International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

CHAPTER 4

The International Legal Regulation of State-Sponsored Cyber Espionage

Russell Buchan

1. Introduction

States are highly competitive actors and the competitiveness that exists between them has become increasingly intensified as the world order has become ever more globalised. In order to be successful and prosperous in this competitive environment states require access to reliable intelligence that reveals the strengths and weaknesses of their competitors.[1] Knowledge is power, after all.

A significant amount of intelligence collected by states is from sources which are publically available. Espionage is a prevalent method of gathering intelligence and describes 'the consciously deceitful collection of information, ordered by a government or organisation hostile to or suspicious of those the information concerns, accomplished by humans unauthorised by the target to do the colleting'.[2] Espionage, then, is the unauthorised collection of non-publically available information. The act of espionage can be committed through various methods. In its traditional conception, espionage describes the practice whereby a state dispatches an agent into the physical territory of another state in order to access and obtain confidential

1 'Responsible leaders in every nation seek knowledge – and, ideally foreknowledge – of the world around them. For with a better understanding of global affairs, they are apt to protect and advance more effectively the vital interests of their citizens'; Loch K. Johnson, *Secret Agencies: US Intelligence in a Hostile World* (Yale University Press, 1998), 1.

2 Geoffrey B. Demarest, 'Espionage in International Law,' *Denver Journal of International Law and Policy* 24 (1996): 326.

information.[3] States have, however, exploited technological developments in order to devise more effective methods through which to conduct espionage. Since the emergence of vessels, aeroplanes and celestial bodies, the sea, the skies and outer space have all been used as platforms to engage in (often electronic) surveillance of adversaries; that is, to commit espionage from afar.[4] It therefore comes as no surprise that since its creation cyberspace has also been harnessed as a medium through which to commit espionage.[5] Indeed, the exploitation of cyberspace for the purpose of espionage has emerged as a particularly attractive method to acquire confidential information because of the large amount of information that is now stored in cyberspace and because cyberspace affords a considerable degree of anonymity to perpetrators of espionage and is thus a relatively risk free enterprise.

Unsurprisingly, espionage has 'metastasised'[6] since the emergence of cyberspace and reports suggest that 'cyber espionage projects [are] now prevalent'.[7] As an illustration, in February 2013 the Mandiant Report identified China as a persistent perpetrator of cyber espionage.[8] In fact, the report claims that a cyber espionage entity known as Unit 61398 has been specifically created by the Chinese government and is formally incorporated into the Chinese People's Liberation Army. The Report suggests that Unit 61398 is responsible for organising and instigating a massive cyber espionage campaign against other states and non-state actors, seeking to exploit vulnerable computer systems in order to access sensitive and confidential information with the aim of bolstering China's position in the international political and economic order.

Only 4 months later in June 2013 cyber espionage was again thrust firmly into the international spotlight when Edward Snowden, a former contractor for the US National Security Agency (NSA), disclosed through WikiLeaks thousands of classified documents to several media entities including *The Guardian* and *The New York Times*. The documents were alleged to reveal that the NSA had been engaged in a global surveillance programme at the heart of which was the collection of confidential information that was being stored in or transmitted through cyberspace. In particular, the allegations were that the NSA had been engaged in a sustained and widespread campaign of intercepting and monitoring private email and telephone communications. This cyber espionage allegedly targeted numerous state and non-state actors, including officials of international organisations such as the EU, state organs (including heads of state such as

3 The use of individuals to obtain information is referred to as human intelligence (HUMINT).

4 Obtaining information by communications intercepts or other electronic surveillance is referred to as signals intelligence (SIGINT).

5 Cyber espionage is defined as '[o]perations and related programs or activities conducted … in or through cyberspace, for the primary purpose of collecting intelligence … from, computers, information or communication systems, or networks with the intent to remain undetected'; Presidential Policy Directive/PPD-20, *U.S. Cyber Operations Policy* (October 2012), http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf.

6 David Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Technologies,' *AJIL Insights*, March 20, 2013, http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving.

7 Pete Warren, 'State-Sponsored Cyber Espionage Projects Now Prevalent,' *The Guardian*, 30 August, 2012, http://www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent.

8 Mandiant Intelligence Center Report, *APT1: Exposing One of China's Cyber Espionage Units*, 19 February, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

German Chancellor Angela Merkel and Israeli Prime Minister Ehud Olmut), religious leaders (the Pope), companies (such as the Brazilian oil company Petrobas), non-governmental organisations (including UNICEF and Médecins du Monde) and individuals suspected of being involveed in international terrorism.[9]

In light of the scale and intensity of cyber espionage in contemporary international relations commentators have claimed that 'cyber espionage is more dangerous than you think'.[10] Important questions are now rightly being raised as to whether cyber espionage is a permissible cat-and-mouse exercise that is part of the ebb and flow of a competitive international environment, or whether it is a pernicious practice that undermines international cooperation and is prohibited by international law. This article assesses the international legality of transboundary state-sponsored cyber espionage and therefore further contributes to the ongoing discussion of which and to what extent international legal rules regulate malicious transboundary cyber operations.[11]

This article is structured as follows. Section 2 identifies the international law implicated by cyber espionage. In section 3, I argue that when cyber espionage intrudes upon cyber infrastructure physically located within the territory of another state, such conduct constitutes a violation of the principle of territorial sovereignty. In section 4, I contend that where a state stores information outside of its sovereign cyber infrastructure or transmits its information through the cyber architecture of another state, the appropriation of that information can, in sufficiently serious circumstances, amount to a violation of the non-intervention principle. Section 5 assesses whether the seemingly widespread state practice of espionage has given rise to a permissive rule of customary international law in favour of espionage generally and cyber espionage in particular. Section 6 offers some conclusions.

2. Cyber Espionage and International Law

The general starting point for determining the international legality of state conduct is the well-known *Lotus* principle.[12] Stated succinctly, this principle provides that international law leaves to states 'a wide measure of discretion which is limited only in certain cases by prohibitive rules' and that in the absence of such rules

9 For an overview of the Snowden revelations see, Ed Pilkington, 'The Snowden Files – Inside the Surveillance State,' *The Guardian*, 2 December, 2013, http://www.theguardian.com/technology/2013/dec/03/tim-berners-lee-spies-cracking-encryption-web-snowden.

10 David Fidler, 'Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous than You Think,' *International Journal of Critical Infrastructure* 5 (2012): 29.

11 The focus of this chapter is upon the international legality of state-sponsored cyber espionage. Non-state actors such as companies are also frequent perpetrators of cyber espionage. Time and space limitations mean however that my analysis is restricted to acts of cyber espionage that are legally attributable to states under the rules on state responsibility.

12 The Case of S.S. 'Lotus' (France v. Turkey), ser. A. - No. 10 Publications of the PCIJ (Permanent Court of International Justice 1927). Interestingly, in the Kosovo Advisory Opinion, Judge Simma referred to the Lotus principle as an 'old, tired view of international law'; Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion (Declaration of Judge Simma), ICJ Reports 2010, p. 403, para. 2.

'every State remains free to adopt the principles which it regards best and most suitable'.[13]

There is no specific international treaty that regulates cyber espionage. There is also no specific international treaty that regulates espionage and which could be adapted to regulate cyber espionage.[14] However, in an international legal order premised upon the sovereign equality of states,[15] it is inherent in the nature of an intrusive transboundary activity such as cyber espionage that this type of conduct can run into conflict with general principles of international law. In this sense, whilst cyber espionage is not specifically regulated by international law it may be nevertheless unlawful when appraised against general principles of international law.

The principle of state sovereignty is often regarded as a constitutional norm of international law and is the basis 'upon which the whole of international law rests'.[16] However, '[s]overeignty has different aspects'[17] and in order to protect the different features of state sovereignty the international community has developed various principles of international law. These include the principle of territorial sovereignty, which protects the territory of a state from external intrusion;[18] the principle of non-intervention, which protects the political integrity of a state from coercion;[19] the prohibition against the use of force,[20] which protects states against the use of violence, and where the use of violence is of sufficient scale and effects international law casts such conduct as an armed attack entitling the victim state to use force in self-defence.[21] Given that cyber espionage does not involve the use of violence, this chapter will not consider whether cyber espionage can amount to a use of force or an armed attack. Instead, my focus will be upon whether cyber espionage violates the principles of territorial sovereignty and non-intervention.[22]

13 The Case of S.S. 'Lotus', paras. 18-19.

14 At least during times of peace. Espionage, and by extension cyber espionage, committed during times of armed conflict is subject to Article 46 of Additional Protocol 1 (1977) to the Geneva Conventions (1949). See *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)* (8 June 1977), Article 46, https://www.icrc.org/ihl/INTRO/470. This chapter, however, concerns the international legality of cyber espionage committed outside of armed conflict.

15 United Nations, *Charter of the United Nations* and *Statute of the International Court of Justice* (24 October 1945), 1 UNTS XVI, Article 2(1).

16 Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 14 Reports of Judgments, para. 263 (International Court of Justice 1986).

17 Robert Jennings and Adam Watts, eds., *Oppenheim's International Law*, 9th edn (London: Longman, 1996), 382.

18 The Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania), 1, 35 Reports of Judgments (International Court of Justice 1949).

19 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 202.

20 United Nations, *Charter of the United Nations*, Article 2(4).

21 Ibid, Article 51.

22 Whether cyber espionage contravenes international human rights law is outside of the scope of this chapter. On cyber espionage and international human rights law see David Fidler, 'Cyberspace and Human Rights,' in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar, 2015).

3. The Principle of Territorial Sovereignty

Sovereignty denotes *summa potestas* – the capacity to exercise full and exclusive authority. In international law the emergence of the concept of sovereignty 'coincided with the emergence of the State as a political unit following the apportionment of territories and the political and legal recognition of such territorial compartmentalisation by the Treaty of Westphalia'.[23] As a result, sovereignty is typically understood as the right of states to exercise exclusive authority over their territory. As Arbitrator Max Huber explained in the *Island of Palmas* Arbitration Award, '[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right therein, to the exclusivity of any other States, the functions of a State'.[24] In the words of the International Court of Justice (ICJ) in the *Corfu Channel* case, '[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations'.[25] There is thus little doubt that the principle of territorial sovereignty is firmly entrenched in international law.

In order to constitute a violation of the principle of territorial sovereignty is the mere intrusion into a state's territory unlawful or, in addition, must the intrusion produce physical damage?[26] This is an important question in the context of cyber espionage because this is a practice that describes the accessing and copying of confidential information and is committed regardless of whether information is lost or damaged (in the sense that it is modified or deleted); in short, cyber espionage cannot be said to produce physical damage.

Wright argues for a broad definition of the principle of territorial sovereignty which does not require the infliction of physical damage. Writing in the context of traditional espionage, Wright explains that:

> '[i]n times of peace … espionage and, in fact, any penetration of the territory of a state by agents of another state in violation of the local law is also a violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of other states.'[27]

23 Nicholas Tsagourias, 'The Legal Status of Cyberspace,' in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar, 2015), 17.

24 Island of Palmas Case (Netherlands v. USA), 2 RIAA 829, 838 (Perm. Ct. Arb. 1928).

25 The Corfu Channel Case, 35.

26 The Commentary to the *Tallinn Manual* explains that the International Group of Experts agreed that an intrusion into the territory of another state which causes physical damage results in a violation of territorial sovereignty but notes that there was 'no consensus' between the experts as to whether intrusion into territory that does not produce physical damage also represents a violation; Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 16.

27 Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs,' in *Essays on Espionage and International Law*, ed. Richard Falk (Ohio State University Press, 1962), 12. '[The principle of territorial integrity] negates the general permissibility of strategic observation in foreign territory'; John Kish and David Turns, *International Law and Espionage* (Boston: Martinus Nijhoff, 1995), 83.

It is on the same basis that the use of reconnaissance aeroplanes in the territorial airspace of another state is generally accepted as an unlawful infraction of the territorial sovereignty of that state.[28]

Importantly, there is support for this broad interpretation of the principle of territorial sovereignty within international jurisprudence. In the *Lotus* case the Permanent Court of International Justice explained that the 'first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State'.[29] In the *Corfu Channel* case the ICJ determined that the UK's decision to send warships into Albania's territorial waters to collect evidence of illegal mining represented an unauthorised incursion into Albania's territory and thus 'constituted a violation of Albanian sovereignty'.[30] Although physical evidence was collected from Albanian territory, a careful reading of the ICJ's judgment reveals that the Court determined that the UK's conduct was unlawful solely on the basis of its unauthorised intrusion into Albania's territorial sea.

The weight of evidence, then, suggests that a violation of territorial sovereignty occurs where a state makes an unauthorised intrusion into the territory of another state, regardless of whether physical damage is caused.[31]

Turning now to the international legality of transboundary cyber conduct, the initial question is whether states possess territorial sovereignty in cyberspace. At its creation commentators asserted that cyberspace was an a-territorial environment and, because of the interdependent relationship between territory and sovereignty (territory contains sovereign power within strictly defined physical parameters), international legal concepts such as territorial sovereignty were not applicable to cyberspace.[32]

In light of state practice, however, '[t]he argument that cyberspace constitutes a law-free zone is no longer taken seriously'.[33] In particular, state practice clearly reveals that states regard themselves as exercising sovereignty in cyberspace.[34]

---

28 'The principle of the respect for territorial sovereignty is also directly infringed by the unauthorized overflight of a State's territory by aircraft belonging to or under the control of the government of another State'; Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 251.

29 The Case of S.S. 'Lotus', paras. 19-20.

30 The Corfu Channel Case, 35.

31 '[D]amage is irrelevant and the mere fact that a State has intruded into the cyber infrastructure of another State should be considered an exercise of jurisdiction on foreign territory, which always constitutes a violation of the principle of territorial sovereignty'; Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace,' *International Law Studies* 89 (2013): 129. For the opposing view that physical damage is required see Katharina Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law,' in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy,* ed. Katharina Ziolkowski (Tallinn: NATO CCD COE Publications, 2013), 458.

32 David Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace,' *Stanford Law Review* 48 (1996): 1367.

33 For a discussion of this state practice see Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention,' *Baltic Yearbook of International Law* 14 (2014): 142.

34 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General*, A/68/98 (24 June 2013), paras. 19-20, https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf; 'Long-standing international norms guiding state behaviour – in times of peace and conflict – also apply in cyberspace': The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011), 9, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; see also Schmitt, *Tallinn Manual*, Rule 1.

Moreover, states assert that they exercise *territorial* sovereignty in cyberspace.[35] Although on the face of it cyberspace would appear immune from territorial sovereignty because it is a virtual, borderless domain, it must nevertheless be appreciated that cyberspace is a man-made environment that 'requires physical architecture to exist',[36] including fibre-optic cables, copper wires, microwave relay towers, satellite transponders, Internet routers etc. As a result, where computer networks are interfered with, or where information is interfered with that is located on those networks, and those networks are supported by cyber infrastructure physically located in a state's territory, that state's territory can be regarded as transgressed and thus a violation of the principle of territorial sovereignty occurs.[37] Note that the key issue is not to whom the cyber infrastructure belongs but whether it is located on the territory of the state: 'it is irrelevant whether the cyber infrastructure protected by the principle of territorial sovereignty belongs to or is operated by government institutions, private entities or private individuals'.[38]

In relation to cyber espionage specifically, as I noted in the introduction to this article there has been a dramatic increase in this practice in recent years. State practice in this area is instructive and indicates that where computer systems are accessed and information is obtained that is resident on or transmitting through those computer networks, states consider their territorial sovereignty violated where those networks are supported by cyber infrastructure located within their territory. To put the same matter differently, there is state practice to suggest that where a state considers itself to have been the victim of cyber espionage it regards such behaviour as falling foul of the principle of territorial sovereignty.

For example, when it was revealed that the US had routinely committed cyber espionage against Brazil, Brazilian President Dilma Rousseff cancelled a scheduled visit to Washington DC to meet representatives of the Obama administration to discuss important issues of international concern. Instead, she proceeded to New York to formally denounce the NSA's activities before the UN General Assembly. Indeed, in doing so she explained that cyber espionage violates state sovereignty:

> 'intrusion [and] [m]eddling in such a manner in the life and affairs of other countries is a breach of international law [and] as such an affront to the principles that must guide the relations among them, especially among friendly nations. A country's sovereignty can never affirm itself to the detriment of another country's sovereignty.'[39]

35 For a discussion of this state practice see von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace,' 126 ('State practice provides sufficient evidence that components of cyberspace are not immune from territorial sovereignty'). For further discussion see Sean Kanuck, 'Sovereign Discourse on Cyber Conflict under International Law,' *Texas Law Review* 88 (2010): 1571.

36 Patrick W. Franzese, 'Sovereignty in Cyberspace: Can it Exist?' *Air Force Law Review* 64 (2009): 33.

37 Rule 1 of the Tallinn Manual explains that '[a] State may exercise control over cyber infrastructure and activities within its sovereign territory': Schmitt, *Tallinn Manual*.

38 Von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace,' 129. For a similar view see Schmitt, *Tallinn Manual*, 16.

39 Quoted in Julian Borger, 'Brazilian President: US Surveillance a 'Breach of International Law,' *The Guardian* September 24, 2013, http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

The President further noted that Brazil's objections to such 'illegal actions' had been communicated to the US by 'demanding explanations, apologies and guarantees that such acts or procedures will never be repeated again'.[40] Germany also stated that the conduct was 'completely unacceptable',[41] with France claiming that it 'cannot accept this kind of behaviour from partners and allies'.[42] China adopted a similar position, determining that the NSA had 'flagrantly breached international laws, seriously infringed upon the [sic] human rights and put global cyber security under threat'.[43] China further declared that the NSA's conduct 'deserve[d] to be rejected and condemned by the whole world'.[44]

The Snowden revelations have provoked a considerable international backlash from the international community and much of this criticism has been from a political, moral and even economic perspective. Schmitt and Vihul therefore correctly suggest that we approach state reactions to the Snowden revelations with caution because their 'comments do not necessarily confirm their position on the legality of the [surveillance] programme'.[45] International relations are of course complex and operate on various different levels and it is therefore necessary to approach state responses to international events cautiously and we need to be careful not to overstate the international legal significance of their claims. For example, France's claim that it 'cannot accept this kind of behaviour from partners and allies' can perhaps be interpreted in a variety of ways and such a statement does not unambiguously indicate that France considered the NSA's conduct to be in violation of international law. In addition, it is curious that France determines that cyber espionage is unacceptable when committed by states that it regards as its 'partners and allies'. One also needs to take with a pinch of salt China's condemnation of the NSA's activities given that only a few months before the Snowden revelations the Mandiant Report alleged that China is a persistent perpetrator of cyber espionage. However, the fact the Brazilian President cancelled a scheduled visit to Washington DC to meet the Obama administration, instead preferring to address the plenary body of the UN (the General Assembly), and in doing so carefully and purposively invoked unequivocal language in criticising the US's actions from an international law perspective, must be taken seriously when attempting to discern how the international community reflected upon the international legality of the NSA's conduct. The German position that the NSA's conduct was 'completely unacceptable' also implies condemnation of the NSA's conduct in every dimension (legal, political, ethical etc.) and can be reasonably construed as an international legal rebuke of the NSA's cyber espionage activities.

40 Ibid.

41 Quoted in 'Merkel Calls Obama about "US Spying on Her Phone"', *BBC News*, October 23, 2013, http://www.bbc.co.uk/news/world-us-canada-24647268.

42 Quoted in 'Hollande: Bugging Allegations Threaten EU-US Trade Pact,' *BBC News*, July 1, 2013, http://www.bbc.co.uk/news/world-us-canada-23125451.

43 Quoted in 'China Demands Halt to 'Unscrupulous' US Cyber-Spying,' *The Guardian*, May 27, 2014, http://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying.

44 Ibid.

45 See chapter 2 by Michael N. Schmitt and Liis Vihul, 44.

In this section I have argued that the principle of territorial sovereignty protects the territory of states from physical intrusion regardless of whether the intrusion produces damage. I have further argued that states exercise territorial sovereignty over cyber infrastructure that is physically located within their territory. As a result, I contend that acts of cyber espionage that intrude on the cyber infrastructure of a state for the purpose of intelligence-gathering constitute a violation of the principle of territorial sovereignty. I have alluded to recent examples of state practice in the context of cyber espionage to support this interpretation of international law.

4. The Principle of Non-Intervention

Cyberspace is used primarily as a domain for information communication. As such, it is possible that a state's confidential information may be intercepted as it is being transmitted through cyber infrastructure located on the territory of another state. In addition, since the emergence of cloud computing (and indeed its now widespread use), many states may even store confidential information in a central server that is located in the territory of another state. In such situations, although a state may assert ownership over the information that has been intercepted, there is no territorial basis on which it can claim a violation of its territorial sovereignty. Indeed, if information owned by one state (say the UK) is transmitted through the cyber infrastructure located on the territory of another state (say the US), and during transmission it is intercepted by another state (say France), it may be that the state on whose territory the cyber infrastructure is physically located (in my example, the US) will assert a violation of its territorial sovereignty. In such circumstances the principle of territorial sovereignty offers the state that has authored and thus asserts ownership over the information (the UK) very little protection. It is here that the principle of non-intervention becomes important.

Although sovereignty exhibits a strong territorial dimension '[a] State's power reaches beyond its territory'[46] and, in the words of the ICJ, protects its 'political integrity'[47] more generally. The non-intervention principle therefore represents international law's attempt to protect a state's sovereign right to determine its internal and external affairs free from external intervention.

The principle of non-intervention is firmly enshrined in international law. It is incorporated within numerous international (regional and bilateral) treaties[48] and, independent of these treaties, through their practice states have evidenced a clear view that

46 Benedict Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace,' in *Peacetime Regime*, Ziolkowski, 196.

47 'Between independent States, respect for territorial sovereignty is an essential foundation of international relations', and international law requires political integrity also to be respected'; Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 202, citing its judgment in The Corfu Channel Case, 35.

48 For a discussion see Maziar Jamnejad and Michael Wood, 'The Principle of Non-Intervention,' *Leiden Journal of International Law* 22 (2009): 362 *et seq*.

external intervention in their internal and external affairs is prohibited by way of customary international law. Consider, for example, the 1970 UN General Assembly's Friendly Relations Declaration, where the participating states acted with the purpose of giving expression to principles of a legal character and specifically declared that states are under a duty 'not to intervene in matters within the domestic jurisdiction of any State'.[49]

In 1986, the ICJ reiterated that the principle of non-intervention is 'part and parcel of customary international law'.[50] Clarifying the scope of the non-intervention principle, the ICJ explained:

> 'A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.'[51]

On the basis of this often quoted paragraph, the principle of non-intervention is generally distilled into two constitutive elements.[52] In order for an unlawful intervention to occur it must be established that: 1) the act committed intervenes in a state's sovereign affairs; and 2) that the act is coercive in nature. The application of these two elements to acts of cyber espionage against information which is being stored on or transmitted through cyber infrastructure located within the territory of another state will now be considered.

4.1 Sovereignty over Information Located outside State Territory

First and foremost, in order to establish an unlawful intervention the act in question must have a bearing upon matters which, by virtue of the principle of state sovereignty, a state is entitled to decide freely. The purpose of this criterion is to assess whether the alleged intervention pertains to a matter that is permissibly regulated by states on the basis that it falls within their sovereign authority, or whether states have instead determined through international law that it is a matter that falls outside of the realm of state sovereignty.

In the context of the current discussion, the important question is whether states exercise sovereignty over information that they have authored and compiled but which is stored on or being transmitted through cyber infrastructure located on the territory of another state.

In the mid-1960s the US began sending satellites into outer space in order to collect intelligence relating to the activities of other states. The principle of territorial

49 United Nations, General Assembly resolution 25/2625, *2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations*, A/RES/25/2625 (24 October 1970), http://www.un-documents.net/a25r2625.htm.

50 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 202.

51 Ibid, para. 205.

52 Jamnejad and Wood, 'The Principle of Non-Intervention,' 347.

sovereignty was not relevant because the surveillance was committed from outer space and no physical infraction of the victim state's territory was committed.[53] When the US used its satellites to collect information relating to the activities of the Soviet Union, the Soviet Union insisted that its sovereignty had been interfered with. In the words of the Soviet representative to the UN:

> 'The object to which illegal surveillance is directed constitutes *a secret guarded by a sovereign state*, and regardless of the means by which such an operation is carried out, it is in all cases an intrusion into something guarded by a sovereign state in conformity with its sovereign prerogative.'[54]

The recent *East Timor v Australia* litigation before the ICJ is also instructive here. East Timor alleged that Australia had sent its agents into the office of an Australian lawyer acting as legal counsel for East Timor to collect confidential information relating to existing litigation between the two states. The office was physically located in Australia. East Timor applied to the ICJ for a provisional order that declared '[t]hat the seizure by Australia of the documents and data violated (i) the sovereignty of Timor-Leste and that 'Australia must immediately return to the nominated representative of Timor-Leste and all of the aforesaid documents and data, and to destroy beyond recovery every copy of such documents and data that is in Australia's possession or control'.[55]

In addressing these requests, the ICJ noted that '[a]t this stage of proceedings, the Court is not called upon to determine definitively whether the rights which Timor-Leste wishes to see protected exist; it need only decide whether the rights claimed by Timor-Leste on the merits, and for which it is seeking protection, are plausible'.[56] Importantly, the ICJ did consider East Timor's claim 'plausible'[57] and granted a provisional order that 'Australia [must] not interfere in any way in communications between Timor-Leste and its legal advisers',[58] indicating that this conclusion 'might be derived from the principle of the sovereign equality of States, which is one of the fundamental principles of the international legal order and is reflected in Article 2, paragraph 1, of the Charter of the United Nations'.[59]

This was a provisional order of the ICJ and the Court did not definitively pronounce on the international legality of Australia's conduct. But this does not mean that the ICJ's interpretation of international law is without significance. Instead, I contend that the ICJ's reasoning is important because it suggests that although the

53 Richard A. Falk, 'Space Espionage and World Order: A Consideration of the Samos-Midas Program,' in *Essays on Espionage*, Falk.
54 Soviet Union Statement to the United Nations First Committee, quoted in Joseph Soraghan, 'Reconnaissance Satellites: Legal Characterisation and Possible Utilisation for Peacekeeping,' *McGill Law Journal* 13 (1967): 470-471 [my emphasis]. Although for a different view see 'Legal Aspects of Reconnaissance in Airspace and Outer Space,' *Columbia Law Review* 61 (1961): 1095 ('Thus it would seem that there are at present no principles of international law that prohibit reconnaissance from outer space').
55 Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), 147 Reports of Judgments (International Court of Justice 2014), para. 2.
56 Ibid, para. 26.
57 Ibid, para. 28.
58 Ibid, para. 55.
59 Questions Relating to the Seizure and Detention, para 27.

appropriated information was physically located in the office of East Timor's legal advisor in Australia, it was nevertheless plausible that the information was clothed with East Timorese sovereignty and intervention with that information was precluded by international law.

By analogy, I would argue that where a state stores confidential information in servers located in another state or transmits such information through cyber infrastructure located in another state, that information represents 'a crucial dimension of national sovereignty that presupposes the nation state' and the right to have that information protected from intrusion flows from the general entitlement of states to have their political integrity respected, that is their sovereignty.[60] The argument that information is integral to a state's sovereignty is particularly convincing where the information that has been intercepted relates to the exercise of a state's public functions. With regard to information relating to a state's commercial transactions, the argument that such information is protected by state sovereignty is harder to sustain.[61]

In support of this approach, Article 5 of the UN Convention on Jurisdictional Immunities of States and Their Property provides that '[a] State enjoys immunity, in respect of itself and its property, from the jurisdiction of the courts of another State'.[62] Article 10 explains however that a state cannot invoke its immunity in relation to proceedings arising out of a 'commercial transaction'. Read together, these provisions indicate that a state's sovereignty extends to its property (providing this property is used for exclusively non-commercial purposes) even when this property is physically located in the territory of another state and, as such, is considered inviolable. In light of these provisions, and specifically in the context of electronic information that a state has authored but which is located outside of its territory, von Heinegg argues that it is a 'general principle of public international law according to which objects owned by a State or used by that State for exclusively non-commercial purposes are an integral part of the State's sovereignty and are subject to the exclusive jurisdiction of that State'.[63] The upshot is that data which belongs to a state but which is being stored on or transmitted through cyber infrastructure located on the territory of another state possesses 'national data sovereignty' and interference with that data (for the purpose of espionage, for example) can be regarded as an intrusion into state sovereignty.[64]

4.2 Coercion and Cyber Espionage

Once it has been concluded that there has been intervention in a matter that falls within a state's *sovereign affairs*, in order to establish an unlawful intervention it must then be determined that the intervention is coercive in nature.

60 Kristina Irion, 'Government Cloud Computing and National Data Sovereignty,' *Policy and Internet* 4 (2012): 42.
61 Vineeth Narayanan, 'Harnessing the Cloud: International Law Implications of Cloud-Computing,' *Chicago Journal of International Law* 12 (2012): 783.
62 United Nations, General Assembly resolution 59/38, *United Nations Convention on Jurisdictional Immunities of States and Their Property*, A/RES/59/38 (2 December 2004), http://legal.un.org/ilc/texts/instruments/english/conventions/4_1_2004_resolution.pdf.
63 Von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace,' 130.
64 Irion, 'Government Cloud Computing and National Data Sovereignty.'

The leading authority on the meaning of coercion is the *Nicaragua* judgement. In this case the ICJ defined coercion as acts interfering with 'decisions' and 'choices' of the victim state in relation to matters falling within its sovereignty. Following on from this decision there seems to be near consensus within academic literature that coercion requires the imposition of 'imperative pressure'[65] which manipulates the will of the state in order for the entity exercising coercion to realise certain objectives or, in Oppenheim's famous and often quoted formulation, intervention is 'dictatorial interference … in the affairs of another State for the purpose of maintaining or altering the actual condition of things'.[66] For Jamnejad and Wood, coercion is imposed where 'action is taken by one state to secure a change in the policies of another'.[67] In this sense, the dividing line between permissible influence and impermissible intervention in sovereign affairs is whether the act in question compels the state to act, or to abstain from acting, in a manner that it would not have voluntarily chosen.

This interpretation may be readily fulfilled in many cases of malicious cyber conduct. Take for example the Distributed Denial of Service Attacks against Estonia in 2007, a series of cyber attacks which impaired the Estonian government's capacity to freely communicate and interact with domestic and international actors.[68] However, an interpretation of coercion that requires the imposition of pressure yields important consequences for the application of the non-intervention principle to cyber espionage. This is because cyber espionage describes the practice of accessing and obtaining confidential information and, provided confidential information is accessed and obtained, cyber espionage is committed regardless of how that information is subsequently used.[69] Thus, in and by itself cyber espionage does not entail the imposition of pressure upon a state. Consequently, an interpretation of coercion that requires the imposition of pressure would mean that cyber espionage cannot be considered coercive and therefore does not violate the principle of non-intervention. For Ziolkowski:

> 'A forbidden intervention in domestic affairs requires an element of coercion by the other state. Scholars assert that illegal coercion implies massive influence, inducing the affected state to adopt a decision with regard to its policy or practice which it would not entertain as a free and sovereign state. It is clear that clandestine information gathering as such will not fulfil such requirements.'[70]

65 William Michael Reisman, *Nullity and Revision: The Review and Enforcement of International Judgments and Awards* (New Heaven: Yale University Press, 1971), 839-40.

66 Lassa Oppenheim and Hersch Lauterpacht, *International Law: A Treatise. Vol. I, Peace*, 8th edn (London: Longman, 1955), 305.

67 Jamnejad and Wood, 'The Principle of Non-Intervention,' 347-348.

68 For a discussion of the impact that the DDOS attacks had on Estonia see The North Atlantic Treaty Organization, *Six Colours: War in Cyberspace*, 2013, http://www.nato.int/ebookshop/video/six_colours/SixColours.html. On the application of international law to this event see Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' *Journal of Conflict and Security Law* 17 (2012): 211.

69 Where information obtained as a result of cyber espionage is subsequently used to exert influence over the victim state, a violation of the non-intervention is likely to occur. However, an examination of the international legality of this type of conduct falls outside of the scope of this chapter.

70 Ziolkowski, 'Peacetime Cyber Espionage,' 433. For a similar view see Terry Gill, 'Non-Intervention in the Cyber Context,' in *Peacetime Regime*, Ziolkowski, 224 ('the obtaining of information in itself falls short of coercive or dictatorial interference, and would not constitute 'intervention' in the legal sense').

I argue that this is a particularly narrow interpretation of the concept of coercion and which is undesirable as a matter of policy and incorrect as a matter of law. In normative terms this narrow interpretation is undesirable because, as I have already noted, the principle of sovereignty is a constitutional norm of international relations and, as such, requires robust protection. As we have seen, the principle of territorial sovereignty is defined broadly in order to provide watertight protection to the territorial dimension of state sovereignty – any intrusion into a state's sovereign territory is prohibited. The principle of non-intervention is also designed to protect a state's sovereignty, but this principle protects the metaphysical aspect of sovereignty (a state's political integrity) rather than its physical dimension (a state's territory). However, if a state's political integrity is protected only where the state is subject to imperative pressure (and especially 'massive influence'), then a state's political integrity is inadequately protected. In order to ensure that the depth and breadth of the legal principle of non-intervention accords with the depth and breadth of the constitutional norm of state sovereignty, I argue that conduct which compromises or undermines the authority of the state should be regarded as coercive.

This broader reading of the term coercion finds support within academic commentary. McDougal and Feliciano argue that a finding of coercion can be made whenever there is an attack against the 'value' of sovereignty.[71] My approach also chimes with Dickinson's claim that coercion is present if 'intervention cannot be terminated at the pleasure of the state that is subject to the intervention'.[72]

This expansive understanding of coercion also finds support in state practice and the practice of international organisations, notably the UN General Assembly. The 1965 UN Declaration on the Inadmissibility of Intervention and the 1970 Friendly Relations Declaration employ identical language in articulating the scope of the non-intervention principle, explaining that no state has 'the right to intervene, directly or indirectly, for any reason whatever, in sovereignty of any other State' or use 'any … measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights'. As is apparent, in these Declarations the principle of non-intervention is formulated in particularly broad terms and they seem intended to encourage an expansive reading of the prohibition against intervention: 'for whatever reason'; 'any measures'; 'to obtain from it the subordination of the exercise of its sovereign rights'.

Additional support for this broader reading of the non-intervention principle is evident from the reaction of the Soviet Union to the US's exploitation of outer space for purpose of unauthorised surveillance in the 1960s, discussed above. Even in the absence of a violation of its territorial sovereignty the Soviet Union asserted that the US's conduct constituted a violation of its political integrity and in making this

71 Myres Smith McDougal and Florentino P. Feliciano, 'International Coercion and World Public Order: The General Principles of the Law of War,' *The Yale Law Journal* 67 (1958): 782.

72 Edwin De Witt Dickinson, *The Equality of States in International Law* (Cambridge, Mass.: Harvard University Press, 1920), 260.

determination explained that 'in all cases an intrusion into something guarded by a sovereign state in conformity with its sovereign prerogative' is unlawful.[73]

Further support for this expansive interpretation of the concept of coercion is found in the recent *East Timor v Australia* litigation. In this case the ICJ granted a provisional order on the basis that it was plausible that Australia's interception of information belonging to East Timor but located on Australian territory constituted a violation of East Timor's sovereignty; namely, a prohibited intervention. Importantly, it was the *impact* of Australia's conduct on East Timor's sovereignty that implied a violation of international law, independent of any attempt by Australia to subsequently use that appropriated information to compel East Timor into acting in one way or another.

The most sustained judicial consideration of the non-intervention principle is the ICJ's judgment in *Nicaragua* and this decision contends that coercion is present only where a state's decision making capacity is affected. However, it is important not to overstate the significance of the ICJ's interpretation of the non-intervention principle. As the ICJ questioned in this case, 'what is the exact content of the [non-intervention] principle so accepted'?[74] In addressing this question the ICJ specifically noted that 'the Court will define only those aspects of the principle which appear to be relevant to the resolution of the dispute'.[75] This is important because the ICJ explained that the specific non-use of force prohibition can be considered an aspect of the general non-intervention principle (the ICJ noted that intervention is 'particularly obvious in the case of intervention which uses force')[76] and the ICJ's immediate focus in this case was the prohibition against the use of force. After noting that Nicaragua's complaints against the US related mainly to its military activities, the ICJ explained that 'it is primarily acts of intervention of this kind with which the Court is concerned in the present case'.[77] Consequently, the ICJ's decision in *Nicaragua* can be read as providing an inchoate or even unfinished delineation of the non-intervention principle and if this is correct then this decision is of little relevance to determining whether conduct not involving the use of force (such as cyber espionage) offends the prohibition against intervention.

All in all, I argue that there is no requirement that influence (let alone massive influence) be imposed upon a state to pursue a particular course of action, or indeed to abstain from one, in order to constitute coercion and thus fall foul of the non-intervention principle. Instead, the key issue is whether the conduct in question compromises or undermines the authority structures of the state, that is, state sovereignty. With reference to cyber espionage, I have already demonstrated that states exercise 'national data sovereignty' over information that they have authored and compiled, even when it is physically located on the cyber infrastructure of another state. In light

73 Soviet Statement in the United Nations First Committee, quoted in Soraghan, 'Reconnaissance Satellites,' 470-471.
74 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 205.
75 Ibid.
76 Ibid.
77 Ibid.

of this, where such data is accessed and appropriated the sovereign authority of the state is compromised and the conduct in question can be regarded as coercive.

Some may express concern that this interpretation of the concept of coercion is overly broad and casts the scope of the non-intervention principle far too widely. In particular, the concern may be that such an expansive interpretation would essentially confer on states an international legal entitlement to operate unaffected by the conduct and activities of other states. Clearly, such an approach does not accord with international reality. Given the pressures of globalisation, and in light of the intensity of state interactions in contemporary international relations, it is clear that a reading of the non-intervention principle which more or less precludes intensive state interactions on the basis that this results in their sovereignty being undermined is incorrect as a matter of international law. To put the same matter differently, states are constantly interacting in order to pursue and realise their particular interests and such interactions frequently result in the sovereignty of other states being undermined, yet states rarely denounce each and every act that impacts upon their sovereignty as unlawful intervention.

In this regard it needs to be remembered that the application of the non-intervention prohibition is subject to the principle of *de minimis non curat lex* – which is generally translated from Latin as *the law does not concern itself with trifles*. The effect of the *de minimis* doctrine is to place 'outside the scope of legal relief the sorts of intangible injuries, normally small and invariably difficult to measure, that must be accepted as the price of living in society'.[78] Thus, this maxim signifies 'that mere trifles and technicalities must yield to practical common sense and substantial justice' so as 'to prevent expensive and mischievous litigation, which can result in no real benefit to the complainant, but which may occasion delay and injury to other suitors'.[79]

Although often described as a maxim, this principle does impose a recognised legal restriction on the operation of the non-intervention principle.[80] McDougal and Feliciano suggest that determining coercion should account for 'consequentiality'.[81] They suggest 'the importance and number of values affected, the extent to which such values are affected, and the number of participants whose values are so affected'.[82] In the context of cyber, Watts argues that when applying the *de minimis* threshold to the non-intervention principle our understanding of the term coercion should include a consideration of 'the nature of State interests affected by a cyber operation, the scale of the effects the operation produces in the target State, and the reach in terms of number of actors affected'.[83] After taking such considerations into account, acts which have an insignificant impact upon the authority structures of a sovereign state (those

78 Jeff Nemerofsky, 'What is a "Trifle" Anyway?' *Gonzaga Law Review* 37 (2001-2002): 323.
79 Ibid.
80 Robert Jennings and Adam Watts, eds., *Oppenheim's International Law* (Longman, 1996) 385 *et seq*; Rosalyn Higgins, 'Intervention and International Law,' in *Intervention in World Politics*, ed. Hedley Bull (Clarendon Press, 1984), 30; Watts, 'Low-Intensity Cyber Operations,' 138.
81 McDougal and Feliciano, 'International Coercion and World Public Order: The General Principles of the Law of War,' 782.
82 Ibid.
83 Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention,' 146.

that cause mere irritation or inconvenience) do not warrant the application of international law and thus do not violate the non-intervention principle.

With regard to cyber espionage specifically, much will depend upon the facts of the case in question, and in particular the extent to which the cyber espionage compromises the sovereign authority of the state. Primarily, this will require an assessment of the scale of the cyber espionage under examination and an analysis of the nature of the information that has been appropriated. For the purpose of illustration, it can perhaps be contended that whilst the systematic accessing of information belonging to senior state officials (such as the Head of State) is likely to exceed the *de minimis* threshold, the one-off accessing of innocuous electronic correspondence of a low-ranking civil servant is unlikely to be considered sufficiently serious to justify the engagement of international law.

5. Is There a Customary Defence of Cyber Espionage?

In the context of espionage a frequently made argument is that even if espionage does constitute a *prima facie* violation of the principle of territorial sovereignty or the non-intervention principle, state practice has established a customary international law that modifies the scope of the these principles. In other words, state practice has given rise to a permissive rule of customary international law that regards espionage as a legally recognised exception to the principles of territorial sovereignty and non-intervention. In the words of Smith:

> 'Because espionage is such a fixture of international affairs, it is fair to say that the practice of states recognises espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law.'[84]

The claim that is frequently advanced is that, if espionage is permissible under customary international law, espionage committed through cyberspace must also be permissible.[85] Several important observations need to be considered here.

Customary international law emerges on the basis of 'general practice accepted as law'.[86] There are thus two elements of customary international law.[87] First, state

84 Jeffrey H. Smith, 'State Intelligence Gathering and International Law: Keynote Address,' *Michigan Journal of International Law* 28 (2007): 544. Similarly, see Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence Operations and International Law,' *Michigan Journal of International Law* 28 (2007): 628 ('[s]tate practice throughout history … supports the legitimacy of spying. Nowhere in international law is peaceful espionage prohibited').

85 Gary Brown and Keira Poellet, 'The Customary International Law of Cyberspace,' *Strategic Studies Quarterly* 6 (2012): 133; Fidler, 'Economic Cyber Espionage.'

86 United Nations, *Statute of the International Court of Justice*, Article 38(1)(b).

87 '[F]or a new customary rule to be formed, not only must the acts concerned amount to a settled practice, but they must be accompanied by the *opinio juris sive necessitatis*'; Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 207.

practice; and second, the requirement that this practice is accompanied by a belief that it is permitted under international law (*opinio juris*). The burden is on those asserting the existence of customary rule to demonstrate that these two criteria are met.

In relation to state practice, in the *North Sea Continental Shelf Cases* the ICJ explained that in order to find that a customary rule has emerged there must be 'extensive and virtually uniform' state practice in favour of that rule.[88] Although this does not require universal acceptance of that rule by states within the international community or even that those states which practice the rule do so with strict conformity,[89] this is nevertheless an extremely high threshold. This notwithstanding, those advocating the existence of a customary rule permitting espionage confidently assert that most states most of the time collect confidential intelligence without authorisation from other states (that is, they commit espionage) and thus this stringent threshold is attained.

However, in order to qualify as state practice it must be conducted publically and openly and state practice committed in secret is irrelevant to the formation of customary international law.[90] In relation to state practice committed in secret, the International Law Commission's Second Report on the Identification of Customary International Law explains that '[i]t is difficult to see how [such] practice can contribute to the formation or identification of general customary international law'.[91] The requirement that state practice be committed publically and openly is important because states must be given the opportunity 'to respond to it positively or negatively', so that they can either make the decision to adopt the rule, and thus further contribute to its formation, or instead reject it and attempt to frustrate its crystallisation;[92] or, if it appears that a state is isolated in its rejection of the rule, it can identify itself as a persistent objector to that rule. Patently, this process cannot occur where state practice is committed in secret. Furthermore, it seems inherent to the notion of the rule of law that binding rules are public in character and it is for this reason that the UN Charter forbids the use of secret treaties.[93]

Almost by definition, espionage is a practice conducted in secret. As a result, regardless of how frequently states engage in espionage, where this practice is engaged in covertly and secretly it cannot be classified as state practice for the purpose of customary law formation. In the context of espionage, the International Law Association's Committee on the Formation of Customary International Law

88 North Sea Continental Shelf Cases (Federal Republic of Germany/Denmark v. Federal Republic of Germany/Netherlands) 4 Reports of Judgments (International Court of Justice 1969), para. 74.

89 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 186.

90 United Nations, General Assembly, International Law Commissions, *Second Report on the Identification of Customary International Law*, A/CN.4/672, para. 47 (22 May 2014), http://legal.un.org/ilc/documentation/english/a_cn4_672.pdf.

91 Ibid.

92 'Another condition for State conduct – if it is to count in assessing the formation of custom – is that it must be transparent, so as to enable other States to respond to it positively or negatively'; Yoram Dinstein, 'The Interaction between Customary Law and Treaties,' *Recueil des Cours Recueil des cours* 322 (2006): 275.

93 United Nations, *Charter of the United Nations*, Article 102.

explains that 'a secret physical act (e.g. secretly 'bugging' diplomatic premises) is probably not an example of the objective element [of state practice]'.[94]

It is correct that in more recent times some states have been prepared to acknowledge *prospectively* that their security services engage in covert operations for the purpose of intelligence-gathering. For example, the Mission Statement of the US Central Intelligence Agency (CIA) explains that one of its objectives is to '[p] reempt threats and further US national security objectives by collecting intelligence that matters, producing objective all-source analysis, conducting effective covert action as directed by the President, and safeguarding the secrets that help keep our Nation safe'.[95] It is well accepted that verbal acts such as these can constitute state practice for the purpose of customary law formation.[96] Fundamentally, however, it must be remembered that customary international law forms on the basis of specific 'instances of State conduct'[97] that form 'a web of precedents'[98] from which an observable pattern is identifiable. Notwithstanding the broad public statements of the CIA relating to covert intelligence-gathering, it nevertheless remains that specific instances of espionage are committed in secret and to accept such conduct as evidence of state practice is at odds with the basic tenet of customary international law that state practice is 'material and detectable'.[99]

Even if we momentarily concede that there is sufficient evidence of state practice of espionage to satisfy the first limb of the customary international law test, in order for custom to form this practice must be accompanied by *opinio juris*; state practice alone, regardless of how widespread and systematic it is, is insufficient. The requirement is that when participating in a particular practice states must assert the international legality of their conduct or, at the very least, when the international legality of their conduct is challenged subsequent to its practice it can be defended on the basis that it is permissible under international law. This is hugely problematic in the context of espionage because when practising this type of activity states do not generally express the belief that it is permissible under international law. Furthermore, when challenged about their espionage activities, states overwhelmingly refuse to admit responsibility for this conduct, let alone attempt to justify it as permissible under international law. In the wake of the Snowden revelations President Obama did attempt to defend the NSA's conduct, but crucially he consistently defended the conduct on the basis that it was necessary to maintain 'national security'.[100] Conspic-

94 'Final Report of the Committee: Statement of Principles Applicable to the Formation of General Customary International Law' (Final Report of the Committee, International Law Association, London conference, 2000), 15.

95 Central Intelligence Agency, 'CIA Vision, Mission, Ethos & Challenges,' https://www.cia.gov/about-cia/cia-vision-mission-values.

96 United Nations, General Assembly, International Law Commissions, *Second Report on the Identification*, para. 37.

97 Case Concerning Military and Paramilitary Activities in and against Nicaragua, para. 184.

98 Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain), 3 Reports of Judgments (International Court of Justice 1970), para. 39 (Separate Opinion of Judge Ammoun).

99 François Gény, 'Méthode d´interprétation et sources en droit privé positif,' *A. Chevalier-Marescq* 1 (1899): section 110, quoted in Anthony A. D´Amato, *The Concept of Custom in International Law* (Ithaca N.Y. and London: Cornell University Press, 1971), 49.

100 The White House, Office of the Press Secretary, *Remarks by the President on Review of Signals Intelligence*, 17 January 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

uously absent from President Obama's defence was that the conduct was permissible under *international law*, and the requirement of *opinio juris* is only satisfied where the conduct in question is justified as acceptable under international law.

It would therefore appear that state practice of espionage 'is accompanied not by a sense of right but by a sense of wrong'[101] and so 'state practice and *opinio juris* appear to run in opposite directions'.[102]

A further point is relevant here. When states discover that they are the victims of espionage they often protest (and often vociferously) that such conduct is contrary to international law. When a customary rule is in the process of formation and a number of states of the international community object to that rule on the basis that it is incompatible with international law, it becomes particularly difficult to sustain the claim that a customary rule has formed – in essence, a common *opinio juris* forms agitating against the emergence of a customary rule.[103] This point is particularly relevant in relation to cyber espionage. If we look at the international reaction to the Snowden revelations we see a cohort of states asserting that the NSA's practice of cyber espionage was incompatible with international law. As we have already seen, Germany and Brazil in particular objected to the NSA's cyber espionage and in doing so clearly employed the language of international law; indeed, Brazil advocated its international law objections before the UN General Assembly.

The events surrounding Sony in late 2014 are also illustrative. As is well known, Sony intended to release a film entitled *The Interview* which depicted the assassination of the leader of North Korea. Days before its release Sony's computer networks were accessed without authorisation and malware was introduced which wiped a substantial amount of confidential information. In addition, certain confidential information was exfiltrated and published on the Internet, including sensitive email correspondence between the company and its employees (well-known actors) and storylines for forthcoming films.[104]

The US Federal Bureau of Investigation (FBI) determined that North Korea was responsible for this malicious cyber conduct.[105] Although the US did not specify on what basis this conduct constituted a violation of international law, the US explained that it would 'respond proportionally and in a space, time and manner that we choose'.[106] Indeed, on 2 January 2015 the US imposed economic sanctions against North Korea, including freezing its assets in the US.[107] As we know, under international law a state that is subject to an internationally wrongful act is entitled

101 Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs,' 17.
102 Simon Chesterman, 'The Spy Who Came in from the Cold: Intelligence and International Law,' *Michigan Journal of International Law* 27 (2006): 1072.
103 Frederic L. Kirgis, Jr., 'Custom on a Sliding Scale,' *American Journal of International Law* 81 (1987): 146.
104 For an overview of the events see 'The Interview: A Guide to the Cyber Attack on Hollywood,' *BBC News*, December 29, 2014, http://www.bbc.co.uk/news/entertainment-arts-30512032.
105 'Sony Hack: Obama Vows Response as FBI Blames North Korea,' *BBC News*, December 19, 2014, http://www.bbc.co.uk/news/world-us-canada-30555997.
106 Ibid.
107 Dan Roberts, 'Obama Imposes New Sanctions against North Korea in Response to Sony Hack,' *The Guardian*, January 2, 2015, http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview.

(subject to caveats) to adopt proportionate countermeasures in order to compel the wrongdoing state to discontinue its internationally wrongful conduct and make appropriate reparations. The only implication, then, is that the US regarded this malicious cyber conduct as incompatible with international law.

For the purpose of this article, which discusses the international legality of cyber espionage, we must approach cautiously the US's determination that this cyber conduct was unlawful under international law. This is because when determining that the malicious cyber conduct was unlawful the US seemed to refer to the incident as a whole and not specifically to those aspects of the malicious cyber conduct that constituted cyber espionage. It is therefore unclear as to whether the US's protest was in relation to the hacking of cyber infrastructure located on its territory, the emplacement of malware that erased data located on cyber infrastructure located on its territory, or the exfiltration of confidential data located on cyber infrastructure located on its territory, or all three. However, given that the cyber espionage dimension of the incident was by far the most pronounced, a reasonable reading of the US's reaction to the Sony incident is that it regarded such conduct as incompatible with international law. If this reading is correct, it would lend further support to the argument that 'there is little doctrinal support for a 'customary' defence of peacetime espionage in international law'.[108]

6. Conclusion

This chapter does not deny the importance of intelligence-gathering in the contemporary world order. However, one must distinguish between intelligence-gathering from publically available sources and intelligence-gathering from private, unauthorised sources, namely espionage. 'Intelligence gathering that relies upon open source information is legally unproblematic'.[109] One must also distinguish between authorised and unauthorised intelligence-gathering. Intelligence that is gathered pursuant to a treaty regime or Chapter VII Security Council Resolution, for example, can be regarded as authorised, and for this reason is not properly regarded as espionage. This chapter has examined the international legality of transboundary state-sponsored cyber espionage and has argued that cyber espionage constitutes a violation of the territorial sovereignty of a state where information is accessed that is resident on computer networks that are supported by cyber infrastructure located on that state's territory. I have identified recent state practice which supports this conclusion. I have also argued that cyber espionage violates the principle of

108 Craig Forcese, 'Spies Without Borders: International Law and Intelligence Collection,' *Journal of National Security Law and Policy* 5 (2011): 203.

109 Chesterman, 'The Spy Who Came in from the Cold: Intelligence and International Law,' 1073.

non-intervention where it has a more than insignificant impact on the authority structures of a state. The utility of the non-intervention principle is particularly apparent in relation to information that belongs to a state but is located on cyber infrastructure in the territory of another state. Finally, I have argued that customary international law develops on the basis of transparent, publically observable state conduct that is committed in the belief that it is permissible under international law. As espionage is a practice that is by definition committed in secret, and where states overwhelmingly refuse to admit responsibility for such conduct let alone justify it as acceptable under international law, I have concluded that there is no customary 'espionage exception' to the principles of territorial sovereignty and non-intervention.