Cyber Espionage and International Law

Russell Buchan

• HART •
OXFORD • LONDON • NEW YORK • NEW DELHI • SYDNEY

HART PUBLISHING

Bloomsbury Publishing Plc

Kemp House, Chawley Park, Cumnor Hill, Oxford, OX2 9PH, UK

HART PUBLISHING, the Hart/Stag logo, BLOOMSBURY and the Diana logo are trademarks of Bloomsbury Publishing Plc

First published in Great Britain 2019

A catalogue record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication data

Names: Buchan, Russell, 1983- author.

Title: Cyber espionage and international law / Russell Buchan.

Description: Oxford, UK ; Portland, Oregon : Hart, an imprint of Bloomsbury, 2019. | Includes bibliographical references and index.

Identifiers: LCCN 2018034245 | ISBN 9781782257349 (hardback : alk. paper)

Subjects: LCSH: Espionage—Law and legislation. | Internet in espionage.

Classification: LCC KZ4079 .B83 2018 | DDC 341.3—dc23 LC record available at https://lccn.loc.gov/2018034245

ISBN: HB: 978-1-78225-734-9
ePDF: 978-1-78225-735-6
ePub: 978-1-78225-736-3

Typeset by Compuscript Ltd, Shannon
Printed and bound in Great Britain by TJ International Ltd, Padstow, Cornwall

To find out more about our authors and books visit www.hartpublishing.co.uk. Here you will find extracts, author information, details of forthcoming events and the option to sign up for our newsletters.

Introduction

1. Background

After land, sea, air and outer space, cyberspace has emerged as the 'fifth domain'[1] of human activity. Over the past several decades, this environment has been progressively 'woven into the fabric of daily life'.[2] Most recent figures indicate that, by the end of 2017, 54 per cent of the world's population were users of the Internet, an increase of 1052 per cent since 2000.[3] Indeed, our reliance upon cyberspace will continue to grow with the proliferation of the so-called 'Internet of Things', a phenomenon that describes a network of physical objects – devices, vehicles, buildings and other items – which are embedded with electronics, software, sensors and network connectivity that enables them to collect and exchange data.

Enormous benefits are now associated with cyberspace. Cyberspace is an inclusive, vibrant and dynamic environment that connects people, empowers communities, expands existing markets and forges new ones, and acts as a global information exchange through which knowledge is disseminated and acquired. However, as well as driving progress, cyberspace has emerged as a repository for a number of threats and vulnerabilities[4] and '[can] be used for purposes that are inconsistent with international peace and security'.[5]

Initially, cyber threats were divided into two distinct categories: cyber network attacks and cyber network exploitation.[6] Cyber network attacks (cyber attacks) describe those computer operations that are designed 'to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or

[1] The Netherlands Ministry of Defence, *The Defence Cyber Strategy* (2012) 4, www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf.

[2] UN Secretary-General, 'Foreword', *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98, 24 June 2013, 4.

[3] Internet World Stats: Usage and Population Statistics, 21 June 2018, www.internetworldstats.com/stats.htm.

[4] 'Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk'; UN Secretary-General, 'Foreword', *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/70/174, 22 July 2015, 4. 'State and non-state actors conduct cyber operations to achieve a variety of political, economic, or military objectives. In conducting their operations, they may strike at a nation's values as well as its interests or purposes'; United States Department of Defense, *The DOD Cyber Strategy* (2015) 1, www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[5] Report of the Group of Governmental Experts 2013 (n 2), 6.

[6] National Research Council, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (WA Owens, KW Dam and HS Lin, 2009).

programs resident in or transiting these systems or networks'.[7] Cyber network exploitation refers to 'the use of cyber offensive actions … usually for the purpose of obtaining information resident on or transiting through an adversary's computer systems or networks'.[8]

As cyberspace has matured, the threats emanating from this environment have become more sophisticated and multifaceted. The consequence is that the bifurcation of cyber threats into destructive cyber attacks on the one hand and non-destructive yet nevertheless damaging cyber network exploitation on the other[9] is no longer adequate to capture the vast array of threats associated with cyberspace. In recent years, a more complex taxonomy has formed and cyber threats now range from hacktivism, cyber vandalism, cyber-crime, cyber terrorism to cyber war.[10] The threat of cyber espionage has emerged as a particular concern for the international society.[11]

Espionage describes the non-consensual collection of confidential information that is under the control of another actor. States are the most prolific perpetrators of espionage[12] and, broadly speaking, they engage in two types of espionage, each defined by reference to the type of information being collected.[13] Political espionage is designed to enhance national security by accessing political and military information that is under the control of other states and, increasingly, prominent

[7] ibid 1–2.

[8] ibid.

[9] 'The main difference between cyber attack and cyber exploitation is that cyber attack is destructive in nature while cyber exploitation is focused on intelligence gathering and, in order to be covert, purposively does not try to affect the normal processes of the computer or network exploited'; A Wortham, 'Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intend That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?' (2012) 64 *Federal Communications Law Journal* 643, 646.

[10] 'Broadly, one can distinguish between cyber war, cyber activism ("hacktivism"), cyber espionage, cyber terrorism, cyberattacks against critical infrastructure, and financially motivated cyber theft'; ZK Goldman and D McCoy, 'Economic Espionage: Deterring Financially Motivated Cybercrime' (2016) 8 *Journal of National Security Law and Policy* 595, 597.

[11] 'More than 100 countries currently have the capacity for digital espionage and their professionalism is growing, as is the threat it poses'; National Coordinator for Security and Counterterrorism: Ministry of Security and Justice, *Cyber Security Assessment Netherlands* (2017) 18, www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2017.html. 'Some of the most sophisticated threats to the UK in cyberspace come from other states which seek to conduct espionage with the aim of spying on or compromising our government, military, industrial and economic assets, as well as monitoring opponents of their own regimes'; UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (2011) para 2.5, www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[12] 'Clandestine intelligence activities are usually associated with nation-states'; MS McDougal, HD Lasswell and WM Reisman, 'The Intelligence Function and World Public Order' (1973) 46 *Temple Law Quarterly* 365, 383.

[13] 'The number of state actors in cyberspace that are involved in cyber espionage targeted at computers connected to the Internet as well as closed networks continues to grow, with their aim being to collect information on both national security as well as economic interests'; Estonia, *Cyber Security Strategy 2014–2017* (2014) 5, www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

non-state actors such as terrorist organisations and their affiliates. States have also demonstrated a proclivity for economic espionage, which is where they seek to boost their national economy by stealing trade secrets that are under the control of companies located within foreign jurisdictions and then passing this confidential information to domestic companies.[14]

States obtain confidential information from a variety of different sources. Information is generally derived from human sources (known as Human Intelligence (HUMINT)) and electronic sources (known as Signals Intelligence (SIGINT)).

Historically, states performed espionage by sending their agents into the physical territory of their adversaries. This is HUMINT in its classic form and has been romanticised in popular culture by espionage novels written by the likes of Ian Fleming and John le Carré. Developments in technology have enabled states to spy on their enemies by using more sophisticated electronic methods (that is, SIGINT), such as the use of high frequency antennas to capture electronic transmissions emanating from the territory of other states and the use of satellites in outer space that are able to observe and monitor events on Earth.[15]

The dawn of cyberspace has dramatically increased the SIGINT capacity of states.[16] The vast quantity of information that resides in cyberspace, the speed and ease with which cyber operations can be launched, and the anonymity that this environment affords, means that '[t]he internet provides a technological platform and target-rich environment for governments to engage in espionage on a scale, speed, intensity, and depth never before witnessed in spycraft'.[17] It is therefore unsurprising that espionage has 'metastasize[d]'[18] since the emergence of cyberspace and that '[political and economic] cyber espionage projects [are] now prevalent'.[19]

[14] 'Espionage can also include the use of state-controlled assets for the purpose of gaining information from a corporation with the aim to improve the knowledge of a competitor based in one's own country'; S Kirchner, 'Beyond Privacy Rights: Crossborder Cyber-Espionage and International Law' (2014) 31 *John Marshall Journal of Information Technology and Privacy Law* 369, 370.

[15] 'States have often used new technologies for espionage purposes'; I Kilovaty, 'World Wide Web of Exploitations – the Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach' (2016) 18 *Columbia Science and Technology Law Review* 42, 62.

[16] 'By its very nature, cyberspace is a medium particularly well suited to espionage in general and commercial and industrial espionage in particular'; S Argaman and G Siboni, 'Commercial and Industrial Cyber Espionage in Israel' (2014) 6 *Military and Strategic Affairs* 43, 44.

[17] DP Fidler, 'Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous Than You Think' (2012) 5 *International Journal of Critical Infrastructure Protection* 28, 29. For Granick, the dawn of cyberspace signals 'a golden age for surveillance'; JS Granick, *American Spies: Modern Surveillance, Why You Should Care, and What To Do About It* (Cambridge, Cambridge University Press, 2017) 53.

[18] DP Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies', 20 March 2013, *ASIL Insights*, www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving.

[19] P Warren, 'State-Sponsored Cyber Espionage Projects Now Prevalent, Says Experts', 30 August 2012, *the Guardian*, www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent. 'No single reason can be given for the increase in trade secret theft. However, one reason

Indeed, the scope and frequency of cyber espionage within the contemporary world order was laid bare in June 2013 when Edward Snowden – a former contractor for the United States (US) National Security Agency (NSA) – disclosed a trove of classified documents to the British newspaper *the Guardian*. These documents revealed that a number of states including the US and the United Kingdom (UK) had utilised an 'extraordinary range of spying methods' to obtain confidential information from a variety of different actors located across the globe.[20] A particularly prominent spying method was the use of cyber operations to collect confidential information that was being stored in or transmitted through cyberspace.[21] Targets of cyber espionage comprised state and non-state actors, including officials of international organisations such as the EU, state organs (including heads of state such as German Chancellor Angela Merkel and Israeli Prime Minister Ehud Olmert), religious leaders (the Pope), companies (such as the Brazilian oil company Petrobras), non-governmental organisations (including UNICEF and Médecins du Monde) and individuals suspected of being involved in international terrorism and other criminal enterprises.[22]

2. The Argument

Notwithstanding the fact that 'intelligence activities are now accepted as a common, even inherent, attribute of the modern state',[23] states have failed to devise either treaty law or customary international law that directly regulates espionage committed during peacetime, demonstrating a degree of 'artful ambiguity'[24] and 'creative ambivalence'[25] on their behalf towards the regulation of this practice. In the absence of international law that specifically addresses peacetime espionage, international lawyers determine that international law is 'remarkably oblivious'[26] to espionage and that, as a result, this is an activity that is 'neither legal nor illegal

for the dramatic increase is undoubtedly the world's ever expanding use of the computer'; H Nasheri, *Economic Espionage and Industrial Spying* (Cambridge, Cambridge University Press, 2005) 9.

[20] E MacAskill and J Borger, 'New NSA Leaks Show how US is Bugging its European Allies', 30 June 2013, *the Guardian*, www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

[21] ibid.

[22] J Ball and N Hopkins, 'GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief', 20 December 2013, *the Guardian*, www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner.

[23] GB Demarest, 'Espionage in International Law' (1996) 24 *Denver Journal of International Law and Policy* 321, 321.

[24] C Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 *Journal of National Security Law and Policy* 179, 205.

[25] ibid 210.

[26] RA Falk, 'Foreword' in RJ Stanger (ed), *Essays on Espionage and International Law* (Columbus, Ohio State University Press, 1962) v. Demarest contends that '[i]nternational law … simply ignores the question of peacetime spying'; Demarest (n 23) 339.

under international law'.[27] This assessment is problematic for a number of reasons, however.

First, from a systemic perspective, the claim that espionage is 'unaddressed'[28] by international law sits uncomfortably with the *Lotus* principle, which provides that in the absence of 'prohibitive rules' of international law 'every State remains free to adopt the principles which it regards as best and most suitable'.[29] In other words, the *Lotus* principle precludes the pronouncement of a *non-liquet*, meaning that under international law state conduct is either lawful and permissible or unlawful and prohibited. Although in recent years the *Lotus* principle has come under criticism for reflecting 'an old, tired view of international law',[30] its legal authority has been affirmed many times by the International Court of Justice[31] (ICJ) and most recently in the *Kosovo* advisory opinion.[32] The upshot of the *Lotus* principle is that, if international law does not directly prohibit espionage, this is a practice that must be permissible under international law.

Second, from a doctrinal standpoint, while espionage per se is residually lawful according to the *Lotus* principle, it is overly simplistic to conclude that international law has 'little impact on the practice of intelligence gathering'.[33] On the contrary, international law has a lot to say on the topic of espionage.[34] In particular, there is a 'checkerboard'[35] of general principles of international law as well as

[27] AJ Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28 *Michigan Journal of International Law* 595, 596. '[I]nternational law neither endorses nor prohibits espionage'; CD Baker, 'Tolerance of International Espionage: A Functional Approach' (2003) 19 *American University International Law Review* 1091, 1092. The view that there is little interaction between international law and espionage explains why 'scholarship on espionage has not been very extensive'; Radsan (n 27) 596. Similarly, Chesterman notes that '[a]cademic literature typically omits the subject [of espionage] entirely, or includes a paragraph or two defining espionage and describing the unhappy fate of captured spies'; S Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2006) 27 *Michigan Journal of International Law* 1071, 1072.

[28] Demarest (n 23) 330.

[29] *The Case of the S.S. Lotus (France v Turkey)*, Judgment [1927] PCIJ Rep (Ser A) No 10 1, 19.

[30] *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* (Advisory Opinion) [2010] ICJ Rep 403, 478 (Declaration of Judge Simma). For further criticism of the *Lotus* principle see H Handeyside, 'The *Lotus* Principle in ICJ Jurisprudence: Was the Ship Ever Afloat?' (2007) 29 *Michigan Journal of International Law* 71.

[31] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, Judgment (Merits) [1986] ICJ Rep 14.

[32] *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* (Advisory Opinion) [2010] ICJ Rep 403.

[33] G Sulmasy and J Yoo, 'Counterintuitive: Intelligence Operations and International Law' (2007) 28 *Michigan Journal of International Law* 625, 625.

[34] Chesterman asks '[w]hat, then – if anything – does international law have to say about the subject [of espionage]? A surprising amount'; Chesterman (n 27) 1072. '[M]any rules of international law may be engaged by spying, depending on the nature of that spying and its geographic location'; Forcese (n 24) 185. 'I believe there is a great deal of interaction between international law and intelligence activities'; JH Smith, 'Keynote Address: State Intelligence Gathering and International Law' (2007) 28 *Michigan Journal of International Law* 543, 544.

[35] Forcese (n 24) 209.

specialised international legal regimes that indirectly regulate espionage insofar as they appertain to the conduct that underlies the espionage operation,[36] with the consequence being that international law 'constrain[s] some practices in some places and in relation to some actors'.[37]

But why do international lawyers maintain the fiction that there is no interaction between international law and espionage?[38] The truth is that international lawyers have been consciously unwilling to apply international law to this practice and, as Chesterman observes, espionage 'is less a lacuna in the legal order than it is the elephant in the room'.[39] The reasons for this agnosticism are clear.

With regard to political espionage, even though international law implements a number of rules that are intended to protect state sovereignty and thus maintain international peace and security, international lawyers nevertheless perceive the world order to be unpredictable and dangerous. In such an environment, they are reluctant to accept that legal rules are able to effectively protect state sovereignty and thereby maintain international peace and security.[40] International lawyers have thus been loath to apply legal rules that curtail the ability of states to undertake espionage, which is regarded as 'necessary for the national security of a nation-state'[41] because it allows states to better understand the intentions and capabilities of other actors operating within the world order.

International lawyers are therefore faced with a dilemma. On the one hand, they cannot deny that international legal rules are applicable to intrusive activities such as espionage because to do so would challenge the authority of international law. On the other hand, they are equally unwilling to renounce espionage as a tool of statecraft because they wish to preserve the national security benefits that this practice affords. Ultimately, their only way out of this impasse is to eschew the question of whether espionage is compatible with international law and proclaim that 'international law is silent on the subject'.[42] Indeed, seemingly

[36] 'It is the underlying act that determines the legality of such cyber operations, not the fact that they are engaged in for the purpose of espionage'; MN Schmitt, 'Cyber Responses "By the Numbers" in International Law', 4 August 2015, EJIL: *Talk!*, www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/. 'While the International Group of Experts agreed that there is no prohibition of espionage *per se*, they likewise concurred that cyber espionage may be conducted in a manner that violates international law due to the fact that certain methods employed to conduct cyber espionage are unlawful'; MN Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, Cambridge University Press, 2017) 170.

[37] C Forcese, 'Creative Ambiguity – International Law's Distant Relationship with Peacetime Spying', 14 November 2013, *Just Security*, www.justsecurity.org/3168/guest-post-creative-ambiguity-international-laws-distant-relationship-peacetime-spying/.

[38] As Sulmasy and Yoo note, '[f]ew have questioned whether intelligence collection activities violate international law'; Sulmasy and Yoo (n 33) 629.

[39] Chesterman (n 27) 1072.

[40] 'One of the fundamental tenets of international law is, of course, that one state not intervene in the internal affairs of another state. It may be a fundamental principle, but it is also fairly tattered. States seek to influence each other daily'; Smith (n 34) 545.

[41] Sulmasy and Yoo (n 33) 628.

[42] G Brown, 'Spying and Fighting in Cyberspace: What is Which?' (2016) 8 *Journal of National Law and Policy* 621, 621.

frustrated by the conundrum that espionage presents for international lawyers Radsan urges: 'Accepting that espionage is beyond the law, we should move on to other projects – with grace.'[43]

Radsan's comments were made in 2007, several years before cyber espionage burst onto the international scene. The dramatic increase in political espionage since the advent of cyberspace has meant that walking away from the espionage debate – with or without grace – has not been possible. While at one point in time it may have been acceptable for international lawyers to turn a blind eye to espionage, it is not appropriate to ignore *cyber-enabled* espionage.[44]

In response, there has been a surge in international legal scholarship dedicated to the topic of political cyber espionage.[45] Yet, under the influence of realist theory, scholars remain fixated upon the national security benefits afforded by political cyber espionage and insist that, as with more traditional forms of political espionage, this conduct operates in a 'legal black hole'.[46] For one commentator, '[c]yberspace remains a netherworld for intelligence activities – whatever surveillance or cyber spying a government does outside of its own national borders is, in most instances, an international law free-for-all'.[47] *Plus ça change, plus c'est la même chose*.

[43] Radsan (n 27) 597. Similarly, Brown and Poellet argue that '[espionage] occupies an ill-defined policy space that permits it to occur without violating international law'; G Brown and K Poellet, 'The Customary International Law of Cyberspace' (2012) 6 *Strategic Studies Quarterly* 126, 133.

[44] '[C]yber espionage has stirred the conventional international complacency by bringing the permissibility of foreign intelligence operations into the daily public spotlight'; D Pun, 'Rethinking Espionage in the Modern Era' (2017) 18 *Chicago Journal of International Law* 353, 385. Deeks explains that since the dawn of cyberspace there has been a 'shift from agnosticism' among international lawyers when it comes to the role of international law in regulating espionage; A Deeks, 'An International Legal Framework for Surveillance' (2015) 55 *Virginia Journal of International Law* 291, 315.

[45] See I Navarrete, 'L'Espionnage en Temps de Paix en Droit International Public' (2016) 53 *Canadian Yearbook of International Law* 1; R Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage' in A-M Osula and H Rõigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (CCDCOE, 2016); K Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (CCDCOE, 2013); RD Williams, '(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action' (2011) 79 *The George Washington Law Review* 1162; C Khalil, 'Thinking Intelligently about Intelligence: A Model Global Framework Protecting Privacy' (2015) 47 *George Washington International Law Review* 919; PCR Terry, '"Absolute Friends": United States Espionage Against Germany and Public International Law' (2015) 28 *Revue Quebecoise de Droit International* 173; C Forcese, 'Pragmatism and Principle: Intelligence Agencies and International Law' (2016) 102 *Virginia Law Review Online* 67; Brown and Poellet (n 43); Deeks (n 44).

[46] Fidler (n 17) 29. 'Espionage has been considered unregulated under the international legal system – meaning cyber activities that constitute espionage are neither lawful nor unlawful under international law'; Brown (n 42) 622.

[47] WC Banks, 'Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage' (2017) 66 *Emory Law Journal* 513, 518.

Why are international lawyers averse to examining the application of international law to *economic* espionage? This question is particularly intriguing given that economic espionage impinges upon the sovereignty of the state that hosts the company whose trade secrets have been appropriated and also has a deleterious impact upon its national economy. However, unlike political espionage, economic espionage does not confer upon the perpetrating state direct and immediate national security benefits. Although economic espionage does ultimately strengthen the perpetrating state's national security (by boosting its economic security), its immediate benefit is that it helps domestic companies remain competitive vis-a-vis their foreign rivals.

Seemingly, the concern among international lawyers is that if they undertake an inquiry into the role of international law in regulating economic espionage this may open up a Pandora's box, raising questions as to how international law applies to political espionage. Stated succinctly, if political espionage is a 'dirty word'[48] that is off-limits to the regulatory gaze of international lawyers, then so too is economic espionage.

At least historically, economic espionage was not as prevalent within the world order as political espionage and this made it easier for international lawyers to ignore the threats posed by economic espionage in favour of insulating political espionage from international legal appraisal. Given the upsurge in economic espionage since the dawn of cyberspace and in light of the damage that it inflicts upon state sovereignty and national economies, the public and private sectors have increasingly called upon international lawyers to scrutinise whether and to what extent international law can be used to counteract economic cyber espionage.[49] But to date, international lawyers have directed remarkably little attention towards exploring the application of international law to economic cyber espionage. Of those that have, most preserve the myth that international law remains 'a bystander to this entire fabric of stealth, deception, and greed'.[50] Again, it seems that international lawyers are concerned that, if economic cyber espionage is submitted to intensive international legal review, this scrutiny will be extended to political cyber espionage, which may open up the possibility that international law will be used to restrict the availability of politically motivated espionage and thus deny the national security benefits that it affords.

In light of the above, the objective of this monograph – and its original contribution to existing academic literature – is to identify the international legal rules implicated by political and economic cyber espionage and to assess the extent to which they regulate this conduct.

[48] International Peace Academy, *Peacekeeper's Handbook* (1984) 39, 59–62, 120–21.

[49] See JP Farwell and D Arakelian, 'China Cyber Charges: Take Beijing to the WTO Instead', 20 May 2014, *The National Interest*, www.nationalinterest.org/blog/the-buzz/china-cyber-charges-take-beijing-the-wto-instead-10496.

[50] Banks (n 47) 517.

3. Chapter Overview

This monograph adheres to the following structure. Chapter 1 frames the scope of this project by formulating a working definition of the concept of cyber espionage. The chapter drills down into the various features of this definition in order to provide a fuller understanding of the types of activity that cyber espionage describes and, in particular, to outline the types of conduct that will be subject to international law analysis as this monograph progresses.

Chapter 2 examines the impact of political and economic cyber espionage upon international relations. This chapter claims that states inhabit an international society that links the maintenance of international peace and security to the protection of the principles of the sovereign equality of states and human dignity. It argues that political espionage represents a threat to the maintenance of international peace and security because, where this conduct is directed against a state or a non-state actor located within another state, it violates the principle of the sovereign equality of states and, where this conduct is targeted against individuals, it violates the principle of human dignity. Additionally, this chapter maintains that, because political espionage is incompatible with the foundational principles of the international society, it disrupts the potential for close and effective cooperation within the society and thus inhibits its ability to address threats to international peace and security. Moreover, this chapter describes the direct and indirect costs that economic espionage inflicts upon victim companies and the negative impact this has upon their financial stability. Where companies struggle financially, the national economy of the host state is also adversely affected. Given that national security is nowadays contingent upon economic security, economic espionage can be said to endanger national security and by implication international peace and security. That cyberspace enhances the capacity of states to perpetrate political and economic espionage means that the threat that these practices represent to international peace and security is magnified in the cyber setting. Appreciating the severity of this threat, this chapter concludes that the international society must possess international legal rules that unambiguously prohibit political and economic cyber espionage.

Chapter 3 analyses the application of the rules of territorial sovereignty, non-intervention and the non-use of force to cyber espionage. This chapter argues that cyber operations that penetrate computer networks and systems supported by cyber infrastructure located within the territory of another state trigger a violation of the territorial sovereignty rule, regardless of whether that cyber infrastructure is operated by state organs or private actors. The rule of territorial sovereignty therefore provides an important and powerful source of legal protection against political and economic cyber espionage. Yet, this chapter concludes that cyber espionage is unlikely to transgress the rule of non-intervention given that such conduct lacks the requisite coercive element. Similarly, the prohibition on the use of force is inapplicable to cyber espionage on the basis

that this activity does not produce physical damage within the territory of the victim state.

Chapter 4 investigates the role of diplomatic and consular law in regulating political cyber espionage. This chapter argues that diplomatic and consular law confers inviolability upon the premises, documents and official correspondence of diplomatic missions and consular posts. Where a state interferes with diplomatic missions and consular posts by launching acts of cyber espionage against them, or otherwise fails to protect these missions and posts from acts of cyber espionage perpetrated by other actors, this conduct (or lack thereof) undoubtedly violates these rules. This chapter also maintains that diplomatic and consular law prohibits the diplomatic missions and consular posts of sending states from engaging in acts of cyber espionage while operating within the receiving state.

Chapter 5 assesses the application of international human rights law to acts of cyber espionage targeted against individuals, with particular reference to the International Covenant on Civil and Political Rights (ICCPR) 1966 and the European Convention on Human Rights (ECHR) 1950. An important preliminary question relates to the territorial scope of the obligations contained within these human rights treaties. It is well-accepted that states owe these human rights obligations in cyberspace to individuals located within their territory. But what about the situation where a state's online activities impinge upon the human rights of individuals located within *foreign* territory, which is often the case with cyber espionage? As this chapter reveals, the human rights bodies that oversee the implementation of the ICCPR have consistently determined that states are subject to a negative obligation to respect human rights where they exercise their authority and control against individuals located abroad, including where this authority and control is exercised within (or through) cyberspace. The European Court of Human Rights (ECtHR) has failed to articulate a clear and consistent approach as to when a state's human rights obligations under the ECHR apply extraterritorially, although its more recent jurisprudence tentatively endorses the model adopted under the ICCPR. With regard to substantive human rights, this chapter argues that cyber espionage is most likely to run into conflict with the right to privacy (as contained in Article 17 ICCPR and Article 8 ECHR), which protects a person's information and communications from interference. At the same time, this chapter acknowledges that privacy is not an absolute right and explores the circumstances in which it can be permissibly restricted in the context of online surveillance.

Chapter 6 evaluates whether the trade agreements that fall under the authority of the World Trade Organization (WTO) apply to economic cyber espionage. Specifically, Article 10*bis* of the Paris Convention 1967 requires that members assure to nationals (including legal persons, that is, companies) of other members effective protection against acts of unfair competition. This chapter maintains that economic cyber espionage constitutes an act of unfair competition within the meaning of Article 10*bis*. Article 10*bis* therefore prohibits members from engaging

in acts of economic cyber espionage against Paris Union nationals located within their territory and, in light of the wording of Article 10*bis*, against Paris Union nationals located abroad, which is important given the transboundary nature of economic cyber espionage. Article 39.2 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) 1994 imposes an obligation upon members to establish causes of action under national law so that nationals (including legal persons) of TRIPS members can protect their undisclosed information from unauthorised acquisition, disclosure or use. While this provision does not directly prohibit members from engaging in economic cyber espionage against nationals of TRIPS members, nevertheless it makes an important contribution to the suppression of this activity insofar as it requires all members to implement minimum legal standards relating to the protection of confidential information.

International legal scholars accept that acts of political cyber espionage may violate certain primary rules of international law, such as the rule of territorial sovereignty and the inviolability provisions of diplomatic and consular law. Yet, by and large, these scholars assert that developments in customary international law have carved out permissive espionage exceptions to these otherwise prohibitive rules. Chapter 7 rejects this contention. This chapter argues that these types of customary exceptions have not come into existence because they are not supported by state practice or *opinio juris*, the essential ingredients of customary international law. With regard to state practice, espionage is usually committed in secret. However, secret state conduct does not qualify as state practice for the purpose of customary international law formation. Moreover, while instances of espionage are widely and credibly reported, states almost always fail to acknowledge responsibility for their espionage operations and unacknowledged state conduct does not count as state practice for the purpose of customary international law development. Even if we accept *arguendo* that sufficient state practice of these types of espionage exists, the policy of silence that states have adopted towards their espionage activities prevents the formation of *opinio juris*, the absence of which precludes the crystallisation of espionage exceptions under customary international law.

Chapter 8 considers the application of the doctrines of self-defence and necessity to acts of political and economic cyber espionage. This chapter argues that states can only invoke self-defence to justify acts of cyber espionage where they are the victim of an actual or imminent threat of an armed attack. Moreover, cyber espionage undertaken in self-defence must not exceed what is necessary and proportionate in the circumstances to halt and repel an armed attack or to prevent further reasonably foreseeable attacks. Additionally, this chapter argues that the defence of necessity can exculpate state responsibility for unlawful acts of cyber espionage where they are necessary to safeguard an essential state interest from a grave and imminent peril and providing they do not seriously impair an essential interest of the victim state(s) or of the international

community as a whole. This chapter concludes that the restrictions to which self-defence and necessity are subject are so stringent that, in practice, these defences will be rarely available to justify acts of political and economic cyber espionage.

Contrary to the mainstream view, cyber espionage does not exist in an international law vacuum. However, notwithstanding the applicability of international law, this monograph concludes by arguing that states should devise and implement a *lex specialis* framework that contains bespoke international legal rules that directly and specifically regulate cyber espionage.