8. Cyber espionage and international law

Russell Buchan

1. INTRODUCTION

Cyberspace has emerged as an indispensable feature of the contemporary era. All actors within the international system now utilise cyberspace in order to perform their manifold activities and maximise their potential. Although it goes without saying that this highly interconnected and instantaneous environment yields enormous benefits, cyberspace has also become the source of significant threats and vulnerabilities.[1]

The threat landscape is multifaceted and dynamic. In recent years however the exploitation of cyberspace for the purpose of espionage has emerged as a particular concern.[2] According to reports, 'cyber espionage projects [are] now prevalent'.[3] Indeed, there are numerous examples of both State and non-State actors infiltrating computer networks of State and non-State actors in order to access and collect confidential information.[4] Several high profile instances of cyber espionage have attracted international attention. In January 2010 Google reported that it had 'detected a highly sophisticated and targeted attack against our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google'.[5] Internal investigations revealed that 'a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists'.[6]

[1] In the words of US President Barack Obama, '[t]hreats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies'; White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure* (2009), <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf> accessed 7 October 2014.

[2] '[D]igital espionage and cyber crime remain the biggest threats to both government and the business community'; National Cyber Security Centre, *Cyber Security Assessment Netherlands* (CSAN) (2013) 7, <http://english.nctv.nl/publications-products/Cyber_Security_Assessment_Netherlands/> accessed 7 October 2014.

[3] *The Guardian*, 'State-sponsored cyber espionage projects now prevalent' (30 August 2012) <http://www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent> accessed 7 October 2014.

[4] Mandiant Report, 'APT1: Exposing one of China's Cyber Espionage Units' (2013) <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf> accessed 7 October 2014.

[5] D Drummond, 'A New Approach to China'(12 January 2010) Google: Official Blog, <http://googleblog.blogspot.co.uk/2010/01/new-approach-to-china.html> accessed 7 October 2014.

[6] *Ibid*. Note that China has denied responsibility for these allegations; Ma Zhaoxu, Foreign Ministry Spokesperson, *Remarks on China-related Speech by US Secretary of State on 'Internet Freedom'* (22 January 2010), <http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t653351.shtml> accessed 7 October 2014.

In another significant incident of cyber espionage in May 2012 the Russian security firm Kaspersky Lab detected computer malware (subsequently referred to as the Flame virus) in computer systems of Iranian Oil Companies which allowed confidential information to be accessed, monitored and collected. According to reports, this virus had the capacity to 'activate computer microphones and cameras, log keyboard strokes, take screen shots, extract geolocation from images, and send and receive commands and data through Bluetooth wireless technology';[7] 'basically an industrial vacuum cleaner for sensitive information'.[8] Although definitive attribution has never been made, it has been alleged that the US and Israel were the authors of this virus and responsible for its deployment.[9]

The publication of the Mandiant Report in February 2013 exposed for the first time the scale and intensity of cyber espionage in the international community.[10] This report in particular identified China as a persistent perpetrator of cyber espionage. In fact, the report claimed 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 Mandiant Report suggested that Unit 61398 was responsible for organising and instigating a massive cyber espionage campaign against other States and non-State actors, looking 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 four 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 companies including *The Guardian* newspaper and *The Washington Post*. The documents revealed that the NSA had been engaged in a global surveillance programme. At the heart of this surveillance programme was the collection of confidential information that was being stored in or transmitted through cyberspace. In particular, the NSA had been engaged in a sustained and widespread campaign of intercepting and monitoring private email and telephone communications. This cyber espionage targeted numerous 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 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 involved in international terrorism.[11]

---

[7] *The Washington Post*, 'U.S., Israel developed Flame Computer Virus to slow Iranian Nuclear efforts, Officials say' (19 June 2012), <http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html> accessed 7 October 2014.

[8] *BBC News*, 'Flame: Massive cyber attack discovered, researchers say' (28 May 2012), <http://www.bbc.co.uk/news/technology-18238326> accessed 7 October 2014.

[9] *The Washington Post* (n 7).

[10] Mandiant Report (n 4).

[11] For an overview of the Snowden revelations see *The Guardian*, 'The Snowden Files – Inside the surveillance state' (2 December 2013) <http://www.theguardian.com/technology/2013/dec/03/tim-berners-lee-spies-cracking-encryption-web-snowden> accessed 7 October 2014.

These incidents raise important questions concerning the legality of cyber espionage under international law generally and the adequacy of international law in protecting State and non-State actors from cyber espionage in particular. To date, these important international legal questions have received inadequate attention in the literature. This chapter will therefore attempt to provide answers to some of these legal questions. This chapter will be structured accordingly. Section 2 formulates a working definition of the concept of cyber espionage in order to focus the research scope of the chapter. Section 3 examines the role and nature of the practice of cyber espionage in the contemporary international order. In particular, this section presents cyber espionage as a pernicious practice that represents a threat to international peace and security and which is thus in need of international regulation. In light of this, section 4 identifies the international law implicated by cyber espionage and assesses the extent to which it regulates this practice. Section 5 offers some conclusions.

2. DEFINING CYBER ESPIONAGE

Although cyber espionage is a relatively new phenomenon, espionage is certainly not. In fact, espionage has been practised 'since the dawn of human history'.[12] In its traditional conception espionage describes the practice whereby agents are physically dispatched into the territory of another State in order to access and obtain confidential information. States have however exploited developments in innovation and technology so as to devise more effective methods through which to conduct espionage. With the discovery of ships, aeroplanes and celestial bodies the sea, the skies and outer space have all emerged as domains that can be exploited as platforms through which to commit espionage. It therefore comes as no surprise that since its creation cyberspace has also been harnessed as a tool through which to commit espionage.

Espionage is defined as 'the consciously deceitful collection of information, ordered by a government or organization hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the colleting'.[13] In order to fit the theme of this handbook this chapter is concerned with *cyber* espionage. According to the US Presidential Policy Directive entitled 'U.S. Cyber Operations Policy', 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 …'[14] Several important features of this definition

[12] Katharina Ziolkowski, 'Peacetime cyber espionage – new tendencies in public international law', in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (CCDCOE, 2013) 425.

[13] Geoffrey B. Demarest, 'Espionage in international law' (1996) 24 *Denv. J. Int'l. L. & Pol.* 321, 326.

[14] US Presidential Policy Directive, 'U.S. Cyber Operations Policy' (October 2012) <http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf> accessed 7 October 2014. Similarly, Lin defines cyber espionage as 'the use of actions and operations – perhaps over an extended period of time – to obtain information that would otherwise be kept confidential and is resident on or

need to be identified and elaborated upon in order to provide some much needed clarification to the practice of cyber espionage and, further, to refine the focus of this chapter.

1. This chapter examines the legality of espionage committed in or through cyberspace. In this context cyberspace refers to a 'global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[15]
2. As with espionage, cyber espionage describes the unauthorised accessing and copying of confidential information. Cyber espionage however relates to the accessing and copying of electronic information that is being stored in or transmitted through cyberspace. Note that cyber espionage requires more than just gaining access to a computer system; electronic information must also be copied.[16] In many instances the accessing and copying of information occurs contemporaneously. However, the copying of information is expressly required in order to distinguish cyber espionage from mere hacking, which describes the practice of accessing computer systems and networks but does not necessarily entail the copying of information.[17] Further note that cyber espionage is committed regardless of whether information is lost or damaged. In order for cyber espionage to be committed all that is required is that confidential information is accessed and copied. Indeed, the victim may never know that they have been the victim of this activity, and this is usually when cyber espionage is at its most effective.
3. The objective of this chapter is to assess the permissibility under international law of *transboundary* cyber espionage. This chapter does not therefore consider the legality of cyber espionage committed by nationals against their own government. This would be an interesting research project, especially in light of the recent conviction of Chelsea Manning under the Espionage Act in the US and the potential trial of Edward Snowden under the same legal framework. However, such a project would be an examination of *national* legal rules relating to cyber espionage. But the issue is that because of the interconnectivity of cyberspace cyber espionage can be committed remotely by actors physically located in foreign jurisdictions. Certainly, transboundary cyber espionage can violate the national (criminal) laws of a State. In May 2014 the US again invoked the

---

transmitting through an adversary's computer systems or networks'; Herbert Lin, 'Offensive cyber operations and the use of force' (2010) 4 *J. Nat'l. Sec. L. & Pol.* 63, 63.

[15] Joint Chiefs of Staff, Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms* (8 November 2010) (as amended through 15 June 2014) 64. The International Telecommunications Union (ITU) describes cyberspace as 'systems and services connected either directly or indirectly to the internet, telecommunications and computer networks'; ITU, *ITU National Strategy Guide* (Geneva: ITU, 2011) 5, <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf> accessed 7 October 2014.

[16] Ziolkowski (n 12) 429.

[17] Whether hacking (as distinguished from cyber espionage) is contrary to international law is beyond the scope of this chapter.

Espionage Act when a Grand Jury indicted five Chinese military officers, allegedly acting at the behest of the Chinese Government, accusing them of committing cyber espionage in order to obtain important trade secrets from US companies.[18] However, the enforcement of national criminal laws against perpetrators that are located in foreign jurisdictions is likely to be extremely difficult, and so national law will often prove ineffective.[19] Ultimately, protection against transboundary cyber espionage will therefore rest with international law. It is for this reason that the focus of this chapter is upon the application and effectiveness of *international* law.

4. Cyber espionage, like espionage, can be committed during times of peace or times of armed conflict. As we shall see, there is no specific conventional or customary international legal framework that regulates peacetime espionage. In contrast espionage committed during times of armed conflict, and where this espionage is committed in support of one of the parties to the armed conflict, is specifically regulated by international humanitarian law, notably Article 46 of Additional Protocol 1 (1977) to the Geneva Conventions (1949). Due to space restrictions, and in light of the recent topicality of peacetime cyber espionage, this chapter will focus exclusively upon the permissibility under international law of cyber espionage committed during peacetime.
5. Various treaties and in particular arms controls treaties permit States to engage in surveillance and monitoring of other State parties so as to assure and verify their compliance with the obligations imposed by the treaty. The accessing and copying of confidential information that is committed *consensually* pursuant to a treaty does not constitute cyber espionage (as defined in this chapter) and does not raise any international legal concerns, providing of course it is committed within the parameters stipulated by the treaty. The focus of this chapter is to examine the international legality of cyber espionage, which by definition requires the *unauthorised* exploitation of cyberspace in order to access and copy confidential information.[20]
6. Historically, espionage was an activity that was practised by States, against States, usually targeting important organs of the State such as those relating to defence and foreign affairs. Significantly, however, and as exemplified by the Snowden

---

[18] *The Guardian*, 'Chinese military officials charged with stealing US data as tensions escalate' (20 May 2014) <http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage> accessed 7 October 2014.

[19] In relation to the indictment of the five Chinese military officials under the Espionage Act, Fidler explains that '[t]he U.S. government knows the likelihood of successfully prosecuting these individuals for violating U.S. criminal law is virtually nil because the cooperation of the Chinese government would be necessary for the U.S. to gain custody and conduct a criminal trial'; David Fidler, 'Cyber espionage indictment of Chinese officials: IU experts comment' (19 May 2014) <http://info.law.indiana.edu/releases/iu/2014/05/china-cyber-spying.shtml> accessed 7 October 2014.

[20] Similarly, the accessing and copying of confidential information pursuant to a resolution adopted by the Security Council under Chapter VII UN Charter does not constitute cyber espionage because it is conducted with legal authority. Such conduct cannot be therefore regarded as unauthorised.

revelations, a combination of the widespread use of cyberspace to store information and an increasingly interdependent and competitive international environment has meant that States are also now committing cyber espionage against non-State actors such as international organisations, non-governmental organisations, companies and even individuals.[21] Moreover, it is not just States that commit cyber espionage. Non-State actors such as companies and individuals have also recognised the benefits of copying confidential information belonging to State and non-State actors, and have thus exhibited a tendency to exploit cyberspace for the purpose of espionage.[22]

The participation of this multitude of different actors in the practice of cyber espionage raises many interesting and complex international legal questions. In relation to cyber espionage committed by States, relevant international law questions include

- Does cyber espionage violate the principle of non-intervention that is contained in customary international law?
- Does cyber espionage constitute an unlawful use of force under Article 2(4) UN Charter or an armed attack under Article 51 UN Charter?
- Does cyber espionage constitute a violation of international human rights law, in particular the right to privacy?

As I have noted, cyber espionage is also committed by non-State actors. As we know, international law was originally devised in order to regulate inter-State relations, and to this day retains a predominantly State-centric focus.[23] This being said, given the increasing importance of non-State actors on the international stage international law has gradually developed the capacity to regulate the activities of non-State actors, even if this is achieved indirectly by holding States responsible for their behaviour. In the context of cyber espionage committed by non-State actors relevant international law questions include

- Under what circumstances can acts of cyber espionage by non-State actors be legally attributed to a State?
- Are States under a duty of due diligence to prevent non-State actors operating in their territory or subject to their jurisdiction from committing acts that are injurious to the legal rights of other States?

---

[21] *BBC News*, 'Ordinary internet users 'made up bulk of NSA intercepts' (6 July 2014) <http://www.bbc.co.uk/news/world-us-canada-28182494> accessed 7 October 2014.

[22] 'A growing array of state and non-state adversaries are increasingly targeting – for exploitation and potentially disruption or destruction – our information infrastructure including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical infrastructure'; Director of National Intelligence Dennis C. Blair, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee*, Statement for the Record (February 2009) 39-40.

[23] Jean d'Aspremont, 'Introduction' in Jean d'Aspremont (ed.), *Participants in the International Legal System: Multiple Perspectives on Non-State Actors in International Law* (Routledge, 2011).

- Does the World Trade Organisation (WTO) or International Telecommunications Union (ITU) impose legal obligations upon States to ensure that companies registered within their jurisdiction respect trade secrets of companies registered in other States?

Due to space restrictions this chapter cannot address all of these questions. For this reason, this chapter does not assess the role of international law in regulating cyber espionage committed by non-State actors. Instead, this chapter assesses the legality under international law of cyber espionage committed by *States*. To be clear, this entails an examination of whether cyber espionage constitutes a violation of the non-intervention principle contained in customary international law or an unlawful use of force or armed attack under the UN Charter. Note that this chapter does not consider whether cyber espionage committed by States against individuals violates international human rights law. This question is examined in detail elsewhere in this handbook.[24]

3. CYBER ESPIONAGE AS A THREAT TO INTERNATIONAL PEACE AND SECURITY

Espionage is often defended on the basis that it serves an important function in facilitating the maintenance of international peace and security.[25] Historically, this defence has been rooted in classic realist theory; the argument runs that States exist in a State of nature because the world order does not possess an overarching government that is capable of protecting State security. In the absence of protection from a centralised authority, States must assume responsibility for their own survival in the system. What this means in practice is that States must acquire sufficient material power, or at least ally with other States in order to bolster and enhance their material strength, so as to deter potential aggressors and, if necessary, repel them.[26] All in all, international peace and security is maintained where a balance of power is achieved between States.[27]

Being able to accurately determine the relative strength of other States is therefore crucial to achieving a balance of power. In this competitive security environment, however, States are reluctant to accept as truthful claims by other States relating to their material capabilities and, moreover, what their intentions are in relation to how those capabilities will be used. Scholars argue that espionage allows States to access confidential information about other States and thus better understand their exact capabilities and intentions. In short, espionage enables States to know each other better. The consequence is that States are able to take steps to more accurately balance their

[24] See Fidler (Ch 5 of this book).

[25] See generally Michael Herman, *Intelligence Power in Peace and War* (CUP, 1996).

[26] See generally Kenneth Waltz, *Theory of International Relations* (Addison-Wesley Pub. Co. 1979).

[27] '[W]ars usually begin when two nations disagree on their relative strength, and wars usually cease when the fighting nations agree on their relative strength'; Geoffrey Blainey, *The Causes of War* (New York: The Free Press, 1988) 293.

material power with other States in the system. In this sense, espionage becomes crucial to the maintenance of international peace and security.[28] In the words of one scholar, '[e]spionage is regarded by States as a necessary tool for pursuing their foreign policy and security interests and for maintaining the balance of power at the inter-State level. Thus, it has always been a common practice in international relations, even in time of peace'.[29]

I reject this realist defence of espionage. Its weakness is that it fails to appreciate that since at least the inception of the UN Charter in 1945 international relations have been predicated upon the principle of the sovereign equality of States.[30] Indeed, such is the importance of this principle that it is often considered to be a constitutional norm of the international community.[31] The 'corollary' of this principle is that States are legally precluded from intervening in each other's internal affairs.[32] The objective is to protect State sovereignty by creating an international covenant of universal applicability that legally compels States to abstain from intervening in each other's internal affairs. In this environment international peace and security is maintained through legal regulation, not the balance of power.[33]

The consequence is that even if espionage is effective in enabling a State to access useful information relating to its adversaries capabilities, it must be recognised that this is necessarily achieved by violating a foundational legal rule of the international community which is designed to guarantee State survival. Somewhat inevitably, espionage therefore constitutes a hostile act that threatens State security and international peace and security more generally.[34]

In light of this, in recent years the defence of espionage has moved away from realist theory and towards a more functionalist approach; namely, that espionage is a desirable feature of international relations because it is a 'tool that enables functional cooperation'.[35] Baker has been a prominent proponent of this approach.

Baker argues that during the Cold War international peace and security was defined narrowly, being maintained where armed conflict between States was avoided. In the contemporary era however Baker contends that international peace and security is

---

[28] Stone has been a particular advocate of this approach; Julius Stone, 'Legal problems of espionage in conditions of modern conflict', in Robert J. Stranger (ed.), *Essays on Espionage and International Law* (Ohio State University Press, 1962).

[29] Christian Schaller, 'Spies' (2009) *Max Planck Encyclopaedia of Public International Law*. Parks argues that states regard espionage 'as a vital necessity in the national security process'; W. Hays Parks, 'The international law of intelligence collection', in John Norton Moore and Robert Turner (eds.), *National Security Law* (Carolina Academic Press, 1990) 433.

[30] Article 2(1) UN Charter 1945.

[31] Bardo Fassbender, 'The United Nations Charter as constitution of the international community' (1998) 36 *Columbia J. Trans. L.* 529.

[32] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 para. 202.

[33] Russell Buchan, *International Law and the Construction of the Liberal Peace* (Hart, 2013) 19 *ff*.

[34] See generally Herbert Scoville Jr., 'Is espionage necessary for our security?' (1976) 54 *Foreign Affairs* 482.

[35] Christopher D Baker, 'Tolerance of international espionage: A functional approach' (2003) 19 *Am. U. Int'l. L. Rev.* 1091, 1112.

defined far more expansively, being maintained not just where armed conflict between States is avoided but also where other important problems facing the world order are effectively addressed, including those relating to human rights violations, environmental degradation, economic insecurity, widespread poverty, pandemic influenza, etc.[36] Baker submits that these common problems can only be resolved, and thus international peace and security maintained, where States act in a collaborative and coordinated manner. International collaboration in resolving common problems is at its most effective, Baker suggests, when promises and commitments are enshrined in legally enforceable international rules which are in turn embedded within international organisations.[37]

It goes without saying that in order for these international agreements to successfully achieve their objectives State parties must comply with and discharge the obligations that these regimes impose. More often than not such regimes will have compliance and verification mechanisms integrated into them, sometimes through the creation of international organisations (for example the WTO) and sometimes through international tribunals (such as the Appellate Body of the WTO). However, Baker argues that in many instances States are able to circumvent these international regimes, thus undermining their effectiveness; 'conventional verification and assurance techniques represent an incomplete method for yielding information sufficient to satisfy States that parties to an agreement are complying with their international obligations'.[38]

It is here where Baker locates the utility of espionage. Obtaining confidential information belonging to States enables other States that participate in that legal framework to accurately determine whether or not such States have complied with their international obligations.[39] Where a State insists that it has complied with its international obligations and through espionage it is revealed that this is in fact true, a sense of trust will emerge and so States will become more willing to cooperate across functional lines and conclude additional international agreements aimed at resolving common problems that undermine the maintenance of international peace and security. He explains that:

> [m]utual trust between treaty parties increases when espionage affirms that the assurances provided are accurate. States will be more willing to cooperate with other states in the future if their espionage confirms that the assurances provided by these parties are truthful.[40]

Thus, for Baker the benefit of espionage is that it plays a key role in encouraging states to conclude international legal rules and institutions, a feature of international life that he considers essential to enabling the maintenance of international peace and security.

Writing in the context of cyber espionage (as opposed to espionage generally as Baker was), Pelican explains that '[t]he benefits to international stability and

---

[36] *Ibid*. 1099.

[37] *Ibid*.

[38] *Ibid*. 1103.

[39] 'When armed with such tools as spying and eavesdropping, states enjoy greater certainty that they will be able to validate international compliance, or at least detect when other participants are failing to comply with the treaty'; *ibid*. 1104.

[40] *Ibid*. 1105 (footnotes omitted).

cooperation as outlined by … Baker are as relevant today as they ever have been'.[41] After explicitly adopting Baker's reasoning Pelican concludes that cyber espionage 'should be recognized as a valuable tool for countries in promoting international stability'[42] and that 'cyber-espionage, like other forms of espionage, should persist unabated'.[43]

I disagree with this functional defence of espionage. I agree with Baker that many of the world's most pressing problems are now held in common and that in order for these to be resolved States must address them cooperatively. Indeed, the functional development of this cooperation into international law is often indispensable to resolving such problems. However, international legal frameworks can only be formulated and implemented if States enjoy close, trusted and effective cooperation. I argue that the surreptitious and unauthorised collection of confidential information, which as I have already argued constitutes a clear violation of a State's constitutional right under international law to have its sovereignty respected, is not conducive to fostering an environment imbued with trust and confidence. The consequence, I argue, and in contrast to Baker's claim, is that espionage inhibits and deters functional cooperation, thus preventing States from addressing important matters pertaining to international peace and security. In this sense, espionage represents a threat to the maintenance of international peace and security. A good example of the adverse implications that espionage yields for international cooperation is evident from the Gary Powers incident. Powers was a pilot of a US plane that was shot down in Soviet Union airspace on 1 May 1960. After initially asserting that the plane was a weather research aircraft the US administration eventually conceded that it was an aerial reconnaissance plane, and Powers was convicted for espionage under Soviet criminal law. This incident prompted a marked deterioration in relations between the US and the Soviet Union. Notably, recriminations over the incident meant that the much anticipated Four Powers Peace Summit that was due to take place in Paris on 16 May 1960 ended in abject failure. In fact, Soviet President Nikita Khrushchev explicitly blamed the US's spying for derailing the talks and subsequently rescinded an invitation he had earlier extended to President Eisenhower to visit the Soviet Union.[44]

As we shall see in the next section, States exert sovereignty in cyberspace notwithstanding the fact that it is a non-physical domain that transcends territorial borders and which at first sight appears immune from the exercise of State sovereignty. Thus, the accessing and copying of confidential information located in cyberspace, and which belongs to entities that fall under the sovereignty of a State (whether this is public authorities, private companies, individuals, etc), is regarded by States as a violation of their sovereignty. Given that cyber espionage results in the transgression of State sovereignty it becomes apparent that cyber espionage jeopardises the potential for

---

[41] Luke Pelican, 'Peacetime cyber-espionage: A dangerous but necessary game' (2012) 20 *Commlaw Conspectus* 363, 385.

[42] *Ibid*. 364.

[43] *Ibid*. 385.

[44] *BBC News*, '1960: east-west summit in tatters after spy plane row' (17 May 1060), <http://news.bbc.co.uk/onthisday/hi/dates/stories/may/17/newsid_2512000/2512335.stm> accessed 7 October 2014.

close and effective international cooperation and therefore undermines the potential for States to engage in dialogue and formulate international regulation in relation to matters that threaten international peace and security. This is well illustrated by Brazil's response to the revelations of NSA cyber espionage. When it was revealed that the US had routinely committed cyber espionage against Brazil, Brazilian President Dilma Rousseff cancelled a scheduled visit to Washington to meet representatives from the Obama administration to discuss important issues of international concern. Instead, she went 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 which, in turn, hinders effective cooperation between States:

> Friendly governments and societies that seek to consolidate a truly strategic partnership, such as is our case, cannot possibly allow recurring and illegal actions to go on as if they were normal, ordinary practice. Such actions are totally unacceptable.[45]

Importantly, because of the particular features and characteristics of cyber espionage, I argue that cyber espionage 'amplifies' the threat to international peace and security represented by espionage generally;[46] '[p]reclusion of espionage endeavours of foreign States has always been in the national interest of the target State. Cyber espionage, however, seems to have escalated the threat picture'.[47] The reason for this is clear. The advent of cyberspace and its ability to store huge amounts of important information, coupled with the speed and ease at which hostile actors can access this data, has significantly enhanced the opportunity for accessing and copying confidential information.[48] Thus, '[t]he internet is God's gift to spies';[49] cyberspace has 'heralded a 'golden age' of espionage'.[50] It is therefore unsurprising that since the emergence of cyberspace the practice of espionage has 'metastasized';[51] and thus why cyber

---

[45] *The Guardian*, 'Brazilian President: US surveillance a 'breach of international law' (24 September 2013), <http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance> accessed 7 October 2014.

[46] Office of the National Counterintelligence Executive, 'Foreign spies stealing US economic secrets in cyberspace: Report to Congress on foreign economic collection and industrial espionage 2009–2011' (2011) i.

[47] Ziolkowski (n 12) 463.

[48] 'The 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'; David Fidler, 'Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think' (2012) 5 *Int. J. Crit. Infra.* 28, 29.

[49] James Lewis from the Centre for Strategic and International Studies explains that '[t]he internet is God's gift to spies'; quoted in Fidler, *ibid*.

[50] Ziolkowski (n 12) 425.

[51] David Fidler, 'Economic cyber espionage and international law: Controversies involving government acquisition of trade secrets through technologies' (20 March 2013) 17 *A.J.I.L. Insights*, <http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving> accessed 7 October 2014.

espionage represents such a serious threat to international peace and security. Fidler is therefore correct in his assertion that 'cyberespionage is more dangerous than you think'.[52]

The argument that cyber espionage represents a threat to international peace and security is perhaps easiest to sustain where confidential information is copied that directly relates to a State's critical national infrastructure. An example would be reports that the NSA intercepted the private communications of Heads of State whilst conducting State business. Indeed, *The Guardian* newspaper reported that German Chancellor Angela Merkel's private communications were monitored for ten years.[53] Given the institution targeted (Head of State) and the likely nature of the information targeted (confidential communications relating to national security), such cyber espionage represents a significant infraction of State sovereignty and is likely to seriously disrupt cooperation between States and thus their ability to resolve matters that adversely impact upon international peace and security. According to Chancellor Merkel's spokesperson Steffen Seibert, Merkel was 'livid' at the revelations that her private communications had been monitored and telephoned US President Barack Obama to inform him that the NSA's actions represented a 'serious breach of confidence' and to demand an explanation.[54]

For similar reasons there is little difficultly in accepting that international cooperation is threatened where a State exploits cyberspace in order to obtain confidential information from a private company that provides services to critical national infrastructure. For example, the theft of terabytes worth of data on the F-35 fighter plane being developed by Lockheed Martin, a private company, for the US Government by (allegedly) the Chinese Government represented a 'direct threat to national security' and, moreover, to international peace and security more generally.[55]

Importantly, I argue cyber espionage constitutes a threat to international peace and security even where cyberspace is exploited to access and copy confidential information that is not immediately linked to critical national infrastructure. The issue is whether the person or entity whose confidential information has been appropriated falls under the authority and control – the sovereignty – of the State. If so, a violation of State sovereignty occurs, international cooperation is disrupted and a threat to international peace and security arises. As an illustration, in response to revelations that the NSA had committed cyber espionage against Brazilian citizens, before the General Assembly the Brazilian President explained that the NSA's violation of fundamental human rights constituted a violation of Brazil's sovereignty, '[a] sovereign nation can never establish itself to the detriment of another sovereign nation. The right to safety of citizens of one country can never be guaranteed by violating fundamental human rights

---

[52] Fidler (n 48).

[53] *The Snowden Files* (n 11) 9.

[54] *The Guardian*, 'Angela Merkel's call to Obama: Are you bugging my phone?' (24 October 2013), <http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german> accessed 7 October 2014.

[55] Alexander Melnitzky, 'Defending America against Chinese cyber espionage through the use of active defenses' (2012) 20 *Cardozo J. Int'l. & Comp. L.* 537, 545. On this incident see *The Wall Street Journal*, 'Computer spies breach fighter-jet project' (21 April 2009), <http://online.wsj.com/news/articles/SB124027491029837401> accessed 7 October 2014.

of citizens of another country'.[56] Similarly, in response to claims that the NSA had committed cyber espionage against German citizens, German Chancellor Angela Merkel explained that '[w]e need to have trust in our allies and partners, and now this must be established again. I repeat that spying among friends is not acceptable against anyone, and that goes for every citizen in Germany'.[57]

4. INTERNATIONAL LAW AND ITS APPLICATION TO CYBER ESPIONAGE

In the previous section I concluded that cyber espionage represents a threat to international peace and security and, consequently, is a practice that is in need of international regulation. This section identifies whether and to what extent international law prohibits cyber espionage.

There is no direct or specific international treaty that regulates cyber espionage. This does not mean however that this practice is conducted in a legal vacuum. It is inherent in the nature of such an activity that it can come into conflict with general principles of international law.[58] In the context of cyber espionage, the most relevant of these general principles are the prohibition against intervention and the prohibition against the use of force. Although there is fairly limited academic material assessing the permissibility of cyber espionage under international law, 'the conventional wisdom'[59] is that cyber espionage is compatible with these principles. Attention will now turn to whether cyber espionage falls foul of these two prohibitions.

The Principle of Non-Intervention

Although not expressly contained in the UN Charter, in the *Nicaragua* judgment the ICJ explained that the principle of non-intervention is nevertheless 'part and parcel of customary international law'.[60] In this decision the ICJ sought to clarify the scope of the non-intervention principle. The ICJ explained that:

> 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.

---

[56] Quoted in US Surveillance a 'breach of international law' (n 45).

[57] Quoted in *The Snowden Files* (n 11) 9.

[58] 'Long-standing international norms guiding state behaviour – in times of peace and conflict – also apply in cyber space'; The White House, *The US International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011) 9, <http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf> accessed 7 October 2014.

[59] John Murphy, 'Cyber war and international law: Does the international legal process constitute a threat to U.S. vital interests?' (2013) 89 *Int'l. L. Studies* 309, 399.

[60] *Nicaragua* (n 32) para. 202.

> Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.[61]

Thus, 'the element of coercion … defines, and indeed forms the very essence of, [a] prohibited intervention'.[62] In this context coercion is defined as the imposition of circumstances or conditions against a State that compromises or undermines its sovereignty.[63] On the basis that State sovereignty is ordinarily (or perhaps has been historically) understood as the exercise of exclusive authority and control over *territory*,[64] coercion is often regarded as at its most obvious and easily detectable where a State engages in conduct that violates the territorial integrity of another State.[65]

Traditional espionage, describing the situation where a State sends agents into the territory of another State to obtain confidential information, constitutes the imposition of coercion against the territorial integrity of a State and thus constitutes a violation of the non-intervention principle. As Wright explains, '[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'.[66] It therefore follows that 'any act by an agent of one State committed in another State's territory, contrary to the laws of the latter, constitutes intervention'.[67] Similarly, it is generally accepted that the use of reconnaissance aeroplanes in the territorial airspace of another State constitutes an unlawful intervention in the sovereign affairs of that State.[68]

Significantly, espionage committed in cyberspace does not result in the transgression of the territory of a State. This is because, to date, States have failed to subject

---

[61] *Ibid*. para. 205. See further UN General Assembly Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (1970) UN Doc A/RES/2625 (XXV).

[62] *Nicaragua* (n 32) para. 205.

[63] Philip Kunig, 'Intervention, Prohibition of' (2008) *Max Planck Encyclopaedia of Public International Law*. See generally Richard N Haass, *Intervention: The Use of American Military Force in the Post-Cold War World* (Brookings Institution, 1999).

[64] 'The basic legal concept of State sovereignty in customary international law … extends to the internal waters and territorial sea of every State and to the air space above its territory'; *Nicaragua* (n 32), para. 212. See generally Tsagourias's chapter in this handbook (Ch 1).

[65] '[T]he first and foremost restriction imposed by international law upon a State is that … it may not exercise power in any form in the territory of another State'; *SS Lotus Case (France v Turkey)* [1927] PCIJ Report Series A No. 10, 18. '[S]overeignty has always been, in part, based on the idea of territoriality … The extent of a sovereign's reach has usually been decided by geographic borders'; Walter Wriston, *The Twilight of Sovereignty: How the Information Revolution is Changing Our World* (New York: Scribner's, 1992) 7.

[66] Quincy Wright, 'Espionage and the doctrine of non-intervention in domestic affairs', in Richard Falk (ed.), *Essays on Espionage and International Law* (Ohio State University Press, 1962) 12.

[67] *Ibid*. 13.

[68] 'It appears that reconnaissance activities [that] are conducted in national airspace … violate national sovereignty'; Note, 'Legal aspects of reconnaissance in airspace and outer space' (1961) 61 *Columbia L. Rev.* 1074, 1095.

cyberspace to territorial claims in the sense of dividing this domain into territorial units.[69] To put the same matter differently, States do not possess territory in cyberspace.[70]

But this does not mean that cyber espionage does not violate the non-intervention principle. What is important to recognise is that the principle of non-intervention is designed to protect State sovereignty;[71] and as Jennings and Watts explain, '[s]overeignty has different aspects'.[72] Crucially, although as I have already noted State sovereignty is generally understood in terms of the possession of exclusive authority and control over territory, it is nevertheless well established in international law that State sovereignty transcends a State's physical territory and encompasses its authority and control over national affairs more broadly.[73] The principle of State sovereignty therefore protects both the territorial integrity of a State and its political integrity.[74] Thus, even in the absence of intervention in the physical territory of a State, where a State pursues a course of action that undermines or compromises the political integrity of another State that conduct is rightly classified as coercive and thus amounts to an unlawful intervention.

It should be noted here that commentators have argued that a State's political integrity will only be compromised or undermined (that is, subject to coercion) where

---

[69] For a more detailed discussion of why states do not possess territory in cyberspace see Tsagourias's contribution in Chapter 1 of this handbook. Note however that other commentators have argued that states do possess territory in cyberspace. Their argument is grounded in the idea that 'cyberspace requires physical architecture to exist', including copper wires, fiber-optic cables, satellite transponders, microwave relay towers, etc; Patrick W Franzese, 'Sovereignty in cyberspace: Can it exist?' (2009) 64 *Air Force L. Rev.* 1, 33. In this sense, the internet is a 'set of inter-connected computer networks linked to state territory and, thus, is liable to the exercise of sovereign jurisdiction on a territorial basis'; Teresa Scassa and Robert J. Currie, 'New first principles? Assessing the Internet's challenges to jurisdiction' (2011) 42 *Georgetown J. Int'l. L.* 1017, 1079. See also von Heinegg who explains that '[s]tate practice provides sufficient evidence that components of cyberspace are not immune from territorial sovereignty'; Wolff Heintschel von Heinegg, 'Territorial sovereignty and neutrality in cyberspace' (2013) 89 *Int'l L. Studies* 123, 126.

[70] The one exception maybe Iran's attempt to create a 'National Internet' (referred to as 'Halal Internet'), which is designed to be completely isolated from the World Wide Web and under the exclusive control of Iran. It is therefore certainly open to argument that the 'National Internet' maps on to the territory of Iran and thus constitutes a national cyberspace with clearly defined legal borders – in this sense the 'National Internet' can be considered an integral even if virtual part of Iran's territory; *The Guardian*, 'Iran clamps down on Internet use' (5 January 2012), <http://ww.guardian.co.uk/world/2012/jan/05/iran-clamps-down-internet-use> accessed 7 October 2014.

[71] '[T]he *raison d'être* of the non-intervention rule is the protection of the sovereignty of the State'; Kunig (n 63).

[72] Robert Jennings & Adam Watts, *Oppenheim's International Law* (Longman, 1996) 382.

[73] As Pirker notes, '[a] State's power reaches beyond its territory'; Benedict Pirker, 'Territorial sovereignty and integrity and the challenges of cyberspace' in Ziolkowski (n 12) 196.

[74] 'Between independent States, respect for territorial sovereignty is an essential foundation of international relations', and international law requires political integrity also to be respected'; *Nicaragua* (n 32) para 202, citing its judgment in the *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania)* [1949] ICJ Rep 35.

'action is taken by one State to secure a change in the policies of another'.[75] This interpretation is important in the context of cyber espionage because cyber espionage describes the practice of accessing and copying confidential information without authorisation i.e. cyber espionage does not require the copied information to be used to impose pressure or influence upon the victim State. Indeed, in many instances a State will be unaware that it has been the victim of cyber espionage. As a result, commentators have argued that cyber espionage does not constitute an infraction of the non-intervention principle:

> A forbidden intervention in domestic affairs requires the element of coercion of 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.[76]

However, this is a very narrow understanding of the principle of non-intervention. As I have explained, the notion of political integrity that is protected by the principle of non-intervention encompasses the capacity of a state to take decisions in an independent manner on matters essentially falling within the realm of its national concern. Thus, a breach of a State's political integrity arises where its authority and control is compromised or undermined. There is therefore 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 fall foul of the non-intervention principle.

In the context of cyber espionage the important question becomes whether States do in fact exercise sovereignty over information that is resident in or transmitted through cyberspace. If a State does not exercise sovereignty over information in cyberspace, a violation of the non-intervention principle cannot occur. In recent years State practice has effectively resolved this question. State practice reveals that States consider their sovereignty to extend to information in cyberspace which belongs to government institutions and to private entities and individuals over which they exercise jurisdiction.[77] In its June 2013 Report the Group of Governmental Experts, established pursuant to General Assembly Resolution 66/24 (2011), explained that '[s]tate sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities'.[78] This was reinforced by the UN Secretary-General in his foreword to the report, which encouraged 'anchoring ICT [information and communication technology] security in the existing framework of international law and

---

[75] Maziar Jamnejad and Michael Wood, 'The principle of non-intervention' (2009) 22 *L.J.I.L.* 345, 347–8.

[76] Ziolkowski (n 12) 433. See also Terry Gill, 'Non-intervention in the cyber context' in Ziolkowski (n 12) 224 ('the obtaining of information in itself falls short of coercive or dictatorial interference, and would not constitute 'intervention' in the legal sense').

[77] On jurisdiction in cyberspace see Kohl (Ch 2 of this book).

[78] UN Doc 68/98 (24 June 2013) 8.

understandings that govern State relations and provide the foundation for international peace and security'.[79]

The recent practice of States in the context of cyber espionage is especially revealing, indicating that States exert sovereignty over information in cyberspace which belongs to entities and individuals over which they exercise jurisdiction and that where this information is accessed and copied without authorisation an unlawful intervention occurs. As I have previously noted, in January 2010 Google alleged that China had infiltrated its computer network in order to access Gmail passwords of human rights activists in China. As Google is a company registered in the US and therefore subject to US jurisdiction (and the information belonging to this company falling under US sovereignty), the US responded to these claims by declaring that the conduct 'raised serious concerns' and demanded an explanation from the Chinese Government.[80] Significantly, the US Senate adopted Resolution 405 which stated that 'this attack was one in a series of attempts to exploit security flaws and *illegally* access computer networks of individuals and institutions through the clandestine installation of phishing an malware technology'.[81]

The revelations of NSA's cyber espionage activities also stimulated a number of legal rebukes, especially from Brazil. The Brazilian President's statement before the General Assembly is informative in so far as it reveals that Brazil considers sovereignty to extend to information resident in cyberspace and, moreover, where such information is accessed and copied a breach of international law occurs. Employing strong and unambiguous language the Brazilian President repeatedly referred to the US's conduct as an

> intrusion [and that the] [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.[82]

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'.[83] 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

---

[79] *Ibid*. 4. See also the remarks of the Chinese Assistant Foreign Minister Zheng Zequang who explained in 2013 that '[i]nternational cyber governance should follow the principles of state sovereignty and non-interference in other's internal affairs'; quoted in <http://www.aspistrategist.org.au/arf-and-how-to-change-the-tune-of-the-cyber-debate/> accessed 7 October 2014.

[80] Hillary Rodham Clinton, Secretary of State, Address, Washington, DC: Statement on Google Operations in China (12 January 2010), <http://www.state.gov/secretary/2009 2013clinton/rm/2010/01/135105.htm> accessed 7 October 2014.

[81] Senate Resolution 405, 111th Congressional (my emphasis).

[82] US Surveillance a 'Breach of International Law' (n 45).

[83] *Ibid*.

threat'.[84] China declared that the NSA's conduct 'deserve[d] to be rejected and condemned by the whole world'.[85]

Three final points need to be recorded. First, it is important to recognise that the claim that espionage (in its traditional conception) is unlawful under international law has attracted considerable criticism. The argument runs that because espionage is so widely practised by States customary international law has modified the scope of the non-intervention prohibition, which now recognises espionage as a permissible exception to the non-intervention principle. For example, Smith argues that:

> because espionage is such a fixture of international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law.[86]

However, just because espionage is widely practised does not render it permissible under customary international law. In order for a customary exception to form State practice must be accompanied by *opinio juris*.[87] Crucially, States overwhelmingly refuse to accept responsibility for espionage when accused, let alone assert the legality of this practice. Consequently, State practice of espionage 'is accompanied not by a sense of right but by a sense of wrong'[88] and to this end State practice and *opinio juris* run in opposite directions. Consequently, 'there is little doctrinal support for a "customary" defense of peacetime espionage in international law'.[89] The same argument can be made in relation to cyber espionage. As I noted in the introduction to this chapter, incidents of cyber espionage have increased dramatically in recent years. However, just because cyber espionage is widely practised by States does not mean that is it lawful under international law. What is important is whether this practice is accompanied by a belief that cyber espionage is lawful. As the above discussion of cyber espionage reveals, when committing cyber espionage States do not advocate that such conduct is permitted by international law. In fact, they often deny their involvement in the practice. Moreover, and as we have seen, States which are the

---

[84] Quoted in *The Guardian*, 'China demands halt to 'Unscrupulous' US cyber-spying (27 May 2014), <http://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying> accessed 7 October 2014.

[85] *Ibid*.

[86] Jeffrey H. Smith, Symposium, 'State intelligence gathering and international law: Keynote Address' (2007) 28 *Michigan J. Int'l. L.* 543, 544. Similarly, see Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence operations and international law' (2007) 28 Michigan J. Int'l. L. 625, 628 ('[s]tate practice throughout history … supports the legitimacy of spying. Nowhere in international law is peaceful espionage prohibited').

[87] Article 38(1)(b) of the Statute of the International Court of Justice 1945.

[88] Wright (n 66) 17.

[89] Craig Forcese, 'Spies without borders: International law an intelligence collection' (2011) 5 *J. Nat'l Sec. L. & Pol.* 179, 203. For a similar approach see Simon Chesterman. 'The Spy Who Came in from the Cold War: Intelligence and international law' (2006) 27 *Michigan J. Int'l. L.* 1071, 1072; Ingrid Delupis, 'Foreign warships and immunity of espionage' (1984) 78 *A.J.I.L.* 53; Manuel Garcia-Mora, 'Treason sedition and espionage as political offenses under the law of extradition' (1964) 26 *University of Pittsburgh L. Rev.* 65, 79-80.

victims of cyber espionage have protested (often vociferously) that such conduct is contrary to international law.

Secondly, it is worth reiterating for the sake of clarity that when determining whether an unlawful intervention in a State's sovereignty has occurred, it is irrelevant whether the information that has been copied belongs to State organs, private companies or even private individuals. Providing that the actor whose information has been accessed and copied is under the authority and control of the State, appropriation of that information constitutes intervention in that State's sovereignty.[90]

Thirdly, 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'.[91] 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'.[92]

Although often described as a maxim, this principle does impose a recognised legal restriction upon the operation of the non-intervention principle.[93] The consequence then is that acts of cyber espionage that can be regarded as insignificant will not trigger the non-intervention prohibition; acts of cyber espionage must be sufficiently serious in order warrant the application of international law. Much will depend upon the context of the specific case of cyber espionage in question. However, and for the purpose of illustration, it can perhaps be contended that whilst the unauthorised copying of information belonging to an important State organ (such as the Ministry of Defence) is likely to exceed the *de minimis* threshold, the one-off accessing and copying of innocuous electronic correspondence of a private individual is unlikely to be considered sufficiently serious to justify the engagement of international law.

The Prohibition against the Use of Force

Article 2(4) UN Charter, which is reflective of customary international law,[94] provides that '[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations'.

Historically, the meaning of the term force within Article 2(4) has been interpreted restrictively to only prohibit conduct that produces physical harm, namely 'the

---

[90] In assessing the application of the non-intervention principle to hostile cyber operations von Heinegg explains that '[i]t 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'; von Heinegg (n 69) 129.

[91] Jeff Nemerofsky, 'What is a trifle anyway?' (2001/2002) 37 *Gonzaga L. Rev.* 315, 323.

[92] *Ibid*.

[93] Jennings and Watts (n 72) 385 *ff*.

[94] *Nicaragua* (n 32) paras 187–190.

destruction to life and property'.[95] According to this understanding Article 2(4) does not extend to attacks against computer systems and networks which do not result in physical harm. In recent years this position has been criticised on the basis that in the contemporary era States are heavily reliant upon computer systems and networks and thus even a cyber attack that does not result in physical harm can still cause significant amounts of damage and disruption, such as a cyber attack that disables banking systems or incapacitates important government communications.[96] Indeed, it has been suggested that where these attacks are against computer systems that sustain critical national infrastructure the disruption may be so severe as to be equivalent to conventional attacks that cause kinetic harm.[97] Commentators have therefore argued that Article 2(4) should be reinterpreted so as to apply to cyber attacks which although not manifesting physical harm nevertheless cause damage and disruption equivalent to a kinetic attack.[98]

Developing this effects-based interpretation of Article 2(4) Melnitzky argues that exploiting computer systems in order to acquire highly sensitive and confidential information (cyber espionage) can, in particularly egregious circumstances, produce extremely serious adverse effects and should therefore be categorised as a use of force

> The severity of the problem of data theft is simply too great and its effects too harmful. […] The scale of theft is unprecedented. […] Prior to the Internet, looting on such a scale could only have been accomplished by a military occupation. The effects-based approach requirement that a cyberattack must cause damage only previous possible by traditional military force is therefore satisfied.[99]

I argue that there is insufficient State practice to support a reinterpretation of the term force within Article 2(4) to include cyber operations that do not produce kinetic harm.[100] Indeed certain States, most notably the US, have expressly rejected this approach. In 2012 the then US Legal Advisor Harold Koh unambiguously stated that cyber operations will only amount to an unlawful use of force where physical harm

---

[95] Ian Brownlie, *International Law and the Use of Force by States* (Clarendon, 1963) 362. On the use of force prohibition in the context of cyber operations see Roscini (Ch 11 of this book).

[96] Michael Schmitt, 'Computer network attack and the use of force in international law: Thoughts on a normative framework' (1998-1999) 37 *Columbia J. Trans. L.* 885.

[97] As Melnitzky notes, '[m]ilitaries have discovered that sophisticated cyberattacks on their own can be as debilitating as any conventional or "kinetic" attack'; Melnitzky (n 55) 542.

[98] See for example Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP, 2013) 55; Matthew Waxman, 'Cyber-attacks and the use of force: Back to the future of Article 2(4)' (2011) 36 *Yale J. Int'l L.* 421, 437.

[99] Melnitzky (n 55) 566. For a similar approach see also Jack Goldsmith, 'How cyber changes the laws of war' (2014) 24 *E.J.I.L.* 129; Todd Huntley, 'Controlling the use of force in cyberspace: The application of the law of armed conflict during a time of fundamental change in the nature of warfare' (2010) 60 *Naval L. Rev.* 1, 39; Anna Wortham, 'Should cyber exploitation every constitute a demonstration of hostile intention that may violate UN Charter provisions prohibiting the threat or use of force?' (2012) 64 *Federal Communications Law Journal* 643.

[100] I develop this argument in more detail in Russell Buchan, 'Cyber attacks: Unlawful uses of force or prohibited interventions?' (2012) 17 *J. Conflict & Sec. L.* 211.

occurs.[101] This is also the position adopted by the influential Tallinn Manual, which attempts to codify the international legal framework relating to the use of force to cyber warfare.[102]

On this basis I argue that cyber espionage cannot be regarded as a use of force under Article 2(4) UN Charter. Indeed, as Fidler concludes, 'no government regards cyber espionage of any kind as a prohibited use of force'.[103] It is worth noting here that if cyber espionage cannot amount to a use of force then, a *fortiori*, it cannot constitute an armed attack and engage a State's right to use force in self-defence under Article 51 UN Charter.[104]

5. CONCLUSION

This chapter has argued that in the contemporary world order international peace and security can only be maintained where States band together as a cohesive international community and address common problems in a coordinated and collaborative manner. In particular, the international community must confront these common problems by proactively adopting international legal regulation. However, States will only forge and implement international law where they have trust and confidence in each other's commitment to international law. In this chapter I have further reasoned that cyber espionage results in the violation of State sovereignty and thus breeds distrust and leads to a deterioration in international relations. In such an environment, I contend, States are unlikely to formulate and conclude international law in relation to important international issues that adversely impact upon the maintenance of international peace and security. When cast in this light, I argue that cyber espionage can be regarded as a threat to the maintenance of international peace and security.

Leading cyber security experts have noted the difficulty in developing computer software that provides effective protection against cyber espionage.[105] Actors therefore

---

[101] Harold Koh, *International Law in Cyberspace* (18 September 2012), <http://www.state.gov/s/l/releases/remarks/197924.htm> accessed 7 October 2014.

[102] Michael Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013) 48.

[103] Fidler (n 48).

[104] '[C]yber espionage cannot be deemed either a 'threat' or 'use of [armed] force' in the meaning of Article 2(4) of the UN Charter, nor an 'armed attack' pursuant to Article 51 UN Charter'; Ziolkowski (n 12) 456. On self-defence in cyberspace see Focarelli (Ch 12 of this book).

[105] See Richard Clarke & Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About it* (Harper Collins, 2010). According to Tim Berners-Lee, who is often accredited with inventing the internet, '[i]nternet security is hard. All systems have undiscovered holes in them, and it's only a question of how fast the bad guys can discover the holes compared with how fast the good guys can patch them up'; The Guardian, *The Snowden Files – Hands off my Baby* (2 December 2013), http://www.theguardian.com/technology/2013/dec/03/tim-berners-lee-spies-cracking-encryption-web-snowden> accessed 7 October 2014. Cf Ziolowski who argues that '[t]he only way to counter the threat of foreign States' cyber espionage is to improve the cyber security and resilience of the [sic] own IT-systems or computer networks'; Ziolkowski (n 12) 464.

look to law, and in the context of transboundary cyber espionage international law, for protection from this pernicious activity. However, according to current academic opinion international law does not prohibit cyber espionage. Fidler, for example, has declared that 'the lack of international law … allows cyberespionage to operate in a legal black hole'.[106]

In this chapter I have disputed this conclusion, arguing that there is international law that applies to cyber espionage. In particular, I have argued that cyber espionage contravenes the non-intervention principle. In order to effectively protect the sovereignty of States the non-intervention principle protects not just the territorial integrity of States but also their political integrity. As I have demonstrated above by reference to recent State practice, States regard information in cyberspace which belongs to entities and individuals which fall under their jurisdiction as representing an important element of their political integrity. For this reason, the unauthorised accessing and copying of such information is regarded as compromising State sovereignty. Consequently, cyber espionage amounts to a proscribed intervention under customary international law.

This is not to say that recent calls to build a new international treaty dedicated to regulating cyber operations (which would include cyber espionage) should not be pursued.[107] An international dialogue on the practice of cyber espionage – and indeed subsequently a specifically devised and technologically savvy international treaty regulating conduct in this new domain – would of course be beneficial. However, formulating international treaties in the field of international peace and security is notoriously difficult.[108] Until this can be achieved we should be reassured that existing principles of international law apply to State-sponsored transboundary cyber espionage and provide a certain degree of legal protection against this activity.

---

[106] Fidler (n 48) 29.

[107] Benjamin Mueller, 'The laws of war and cyberspace: On the need for a treaty concerning cyber conflict' (June 2014) 8, <http://www.lse.ac.uk/IDEAS/publications/reports/pdf/SU14_2_Cyberwarfare.pdf> accessed 7 October 2014.

[108] '[I]t has proven very difficult in today's environment for an international conference to conclude a global treaty to resolve challenges in the most important areas of international relations'; Murphy (n 59) 326.