally prohibit political and economic cyber espionage' (p. 46) the monograph proceeds to examine the status of these activities under international law. The author in a detailed and systematic manner first considers the application of the rules of territorial sovereignty, the principle of non-intervention and the prohibition on the use of force (chapter 3), along with the corollary right to self-defence and necessity vis-à-vis acts of cyber espionage (chapter 8). The findings, informed and supported by the frequent reference to the jurisprudence of *inter alia*, the International Court of Justice (ICJ), the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Tallinn Manual 2.0*) and prominent academic opinion are unequivocal. Acts of political and economic cyber espionage that 'penetrate computer networks and systems supported by cyber infrastructure situated *within the territory of another state* [emphasis added] constitute a violation of that state's territorial sovereignty, irrespective of whether that operation causes damage or harm' (p. 54). This assertion, by the author's own admission, is at variance with the conclusions reached by the majority of Experts responsible for the drafting of the *Tallinn Manual 2.0*, who proposed that 'because cyber espionage involves the collection of confidential information and does not therefore produce destructive effects either offline or online, […] does not qualify as an infringement of the victim state's territorial sovereignty' (p. 53). Ultimately, the chapter clearly articulates the context within which a state's territorial sovereignty would be violated, namely where computer networks and systems supported by cyber infrastructure physically located within its territory are searched for confidential information, irrespective of whether these systems and networks are operated by state organs or private actors and notwithstanding the motives behind accessing such data (p.69). The author finds little utility however in the application of the rules of non-intervention and non-use of force to regulating cyber espionage, concluding that the very definition of cyber espionage (that is the copying of confidential information) indicates that these activities lack the necessary 'coercive element to trigger a violation of the non-intervention rule and does not produce the physical damage necessary to the prohibition on the use of force' (p. 69). The issue of the right of self-defence set out in Article 51 of the Charter of the United Nations 1945 (UN Charter) that is often discussed in the context of the prohibition of the use of force under Article 2(4) UN Charter, is dealt with comprehensively in chapter 8 of the book. The main thrust here is that the fundamental premise that acts of cyber espionage do not qualify as the use of force under Art. 2(4) does not it itself preclude states relaying on self-defence to justify cyber espionage if this conduct is in response to an 'armed attack' and cyber espionage satisfies the customary international law requirements of necessity and proportionality (p. 173). Thus articulated, the author's assertion comports a degree of realism, therefore reflecting the current state practice. Applying the well-entrenched principles articulated by the ICJ in the *Military and*

Paramilitary Activities in and Against Nicaragua and having considered the doctrine of anticipatory self-defence (the 1837 *Caroline* incident) to the practice of states conducting cyber espionage in order to uncover threats to the national security before they materialise (p. 173), the conclusion is unambiguous. Political cyber espionage may be justified on the basis of self-defence only where 'it is designed to shed light on an armed attack that is imminently expected and which is likely to inflict grave violence' but not 'when it is designed to uncover emerging threats' for instead 'non-imminent threats must be addressed by the UN collective security system rather than by states acting unilaterally in the name of self-defence' (p. 173). This threshold of justifiable resort to political cyber espionage to thwart an imminent armed attack is the first barrier against states' unbridled cyber spying, the second and the third being the requirements of necessity and proportionality. As for the doctrine of necessity, this may be invoked only where the acts of cyber espionage are 'designed to mitigate a grave and imminent peril to an essential state interest' (p. 194).

A thorough consideration has also been given to a rather underexplored applicability of the diplomatic and consular law (chapter 4) and the law of the WTO, in particular the Paris Convention 1967 Article 10bis and the Agreement on Trade Related Aspects of Intellectual Property Rights 1997 (chapter 6) . In the former context, the discussion and the analysis has been circumscribed by the application of the Vienna Convention on Diplomatic Relations 1961 and the Vienna Convention on Consular Relations 1963 to demonstrate how this framework relates to and regulates cyber espionage activities. Following a detailed and reasoned application of these rules the conclusion reached is that receiving states are prohibited from conducting acts of cyber espionage of diplomatic missions and consular posts located within their territory, due to the obligation imposed upon them to 'respect the inviolability of the premises, property, documents, correspondence and means of transport' (p. 192). Equally however, diplomatic missions and consular posts are under a duty to comply with the laws of the receiving state and are therefore precluded from engaging in cyber espionage since this offends both national (usually criminal) law and the rule of territorial sovereignty (p. 193).

Further contribution has been made by discussing how international human rights law applies to cyber espionage. The analysis, contained in chapter 5, centres around the International Covenant on Civil and Political Rights 1961 (ICCPR) and European Convention on Human Rights 1950 (ECHR) and focuses on whether cyber espionage targeted against individuals violates the right to privacy as set out under Article 17 and Article 8 respectively. However, in order to engage with these matters, the author's first port of call is to deal with a rather vexed issue of extraterritorial applicability of these human rights treaties so as to examine states' human rights obligations contained therein. In his analysis, the author first addresses the extraterritorial applicability of the ICCPR and again shows no hesitation in engaging with the view expressed by the majority Experts responsible for the drafting of the *Tallinn Manual 2.0*, in whose opinion 'physical control over territory of the individual is required before human rights obligations are triggered' (p. 100). This approach to Buchan is 'unconvincing' both in terms of policy and law, as for him in cyberspace 'states frequently interact with individuals based in foreign territories and often exercise their authority and control over them' (p. 100). His view, reached on the bases of close engagement with the relevant jurisprudence of human rights bodies, the political stance taken by some states and the academic opinion, is incontrovertible-the ICCPR applies to cyber espionage conducted against individuals regardless of where the targeted individuals are located (p. 101). He asserts however, that the same clear conclusion cannot be reached with regards to the extraterritorial applicability of the ECHR, because as evidenced by the author, the

jurisprudence of the Strasbourg court (ECtHR) is far from clear on this issue. Nevertheless, he points to the ECtHR's tentative move towards a more permissive, personal model to establish jurisdiction under the ECHR. In reaching the conclusion that 'online surveillance [..] almost certainly constitute[s] a prima facie violation of the right to privacy' Buchan examines the circumstance where the restriction of this right can be said to be justified. In so doing, he offers a balanced and reasoned argument applying and closely scrutinizing the legal bases for such restriction, namely that of accessibility, foreseeability, and effective oversight, outlining instances and providing sound examples as to where the infringements with this right can be justified.

Buchan is not afraid to express his opinion on a number of issues throughout the monograph and the decisive, well supported and justified stance that he takes in relation to how international law rules apply to state cyber espionage is one of the unique features of this book. In so doing, he authoritatively demonstrates that cyber espionage is subject to a vast array of international law, both general principles and specialist regimes (p. 196). Nevertheless, he recognises and supports the need for states to develop an international law of espionage, which would 'contain bespoke rules that effectively reconcile the competing interests implicated by different forms of espionage, […] which clearly delineate when and under what circumstances the collection of confidential information is acceptable' (p. 195). There is no doubt that the monograph is an important and sound contribution to the existing debate on these issues and will serve as a valuable tool to those who are new to this area of law together with the experts keen to explore the evolution of the legal regimes applicable to state cyber espionage activities.

Dr Eliza Watt
Lecturer in Law
Middlesex University, London
Email: e.watt@mdx.ac.uk