Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions

Iñaki Navarrete† & Russell Buchan‡

This Article demonstrates that peacetime espionage does not benefit from permissive customary international law exceptions. The mainstream view contends that, though peacetime espionage may contravene international law, developments in customary international law (CIL) nevertheless undercut State responsibility for such conduct. The gist of this view is that acts of espionage benefit from permissive CIL exceptions because its practice is widespread and accepted within the international society. However, the mainstream literature has rarely—if ever—meaningfully engaged with the practice of espionage in an effort to tease out the objective and subjective elements supportive of customary espionage exceptions. This Article closes this gap and debunks the mainstream view. We show that, although widespread, most acts of espionage are committed in secret and, as such, they cannot qualify as State practice for the purpose of CIL formation. We further demonstrate that States have failed to issue expressions of the subjective element in support of customary espionage exceptions. We conclude by suggesting that, while States are entitled to develop customary espionage exceptions in the future, for now they have yet to come out of the legal wilderness.

† Iñaki Navarrete, (B.C.L., LL.B., McGill University, Faculty of Law), inaki.navarrete@mail.mcgill.ca.

‡ Dr Russell Buchan, University of Sheffield, UK, r.j.buchan@sheffield.ac.uk. This Article was written jointly by the authors. The authors are grateful to Guilhem de Roquefeuil, Craig Forcese, Kubo Maèák, Rachel Mazzarella, Pierrick Rouat, and Nicholas Tsagourias for their invaluable comments on earlier versions of this paper. All errors are our own.

51 Cornell Int'l L.J. 897 (2019)

Introduction

Peacetime espionage represents a serious conundrum for international legal scholars. On the one hand, while States have failed to implement international law that directly and specifically regulates espionage, scholars must recognize that States inhabit an international society that comprises multiple international laws designed to protect States' sovereign equality.[1] Because of its inherently intrusive nature, espionage is likely to run into conflict with a number of these rules. On the other hand, these scholars perceive the world order to be unpredictable and hostile.[2] In this environment, they are reluctant to allow international law to curtail States' ability to undertake espionage, which is regarded "as a vital necessity in the national security process" because it sheds light on the capabilities and intentions of other actors within the international society.[3]

The conundrum for scholars is therefore clear: disavowing the application of international law to espionage undermines the authority and integrity of the international legal order but at the same time applying international law to espionage deprives States of the national security ben-

1. *See, e.g.*, ANTONIO CASSESE, INTERNATIONAL LAW IN A DIVIDED WORLD 130, 130 (1986) (arguing the principle of the sovereign equality of States—as enshrined in Article 2(1) of the United Nations (UN) Charter 1945—is considered to be "the fundamental premise on which all international law rests.").

2. *Id.* at 131.

3. W. Hays Parks, *The International Law of Intelligence Collection, in* NATIONAL SECURITY LAW 433, 433 (John N. Moore & Robert Turner eds., 1990).

efits afforded by this practice.[4]

How have international legal scholars resolved this *problematique*? The short answer is: they haven't. Rather than tackling head-on the question of whether espionage is compatible with international law, scholars have instead preferred to sidestep this debate and avoid it entirely. In doing so, they have determined that "international law is silent on the subject"[5] of espionage, that is, that this is a practice that is neither "legal nor illegal under international law."[6] In 2007, for example, Radsan—a former assistant general counsel at the Central Intelligence Agency (CIA)—was so exasperated by the predicament that espionage creates for international lawyers that he exhorted: "Accepting that espionage is beyond the law, we should move on to other projects—with grace."[7]

International legal scholars have not been able to walk away from espionage. New and more effective means and methods of espionage keep emerging and these developments force espionage into the international legal spotlight. Take for instance the dawn of cyberspace and the potential for cyber-enabled espionage. Cyberspace is a domain that is now widely utilized by States to store massive quantities of confidential information. Given the speed and ease at which this information can be accessed, coupled with the fact that cyber espionage is a relatively risk-free enterprise insofar as it can be committed remotely, the practice has "metastasize[d]"[8] in the last decade and "cyber espionage projects [are] now prevalent."[9]

Compelled to grasp the nettle, there has been a flurry of international legal scholarship in recent years examining the applicability of international law to peacetime espionage.[10] Increasingly, scholars have conceded

4. Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1072–73 (2006) (Chesterman refers to this conundrum as the "elephant in the room" for international lawyers).

5. Gary Brown, *Spying and Fighting in Cyberspace: What is Which?*, 8 J. NAT'L SEC. L. & POL'Y 621, 621 (2016). *See also* Richard A. Falk, *Foreword* to ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW V (Roland J. Stranger ed., 1962) ("Traditional international law is remarkably oblivious to the peacetime practice of espionage.").

6. A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICHIGAN J. INT'L L. 595, 596 (2007). A number of authors have proposed their own criteria that can be used to determine the legality of peacetime espionage under international law. *See, e.g.*, Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 605 (2016); Ido Kilovaty, *World Wide Web of Exploitations: The Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach,* 18 COLUM. SCI. & TECH. L. REV. 42, 42 (2016); Darien Pun, *Rethinking Espionage in the Modern Era*, 18 CHI. J. INT'L L. 353, 353 (2017).

7. Radsan, *supra* note 6, at 597.

8. David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, 17 ASIL INSIGHTS 10 (2013).

9. Pete Warren, *State-Sponsored Cyber Espionage Projects Now Prevalent,* THE GUARDIAN (Aug. 30, 2012), https://www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent [https://perma.cc/AQ8N-7W9B].

10. *See, e.g.*, Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage*, *in* INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES (Anna-Maria Osula & Henry Rõigas eds, 2016); KRIANGSAK KITTICHAISAREE, PUBLIC INTERNTIONAL LAW AND CYBERSPACE (2016); Katharina Ziolkowski, *Cyber Espionage– New*

that certain forms of espionage transgress international law.[11] However, still wedded to the view that espionage is a necessary national security tool, they have overwhelmingly concluded that, while different forms of espionage violate different international legal rules, this illegality is nevertheless "undercut" and nullified by developments in customary international law (CIL).[12] This has now become the mainstream account of espionage.

This view holds that general and consistent practice of States acting out of a sense of legal right has carved out customary espionage "exceptions"[13] (or "defenses"[14]) to those primary rules of international law. The

---

Tendencies in Public International Law, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY (Katharina Ziolkowski ed., 2013); Jared Beim, *Enforcing a Prohibition on International Espionage*, 18 CHI. J. INT'L L. 647, 647 (2018); Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, 6 STRATEGIC STUD. Q. 126, 133–39 (2012); Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 291 (2015); Craig Forcese, *Pragmatism and Principle: Intelligence Agencies and International Law*, 102 VA. L. REV. ONLINE 67, 68 (2016); Chantal Khalil, *Thinking Intelligently about Intelligence: A Model Global Framework Protecting Privacy*, 47 GEO. WASH. INT'L L. REV. 919, 939 (2015); Iñaki Navarrete, *L'Espionnage en Temps de Paix en Droit International Public*, 53 CANADIAN Y.B. INT'L L. 1 (2016); Patrick C.R. Terry, *"Absolute Friends": United States Espionage Against Germany and Public International Law*, 28 REVUE QUEBECOISE DE DROIT INTERNATIONAL 173, 173 (2015); Robert D. Williams, *Spy Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1162 (2011); RUSSELL BUCHAN, CYBER ESPIONAGE AND INTERNATIONAL LAW (2018); FABIEN LAFOUASSE, L'ESPIONNAGE DANS LE DROIT INTERNATIONAL (2012).

11. Beim, *supra* note 10, at 653.

12. *See, e.g.*, Spencer M. Beresford, *Surveillance Aircraft and Satellites: A Problem of International Law*, 27 J. AIR L. & COM. 107, 114 (1961) (speaking of aerial espionage and arguing that "espionage is condoned by custom and tacitly accepted by long-continued international practice and forbearance."); Deeks, *supra* note 10, at 305 ("[T]he widespread and long-standing practice of spying—committed by many states in different regions of the world during time periods that both precede and post-date the UN Charter—undercuts arguments that these customary principles either were intended to prohibit espionage at the time they developed or should be deemed to do so today."); Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L L. & COM. REG. 443, 477 (2015) ("State practice throughout history . . . supports the legitimacy of spying. Nowhere in international law is peaceful espionage prohibited;" "By extension, cyber espionage in line with the same objectives of traditional espionage may be seen as acceptable state practice under international law as long as such activities stay within the bounds of acceptable limits analogous to those rules of traditional espionage that have been accepted by states."); Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, *The Intelligence Function and World Public Order*, 46 TEMPLE L.Q. 365, 394 (1973) (suggesting "a deep but reluctant admission of the lawfulness of . . . intelligence gathering when conducted within [certain] customary . . . limits."); Alexander Melnitzky, *Defending America against Chinese Cyber Espionage through the Use of Active Defenses*, 20 CARDOZO J. INT'L & COMP L. 537, 564 (2012) (speaking of an espionage exception); Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 628 (2007).

13. The ICJ has consistently used the term "exception" to describe developments in customary international law that modify the scope of international legal rules. *See, e.g.*, Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 207 (June 27).

14. Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SEC. L. & POL'Y 179, 203 (2011).

gist of the argument is that, because almost all States spy almost all of the time, acts of peacetime espionage that conflict with international law are by that very fact lawful.[15] Surprisingly, proponents of customary espionage exceptions have rarely, if ever, meaningfully engaged with the practice of espionage in an effort to tease out whether there is the necessary State practice and *opinio juris* to support their existence. The mainstream view has thus gone unchallenged and unexamined.

The objective of this Article is to close this gap and debunk the thesis currently perpetuated within international legal scholarship that peacetime espionage is permissible because customary espionage exceptions have emerged in relation to prohibitive international law. In pursuit of this objective, this Article is structured as follows.

Part I provides a working definition of peacetime espionage to frame the scope of this Article. It shows that peacetime espionage is best understood as a heterogeneous family of intelligence activities which are generally regulated on the basis of their underlying conduct. Part I also identifies those specific international laws that are violated by acts of espionage. Part II focuses on the current literature on espionage that contends that customary espionage exceptions have emerged under CIL. With this preliminary step achieved, Part III examines whether there is extensive State practice of espionage which supports the existence of customary espionage exceptions. It shows that while there is at least patchy and anecdotal evidence of extensive State practice of espionage, most of the practice conducted on the ground is secret, which prevents it from qualifying as State practice to form CIL. Part IV investigates whether this State practice is accompanied by *opinio juris*, and concludes that States have shied away from defending their intelligence activities under international law.

I. International Law and Peacetime Espionage

'Peacetime espionage' is a colloquial rather than a legal term. It is used here to describe different methods of collecting confidential information from closed as opposed to open sources.[16] Information is considered confidential where the owner possesses a "reasonable expectation of privacy"[17] over it, such as where a State classifies information as secret under national law or, in the cyber setting, where an actor encrypts information or hides it behind a firewall.[18] In order to constitute espionage, confiden-

15. *Id.* at 201–02.

16. Chesterman, *supra* note 4, at 1073 (noting that the collection of information from open sources—such as newspapers, journals, speeches—does not constitute espionage and is regarded as "legally unproblematic").

17. Simon Chesterman, One Nation under Surveillance: A New Social Contract to Defend Freedom without Sacrificing Liberty 246 (2011).

18. *See generally* Johann-Christoph Woltag, *Coded Communications (Encryption)*, Oxford Pub. Int'l L. (Mar. 2009), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e764 (but noting that "under international law coded communications are only protected explicitly in diplomatic law.").

tial information must be appropriated without the owner's consent or lawful authority.

Peacetime espionage is a practice that is generally conducted by States, against States.[19] Ordinarily, States perpetrate espionage to acquire information that reveals the political strategies, economic ambitions and military capabilities of other States. This is often referred to as *political espionage* and this term is used to distinguish it from economic and industrial espionage.[20] While economic and industrial espionage have become prominent practices within contemporary international society,[21] the focus of this Article is upon the regulation of political espionage.

Regulation of espionage derives from different legal sources. States invariably adopt national laws the purpose of which are to deter and suppress espionage by foreign actors. Almost always, States deploy criminal law measures to combat political espionage and foreign spies often receive severe penalties (including capital punishment) upon conviction of espionage. This Article does not undertake a comparative study of domestic legal frameworks with a view to assessing their application to espionage. Similarly, how international humanitarian law applies to wartime espionage falls outside of this Article's scope.[22] Instead, this Article is exclusively concerned with how international law regulates peacetime espionage.

At this point, we should sound a word of caution. It is true that States have failed to devise either conventional or customary international legal rules that regulate peacetime espionage.[23] This does *not* mean, however, that espionage is unregulated by international law. In fact, there is a "checkerboard" of principles of international law as well as specialized international legal regimes that indirectly regulate peacetime espionage on the basis of the underlying conduct of States.[24]

---

19. McDougal, Lasswell & Reisman, *supra* note 12, at 383 ("Clandestine intelligence activities are usually associated with nation-states.").

20. *See* Fidler, *supra* note 8 ("Economic espionage involves a State's attempts to acquire covertly trade secrets held by foreign private enterprises," usually with the intent to relay these trade secrets to domestic companies and thereby strengthen their position in the marketplace. "[I]ndustrial espionage' describes a company's illegal acquisition of another company's trade secrets with no government involvement."); *Espionage*, UK SECURITY SERVICE: MI5 (last visited Jan. 25, 2018) https://www.mi5.gov.uk/targets-of-espionage [https://perma.cc/MJ55-FSCG].

21. Karen Sepura, *Economic Espionage: The Front Line of a New World Economic War,* 26 SYRACUSE J. INT'L L. & COM. 127, 131 (1998). ("[T]he question these days . . . isn't which country commits economic espionage, but which doesn't.").

22. On the applicability of international humanitarian law to cyber espionage see, e.g., G.N. Barrie, *Spying–An International Law Perspective*, 2008 J. S. AFR. L. 238 (2008); Marco Longobardo, *(New) Cyber Exploitation and (Old) International Humanitarian Law* 77 ZEITSCHRIFT FÜR AUSLÄNDISCHES ÖFFENTLICHES RECHT UND VÖLKERRECHT 809 (2017).

23. *See, e.g.*, Martin Scheinin, Human Rights Council, *Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, ¶ 31, U.N. Doc. A/HRC/10/3, (Feb. 4, 2009) ("[N]o general norm exists in international law expressly prohibiting or limiting acts of intelligence gathering.").

24. Forcese, *supra* note 14, at 209.

International law does not therefore regulate espionage *per se* (i.e. the act of collecting closed information without consent) but, instead, regulates the legality of the conduct that is necessary to operationalize espionage, such as where a State sends its agents into another State to collect confidential information and in doing so violates that State's sovereignty.[25] In this sense, the legality of intelligence collection is determined by reference to the *actors* involved,[26] the *type* of information pursued[27] and the international legal *context* (or locus) within which it operates.[28]

The point being made is simple: to contemplate 'is peacetime espionage legal under international law?' is to ask the wrong question. Instead, what is required is that we subdivide "the world of intelligence collection into constituent state acts,"[29] which then have to "be subsumed under established heads of legal terminology, to be assessed, each on its own merits."[30] It is misconceived to categorize activities as prohibited or not prohibited, as very few activities are prohibited *per se* by international law.[31] 'Peacetime espionage' is no exception[32] and, as the practice of the

25. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 170 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0] ("While the International Group of Experts agreed that there is no prohibition of espionage *per se*, they likewise concurred that cyber espionage may be conducted in a manner that violates international law due to the fact that certain methods employed to conduct cyber espionage are unlawful.").

26. *See, e.g.*, Vienna Convention on Consular Relations art. 5(c), Apr. 24, 1963, 21 U.S.T. 77, 596 U.N.T.S. 261 [hereinafter VCCR]; Vienna Convention on Diplomatic Relations art. 3(d), Apr. 18, 1961, 23 U.S.T. 3327, 500 U.N.T.S. 95 [hereinafter VCDR].

27. *See, e.g.*, VCCR, *supra* note 26, art. 33; VCDR, *supra* note 26, art. 24.

28. For example, in another State's territory or in outer space. *See* Leslie Edmondson, *Espionage in Transnational Law*, 5 VAND. J. TRANSNAT'L L. 434, 447 (1972) ("Nations are reacting to espionage activity on the basis of permissible response to given types of spying rather than on the basis of the legality or illegality of espionage per se."). States confirmed this view with the 1960 U-2 incident, when a U.S. surveillance aircraft was shot down over the Soviet Union. States agreed that the U-2 flight had violated Soviet territory, and at the same time, a few States expressly recognized that there was no international law about peacetime espionage. *See* U.N. SCOR, 15th Sess., 858th mtg. at 3 &16, U.N. Doc. S/PV.858 (May 24, 1960) (French delegate stated "[t]here are no rules of international law concerning the gathering of intelligence in peace-time", while Poland delegate noted that "International law has never concerned itself with peacetime espionage.").

29. Forcese, *supra* note 14, at 68.

30. Pål Wrange, *Intervention in National and Private Cyberspace and International Law*, *in* INTERNATIONAL LAW AND CHANGING PERCEPTIONS OF SECURITY: LIBER AMICORUM SAID MAHMOUDI 307, 321 (Jonas Ebbesson et al. eds., 2014).

31. *See* BIN CHENG, STUDIES IN INTERNATIONAL SPACE LAW 437 (1997) ("Under general international law, there are in fact few activities of States that are either universally lawful or universally unlawful. Most of the time, it depends on where an activity is carried out. Thus, the answer to the question . . . on whether the act of intelligence-gathering [is legal depends on whether it is] carried out in a States' own territory, in the territory of another State, [or] the high seas.").

32. There is no functional or juridical reason to lump together different acts of 'peacetime espionage.' States do not possess an international 'right to privacy,' which would render *all* acts of intelligence gathering illegal wherever and by whomever committed. *See* Navarrete, *supra* note 10, at 53 ("[l]es États n'ont pas de droit à la vie privée en droit international comparable à celui reconnu aux individus par les droits de la personne.") ["States do not have a right to privacy similar to that of individuals under

International Court of Justice (ICJ) exemplifies, the legality of espionage is addressed by focusing upon the underlying conduct and without ever making reference to the concept of 'peacetime espionage' itself.[33]

To summarize, the international law *about* peacetime espionage is best modeled as the international law *about* the specific conduct of States when collecting intelligence.[34] This is important for our analysis of customary espionage exceptions, as the driving question behind this study is not whether customary international law has carved out one *blanket customary exception* for 'peacetime espionage' generally, but rather whether customary international law has carved out various exceptions to permit certain activities of intelligence collection which are otherwise prohibited by international law on the basis of their underlying conduct.

With these preliminary remarks in mind, we now identify those international legal rules that prohibit peacetime espionage and for which the current scholarship has identified customary exceptions. Thus, we do not provide an exhaustive discussion of how *all* rules that are potentially implicated by peacetime espionage apply to such conduct (e.g., the principle of

---

human rights law."] (our translation). *See generally* LÉOPOLD PEYREFITTE, DROIT DE L'ESPACE 274 (1993); Lieutenant Commander Robert E. Coyle, *Surveillance From the Seas*, 60 MIL. L. REV. 75, 91 (1973) (observing that while "states hold strong *wishes* that contents of their transmissions remain private, they have no *expectation* that their transmissions will be private."); J.F. McMahon, *Legal Aspects of Outer Space*, 38 BRIT. Y.B. INT'L L. 339, 369 (1962) ("[T]here is no international 'right to privacy' which would render every act of espionage contrary to international law."). *But see* Paul Reuter, *Le droit au secret des institutions internationales*, 2 ANNUAIRE FRANÇAIS DE DROIT INTERNATIONAL 46 (1956) (discussing the right to secrecy of international organizations). Nor do States have a general right to property, which could protect all forms of data collected. *See also* Peter Tzeng, *The States' Right to Property under International Law*, 125 Yale L.J. 1805, 1816 (2016).

33. Navarrete, *supra* note 10, at 16. *See, e.g.*, *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13.

34. On this bottom-up approach to intelligence collection, see Forcese, *supra* note 14, at 67 (speaking of a 'fourth approach' which "disregards a preoccupation with form ('intelligence collection') and instead examines law governing specific conduct (e.g., invasive surveillance, conduct of diplomats, interrogation, and so forth)."); Navarrete, *supra* note 10, at 2 (suggesting that "[l]a prise en compte de la pluralité des formes [d'espionnage en temps de paix] conduit à une image beaucoup plus nuancée; [l'espionnage en temps de paix] est une activité *a priori* licite, s'autorisant du principe de liberté des États, que des règles hétérogènes prohibent dans certains cas bien précis.") ["[l]ooking at the plurality of existing forms of peacetime espionage allows us to form a more nuanced view: peacetime espionage is an activity which is *a priori* lawful on the basis of the Lotus principle; except in specific cases where the practice under examination is prohibited by a set of specific and heterogenous legal rules."] (our translation); Chesterman, *supra* note 4, at 1127 (Chesterman also appears to favor this approach when speaking of a normative context which "draws on the various legal regimes that touch on aspects of intelligence work, but also on the emerging customs and practice of the intelligence community itself"); Terry, *supra* note 10, at 179 (Terry also seems to adopt this approach when he states: "The decisive discussion that needs to be had is whether the individual actions undertaken by foreign States in order to obtain information or influence events are compatible with international law."). This bottom-up approach is also used by TALLINN MANUAL 2.0, *supra* note 25, at 170 (noting that "[b]y styling a cyber operation as a 'cyber espionage operation,' a State cannot therefore claim that it is by definition lawful under international law.").

non-intervention;[35] international telecommunication laws;[36] international human rights law;[37] the right of States to conduct arbitration proceedings or negotiations without interference;[38] immunity of Heads of State,[39] etc.). Rather, we focus on (a) the principle of territorial sovereignty; (b) the law of the sea; and (c) diplomatic and consular law.

A. Principle of Territorial Sovereignty

Territorially intrusive forms of espionage violate the principle of territorial sovereignty. This principle is firmly established in international law[40] and, according to Arbitrator Max Huber in the *Island of Palmas* award: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[41] Central to the principle of territorial sovereignty is that States possess the

35. *See generally* Russell Buchan, *Cyber Espionage and International Law*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 180–86 (Nicholas Tsagourias & Russell Buchan eds., 2015).

36. *See generally* International Telecommunication Convention art. 22, Nov. 6, 1982, 1531 U.N.T.S. 319; Ian Waldon, *International Telecommunications Law, the Internet and the Regulation of Cyberspace*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 261–90 (Katharina Ziolkowski ed., 2013).

37. *See generally* International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171; David P Fidler, *Cyberspace and Human Rights*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 180–86 (Nicholas Tsagourias & Russell Buchan eds., 2015).

38. *See* Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Austl.), Provisional Measures Order, 2014 I.C.J. 147, ¶ 27 (Mar. 3); Navarrete, *supra* note 10, at 58 (arguing that the ICJ was correct in finding a "plausible legal right" for Timor-Leste "to conduct arbitration proceedings or negotiations without interference by Australia, including the right of confidentiality of and non-interference in its communications with its legal advisers."). *But see* Stefan Talmon, *Determining Customary International Law: the ICJ's Methodology Between Induction, Deduction and Assertion*, 26 EUR. J. INT'L L. 417, 423 (2016) (criticizing the methodology used by the ICJ to reach this conclusion).

39. Jovan Kurbalija, *E-Diplomacy and Diplomatic Law in the Internet Era*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 413 (Katharina Ziolkowski ed., 2013) (observing that "the alleged surveillance of the Presidents of Brazil, Mexico and others by the NSA could raise the question of a breach of international customary rules guaranteeing immunities for Heads of State."). *See also, e.g.*, *Is it illegal to spy on Indonesian officials, as president Susilo Bambino Yudhoyono Claims?*, ABC NEWS (Dec. 9, 2013), https://www.abc.net.au/news/2013-12-03/yudhoyono-goes-too-far-on-legality-of-spying/5117318 [https://perma.cc/6L88-LEKZ].

40. *See* Corfu Channel (U.K. v. Albania), Merits, 1949 I.C.J. 35 (Apr. 9) (the Court explained that "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations.").

41. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928) (emphasis added). On the customary status of the principle of territorial sovereignty see Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEXAS L. REV. 1639, 1645 (2017). *But see* Gary P. Corn & Robert Taylor, Online Symposium, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207, 209–10 (2017) (arguing that the principle of territorial sovereignty is a political norm rather than a legal rule).

right to determine entry to and egress from their territory, where State territory encompasses its land area, internal waters,[42] territorial sea,[43] national airspace[44] and, most recently, cyber infrastructure that is physically located within its borders.[45]

Any non-consensual or unauthorized intrusion into State territory represents a violation of the principle of territorial sovereignty. As the Permanent Court of International Justice (PCIJ) explained in the *Lotus* case, 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."[46] It was for this reason that in 1986 the ICJ determined that the US's unauthorized use of (reconnaissance) airplanes violated Nicaragua's sovereignty.[47]

A growing body of national decisions has steadily recognized that territorially intrusive forms of espionage violate the principle of territorial sovereignty.[48] In 2008 the Federal Court of Canada refused to grant a warrant to the Canadian Security Intelligence Service (CSIS) to conduct espionage activities abroad on the basis that they contravened international

42. United Nations Convention on the Law of the Sea art. 8, Dec. 10, 1982, 1833 U.N.T.S. 23 [hereinafter UNCLOS].

43. *Id.* art. 3.

44. Chicago Convention on International Civil Aviation art. 1, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 95, Doc 7300/9 I.C.A.O. 2 ("The contracting states recognize that every state has complete and exclusive sovereignty over the airspace above its territory.").

45. TALLINN MANUAL 2.0, *supra* note 25, rule 2.

46. The Case of the S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18–19 (Sept. 7).

47. *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13, ¶ 251 (The ICJ explained that "[t]he 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.").

48. The current literature has been mostly oblivious to these national decisions. *See* Scheuner, *Der Notenwechsel zwischen der Schweiz und Italien in der Angelegenheit Cesare Rossi*, 1 ZEITSCHRIFT FÜR AUSLÄNDISCHE UND ÖFFENTLICHE RECHT 280, 283 (1928) (Ger.), https://goo.gl/Bf9b15 [https://perma.cc/SDY4-PNX8] (Swiss federal agent Motta stating that the sending of undercover agents into another State's territory to collect information constitutes a violation of international law); Rex v. Rose, [1946] 3 C.R. 282 (Quebec Court of King's Bench) (stating that since the war of 1914–18, conspiring against the host State or organizing espionage constitute abuses of office under international law), *reprinted in* 13 ANN. DIG. & REP. PUB. INT'L L. CASES 161, 164 (H. Lauterpacht ed., 1951); In re Flesche, [1949] (Holland, Special Criminal Court, Amsterdam) (stating that peacetime espionage "when taking place by order of a State, constitutes an international delinquency by that State against another State for which it is answerable under international law"), *reprinted in* 16 ANN. DIG. & REP. PUB. INT'L L. CASES 266, 272 (H. Lauterpacht ed., 1955); Yao Lun, Military Procurator of the Supreme People's Procuratorate v. Arnold et al., [1954] (Military Tribunal of the Supreme People's Court, China) (stating that aerial reconnaissance jeopardized China's national security and was an intrusion into its territorial air space), *reprinted in* 47 ANN. DIG. & REP. PUB. INT'L L. CASES 109, 111 (H. Lauterpacht ed., 1974); Powers case, [1960] (Union of Soviet Socialist Republics, Supreme Court) (where the Supreme Court of the USSR considered that agent Powers violated the USSR's airspace for purposes of espionage), *reprinted in* 30 INT'L L. REP. 69, 73–74 (E. Lauterpacht ed., 1966).

law.[49] In refusing to issue this warrant, the Federal Court observed that the intrusive activities contemplated would "clearly impinge upon the . . . principles of territorial sovereign equality and non-intervention and are likely to violate the laws of the jurisdiction where the investigative activities are to occur."[50] In light of the above, it can be concluded 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."[51]

This conclusion should be tempered in the case of cyber espionage as States are still debating the precise remit of the principle of territorial sovereignty in cyberspace. In this respect, there was agreement among the International Group of Experts responsible for compiling the influential Tallinn Manual 2.0 that cyber operations violate a State's territorial sovereignty where they produce real-world physical damage (such as death or injury to people or damage to physical property)[52] or give rise to destructive effects in cyberspace (such as affecting the availability or functionality of computer systems).[53] According to this view, because cyber espionage only involves the copying of confidential information it does not trigger a violation of the territorial sovereignty principle.[54] This being said, there is another school of thought that contends that *any* cyber operation (includ-

49. Canadian Security Intelligence Service Act (Re) (F.C.), 2008 F.C. 230, [2008] 4 F.C.R. 230.

50. *Id.* at paras. 49–55; *see also* X(Re), 2013 F.C. 1275, para. 105, [2015] 1 F.C.R 635, para. 105.

51. Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, 12 (Roland J. Stanger ed., 1962). *See also* JOHN KISH INTERNATIONAL LAW AND ESPIONAGE 84 (David Turns ed., 1995) ("[The principle of territorial integrity] negates the general permissibility of strategic observation in foreign territory."); Manuel R. Garcia-Mora, *Treason, Sedition, and Espionage as Political Offenses under the Law of Extradition*, 26 U. PITT L. REV. 65, 79–80 (1964) ("Though international law does not explicitly condemn wartime espionage, peacetime espionage is regarded as an international delinquency and a violation of international law."); Andrey L. Kozik, *The Concept of Sovereignty as a Foundation for Determining the Legality of the Conduct of States in Cyberspace*, 14 BALTIC Y.B. INT'L L. 93, 99 (2014) ("[S]ending spies into the territory of another State would be a violation of the territorial sovereignty rule"); Frederick Alexander Mann, *The Doctrine of Jurisdiction in International Law*, 111 COLLECTED COURSES OF THE HAGUE ACADEMY OF INT'L L. 1, 139 (1964) ("[A State may not] send its police officers, even if they are in civilian clothes, into foreign States to investigate crimes or make enquiries affecting investigations in their own country. Nor can it allow spies or informers to operate abroad.").

52. *See* TALLINN MANUAL 2.0, *supra* note 25, at 20 ("To the extent that non-consensual physical presence on another State's territory to conduct cyber operations amounts to a violation of sovereignty, the Experts concurred that the causation of physical consequences by remote means on that territory likewise constitutes a violation of sovereignty.").

53. *Id.* at 20–21 ("[T]he Experts agreed that, in addition to physical damage, the remote causation of loss of functionality of cyber infrastructure located in another State sometimes constitutes a violation of sovereignty, although no consensus could be achieved as to the precise threshold at which this is so due to a lack of *opinio juris* in this regard.").

54. *Id.* at 171 ("The majority of the Experts was of the view that exfiltration violates no international law prohibition irrespective of the attendant severity.").

ing espionage) that intrudes upon a State's cyber infrastructure without consent or authorization contravenes the principle of territorial sovereignty, regardless of whether additional damage or harm is caused.[55] The reaction of a number of States to the Snowden revelations supports this latter, broader view but State practice in this area is embryonic and even contradictory.[56]

Not all forms of espionage are territorially intrusive and hence captured by the principle of territorial sovereignty. Technological developments have enabled States to spy without having to physically penetrate each other's territory. States can therefore conduct espionage *passively* (e.g., by using listening posts within their own territory or upon the high seas to capture electronic signals emanating from the territory of other States) or *peripherally* (e.g., by using satellites or drones in outer space to observe events occurring within another State's territory).

There is a related point. As well as protecting their physical territory, the principle of territorial sovereignty also protects the right of States to perform governmental functions (so called 'enforcement jurisdiction') within their territory to the exclusion of all others.[57] This means that the principle of territorial sovereignty can be violated even in the absence of a physical intrusion into State territory—the question is whether the act under examination "interferes with or usurps the inherently governmental functions of another State."[58] With regard to espionage, State practice indicates that conduct that deprives a State of its confidentiality over information does not in and by itself amount to interference in or usurpation of a State's sovereignty. For example, the use of satellites to conduct remote sensing is widely regarded as compliant with international law,[59] as are the use of listening posts stationed within a State's territory to passively cap-

55. *See* Wrange, *supra* note 30, at 322 ("[E]spionage that involves unauthorized access to servers and other computers in a foreign state generally constitute illegal interventions into the sovereignty of that state.").

56. *See* Jeremy Wright, UK Attorney General, Speech Delivered at Chatham House, London, *Cyber and International Law in the 21st Century* (May, 23 2018) (explaining the United Kingdom's position on applying international law to cyberspace and stating: "Some have sought to argue for the existence of a cyber specific rule of a 'violation of territorial sovereignty' in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law."). For a discussion of this State practice see *infra* Table 1. *See also* BUCHAN, *supra* note 10, chapter 3.

57. *See* Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123, 124 (2013) (explaining that the principle of territorial sovereignty means that "the State alone is entitled to exercise jurisdiction, especially by subjecting objects and persons within its territory to domestic legislation and to enforce these rules. Moreover, the State is entitled to control access to and egress from its territory.").

58. TALLINN MANUAL 2.0, *supra* note 25, at 21; Navarrete, *supra* note 10, at 31. *See also* R. v. Hape, [2007] 2 S.C.R. 292 (Can.).

59. *See Principles Relating to Remote Sensing of the Earth from Outer Space*, G.A. Res. 41/65, U.N. GAOR, 41st Sess., U.N. Doc. A/RES/41/64 (1986). *See generally* Harry

ture electronic signals emanating from the territory of another State.[60]

B. Law of the Sea

Peacetime espionage may also run into conflict with the rules of the United Nations *Convention on the Law of the Sea* (UNCLOS).[61] UNCLOS delineates the legal framework applicable to the sea and determines who exercises jurisdiction over this environment and how activities must be conducted within it more generally.[62] For the purpose of this Article, it suffices to say that every State has the right to establish the breadth of its territorial sea up to a limit not exceeding 12 nautical miles from its baseline,[63] which is usually the low-water line of the State's coast.[64]

To facilitate global navigation, States are entitled to innocent passage through the territorial sea of other States. Article 19 UNCLOS provides that "[p]assage is innocent so long as it is not prejudicial to the peace, good order or security of the coastal State" and proceeds to give examples of conduct that can be regarded as prejudicial.[65] In particular, Article 19(2)(c) explains that passage is non-innocent where it involves "any act aimed at collecting information to the prejudice of the defence or security of the coastal State."[66] Article 19(2)(c) is cast in broad terms and encompasses different forms of information collection including the acquisition of information from closed sources, that is, espionage.[67] Indeed, State practice subsequent to UNCLOS's adoption demonstrates that States regard the presence of vessels in their territorial sea for espionage purposes as non-innocent and have protested and objected in such instances.[68]

Beyond the territorial sea exists the high sea. Enshrined within UNCLOS is the principle of the freedom of the high seas,[69] which recognizes the right of all nations to freedom of navigation and overflight. The corollary of this principle is that UNCLOS does not prohibit States from

---

Feder, *The Sky's the Limit? Evaluating the International law of Remote Sensing*, 23 NYU J. INT'L L. & POL'Y 599 (1991).

60. Weber and Saravia v. Germany, App. No. 54934/00, 2006-XI Eur. Ct. H.R. 309, 344; Navarrete, *supra* note 10, at 21.

61. UNCLOS, *supra* note 42, art. 19.

62. *See generally id.*

63. *Id.* art. 3.

64. *Id.* art. 5

65. *Id.* art. 19.

66. *Id.*

67. *See* James Kraska, *Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters*, 54 COLUM. J. TRANSNAT'L L. 164, 219 (2015) ("[T]he proscription against 'any act aimed at collecting information to the prejudice of the defense or security of the coastal State,' quite plainly makes intelligence gathering inherently not innocent"); *See also* Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical* Vade Mecum, 8 HARV. NAT'L SECURITY J. 239 (noting that "[a]lthough espionage is not unlawful *per se*, engaging in it during innocent passage is an internationally wrongful act.").

68. For a discussion of this practice see *id.* at 212 *et seq*.

69. UNCLOS, *supra* note 42, art. 87.

engaging in espionage while on the high seas.[70] Such conduct is, however, residually regulated by general principles of international law.

C. Diplomatic and Consular Law

Finally, peacetime espionage may also violate the *Vienna Convention on Diplomatic Relations* (VCDR) and the *Vienna Convention on Consular Relations* (VCCR). These conventions prohibit receiving States from committing espionage against the diplomatic and consular missions of sending States.[71] This legal framework imposes a triple lock of protection to this effect.

First, diplomatic and consular premises are "inviolable" and can only be entered with the consent of the head of mission.[72] Diplomatic and consular premises include the buildings or parts of buildings and the land ancillary thereto (irrespective of ownership) that is used for the purposes of the mission.[73] Premises also include cyber infrastructure located upon their territory, which extends to computer networks and systems supported by that cyber infrastructure.[74] Any intrusion into these premises—including for the purpose of espionage—is prohibited.[75]

Second, archives and documents of diplomatic and consular missions are inviolable at all times and wherever they may be.[76] In this context, 'archives and documents' are defined broadly to include "all the papers, documents correspondence, books, films, tapes and registers of the consular post, together with the ciphers and codes, the card-indexes and any article of furniture intended for their protection or safekeeping."[77] Certainly, it is prohibited to commit acts of espionage against the archives and documents of diplomatic and consular missions.

---

70. *See* Petros Liacouras, *Intelligence gathering on the High Seas*, *in* UNRESOLVED ISSUES AND NEW CHALLENGES TO THE LAW OF THE SEA: TIME BEFORE AND TIME AFTER 121, 134 (Anastasia Strati, Maria Gavouneli & Nikolaos Skourtos eds., 2006) ("[I]ntelligence gathering on vessels sailing in international waters is permitted in principle."); Oliver J. Lissitzyn, *Electronic Reconnaissance from the High Seas and International Law*, 61 INT'L L. STUD. 563, 569 ("[I]nternational law does not forbid electronic reconnaissance from the high seas."); Chesterman, *supra* note 4, at 1082–83.

71. VCDR, *supra* note 26, art. 21; VCCR, *supra* note 26, art. 31. While the VCDR and the VCCR prohibit diplomatic and consular posts from engaging in espionage, these conventions confer upon diplomatic and consular officials immunity from the criminal jurisdiction of the receiving state. *See* VCDR, *supra* note 26, art. 31(1) and VCCR, *supra* note 26, art. 41(1). This is significant because acts of espionage committed by diplomatic and consular officials almost certainly violate the national criminal law of the receiving state, as all states criminalize espionage. However, even if diplomatic and consular officials can invoke immunity in relation to criminal acts of espionage, the sending state is nevertheless responsible for violations of diplomatic and consular law committed by its diplomatic and consular officials and thus the question of whether customary espionage exceptions exist in relation to those prohibitive rules remains apposite.

72. VCDR, *supra* note 26, art. 21; VCCR, *supra* note 26, art. 31.

73. VCDR, *supra* note 26, art. 1(i); VCCR, *supra* note 26, art. 1, ¶ 1(j).

74. TALLINN MANUAL 2.0, *supra* note 25, at 212.

75. *See* René Värk, *Diplomatic and Consular Privileges and Immunities in Case of Unfriendly Cyber Activities*, 14 BALTIC Y.B. INT'L L. 125, 130 (2014).

76. VCDR, *supra* note 26, art. 24; VCCR, *supra* note 26, art. 33.

77. VCCR, *supra* note 26, art. 1, ¶ 1(k).

Third, in addition to the inviolability of archives and documents, diplomatic and consular law provides that "official correspondence" belonging to diplomatic and consular missions is "inviolable."[78] The objective of this provision is to guarantee the secrecy between diplomatic and consular missions and their sending State and in doing so buttress the legal protection afforded to these missions against espionage.

Diplomatic and consular law proscribes diplomatic and consular missions from being used as a platform for espionage. First, diplomatic and consular law imposes a duty upon staff to respect the laws and regulations of the receiving State.[79] Given that most States adopt national laws that prohibit espionage, diplomatic and consular staff that engage in espionage will violate local law and thus the sending State will violate its treaty obligation. Second, diplomatic staff "have a duty not to interfere in the internal affairs of that [the receiving] State."[80] For the purpose of this provision, considerable State practice has affirmed that acts of espionage—regardless of whether this conduct physically intrudes upon State territory or is conducted passively—constitute interference in a State's internal affairs.[81] Third, the premises of diplomatic and consular missions cannot be used in any manner incompatible with the functions of the mission.[82] Undoubtedly, diplomatic and consular missions are permitted to collect information while operating within the territory of a receiving State.[83] Yet, they can only collect information by 'all lawful means.' 'Lawful means' includes those measures that are acceptable under the domestic law of the receiving State. Given that espionage is likely to violate the domestic law of most States, espionage represents an "abuse of . . . function"[84] and, on this basis, cannot be regarded as a lawful means through which diplomatic and consular missions can collect information.[85]

II. Customary Exceptions and Peacetime Espionage

Article 38(1)(b) of the *Statute of the International Court of Justice* 1945 refers to "international custom" as a source of international law, which it defines as a "general practice accepted as law."[86] The jurisprudence of the

78. VCDR, *supra* note 26, art. 27, ¶ 2; VCCR, *supra* note 26, art. 35, ¶ 2.

79. VCDR, *supra* note 26, art. 41, ¶ 1; VCCR, *supra* note 26, art. 55, ¶ 1.

80. VCCR, *supra* note 26, art. 55, ¶ 1.

81. *E.g.*, U.S. Dep't of State, *Expulsions of Soviets Worldwide, 1986*, Foreign Affairs Note, 4 (Jan. 1987) (In 1985 Liberia expelled the entire Soviet diplomatic mission for acts of espionage that it considered amounted to "'gross interference' in Liberian internal affairs.").

82. VCDR, *supra* note 26, art. 41, ¶ 3; VCCR, *supra* note 26, art. 55, ¶ 2.

83. VCDR, *supra* note 26, art. 3, ¶ d; VCCR, *supra* note 26, art. 5, ¶ c.

84. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, ¶ 84 (May 24); Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. INT'L L. 53, 69 (1984) ("[D]iplomats commit acts contrary to international law if they gather secret information.").

85. *See* TALLINN MANUAL 2.0, *supra* note 25, at 229.

86. Statute of the International Court of Justice, June 26, 1945, art. 38, ¶ 1(b), 59 Stat. 1055.

ICJ[87] and the work of the International Law Commission (ILC)[88] confirm that two elements must be established for CIL to form. First, State practice of the rule in question; and second, the requirement that this practice is accepted by States as law (*opinio juris*). This methodology for the identification of CIL is known as the "two-element approach"[89] and requires, *au fond*, an arithmetical exercise of counting State practice coupled with *opinio juris* to determine whether a certain practice has attracted sufficient support between States for it to be regarded as communally accepted and thus binding CIL. This methodology applies to the identification of 'customary exceptions.'[90]

It can be preliminarily concluded from the previous section that espionage contravenes a number of primary norms of international law. While scholars have been prepared—facially—to accept that espionage runs into conflict with these rules, they invariably assert the thesis that, because espionage is so widespread within the world order, CIL permits such conduct.[91] In essence, these scholars argue that "[y]ears of state practice" of espionage has given rise to a permissive rule or rules of CIL in favor of the legality of such conduct.[92] Scholars have articulated this claim in two different ways, which must be distinguished.

One group of scholars has asserted that CIL embraces what we term a *blanket espionage exception*. The gist of this approach is that "because espionage is such a fixture in 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."[93] This blanket exception is rooted not so much in an assessment of the full empirical record of State practice and *opinio juris* for each form of spying, but on the idea that "intelligence activities [as whole] are now accepted as a common, even inherent, attribute of the modern state."[94]

---

87. *E.g.*, *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13, ¶ 207 ("[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*."); Continental Shelf (Libya Arab Jamahiriya/Malta), Judgment, 1985 I.C.J. 13, ¶ 27 (June 3) ("It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and *opinio juris* of States.").

88. *See* Int'l Law Comm'n, *Report of the International Law Commission: Seventieth Session*, U.N. Doc. A/73/10, at 124 (2018) ("To determine the existence and content of a rule of customary international law, it is necessary to ascertain whether there is a general practice that is accepted as law (*opinio juris*)").

89. *See* Michael Wood (Special Rapporteur), *Second Rep. on Identification of Customary International Law*, U.N. Doc. A/CN.4/672, ¶ 21 (2014).

90. *See id.* We elaborate more on this two-element approach in Part IV below.

91. *See supra* note 12.

92. Brown & Poellet, *supra* note 10, at 134 ("Years of state practice accepting violations of territorial sovereignty for the purpose of espionage have apparently led to the establishment of an exception to traditional rules of sovereignty—a new norm seems to have been created.").

93. Jeffrey H. Smith, *State Intelligence Gathering and International Law*, 28 MICH. J. INT'L L. 543, 544 (2007).

94. Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 321 (1996). *See also* KISH, *supra* note 51, at xv (observing that espionage has become an "established international function of States . . . [and] Governments have

However, this all-encompassing approach is methodologically flawed. As we have seen, 'peacetime espionage' is not an operative legal concept. Different forms of espionage engage different international legal rules. Another group of scholars has therefore correctly observed that when determining whether CIL contains a right to spy, what is required is an assessment of State practice with regard to the specific international legal rule that it contravenes.

Building on the above, these scholars have maintained that territorially intrusive acts of espionage (e.g., that violate the principle of territorial sovereignty or UNCLOS) benefit from a customary exception because "states have practiced territorially intrusive intelligence collection by air, sea, and on land, through a variety of means, from time immemorial."[95] With regard to remotely launched acts of cyber espionage, the claim is that such conduct is akin to territorially intrusive acts of espionage and thus—by extension—benefits from the same customary exception.[96] Others have gone further and argued that State practice of remotely launched cyber espionage operations is—in and of itself—"so thick, and the condemnation on the basis of international law so muted,"[97] that customary international law regards such conduct as lawful.

Other scholars have further claimed that a customary exception has emerged which permits States to listen to communications to, from and within diplomatic and consular premises, this being conduct that is *prima facie* in violation of the VCDR and VCCR. Deeks, for instance, considers that in light of the extensive practice of violating the VCDR, and the fact that States did not explicitly address spying in this treaty despite it being so widespread, "it would be a notable change to interpret the VCDR to prohibit such activities."[98] Similarly, Reisman and Freedman note that States that "engage in such conduct must conclude, and presumably have concluded, that the need for and value of intelligence gained by electronic surveillance outweighs the incremental erosion of the norm upholding the

publicly admitted the existence of their intelligence services and systematic espionage operations"); THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 350 (2000) ("[T]he practice of states has specifically recognized a right to engage in such clandestine intelligence collection activities as an inherent part of foreign relations and policy."); Kilovaty, *supra* note 6, at 60 (noting that "peacetime espionage is inherent to the function of a state, and it has been used massively throughout history").

95. Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 226 (1999). *See also supra* note 22.

96. *See* TALLINN MANUAL 2.0, *supra* note 25, at 171 ("A few of the Experts took the view that this activity would not be unlawful, suggesting that acts of espionage represent an exception to the prohibitions of violation of sovereignty (Rule 4) and intervention (Rule 66).").

97. Michael N. Schmitt, *Cyber Response "By The Numbers" in International Law*, EJIL: *Talk!* (Aug. 4, 2015), https://goo.gl/YwiHgx [https://perma.cc/59B7-JVM6].

98. Deeks, *supra* note 6, at 255; *see also* Deeks, *supra* note 10, at 313 (arguing that "[t]he same analysis could apply to the question of spying by the sending state using the mission as a base: It is so widespread that it is inappropriate to interpret VCDR Art. 41 as prohibiting such activity.").

inviolability of diplomatic premises and their communications."[99] The Tallinn Manual 2.0 notes that "a few" of its Experts were of the view that diplomatic and consular missions can be used to engage in cyber espionage against third party States "because long-standing allegations of State practice" points to the permissibility of such practice.[100]

To summarize, international legal scholarship has claimed specific customary exceptions for the following conduct:

1. Non-consensual or unauthorized intrusions by (a) undercover agents on the ground (without diplomatic or consular character), (b) ships, (c) submarines, and (d) planes into the territory of another State to collect confidential information in violation of the principle of territorial sovereignty, the Chicago Convention 1944 or UNCLOS 1982.
2. Non-innocent passage by a ship or submarine into the territorial sea of another State to collect confidential information in violation of Article 19(2)(c) UNCLOS 1982, and parallel principles of customary international law.
3. Spying from diplomatic and consular premises in violation of VCDR 1961 and VCCR 1963, and parallel principles of customary international law.
4. Spying on diplomatic and consular premises, archives, documents or official correspondence in violation of the VCDR 1961 and VCCR 1963, and parallel principles of customary international law.
5. Non-consensual or unauthorized remote access cyber intrusions into the networks and systems of another State to collect confidential information, *possibly* in violation of the principle of territorial sovereignty.

For each of these customary exceptions, the obligation is upon the State asserting a right under CIL to prove that there is sufficient State practice accompanied by *opinio juris* to support its existence.[101] We now turn to these two elements holistically for each form of spying.

III. State Practice

State practice is the objective or material element of CIL and it can take the form of acts or omissions.[102] State practice comprises physical and verbal conduct undertaken by the legislature, executive or judiciary and includes but is not limited to:[103] physical conduct of States 'on the ground,' diplomatic correspondence, policy statements, press releases, opinions of government legal advisers, official manuals on legal questions (e.g., military manuals), executive decisions and practices, orders to military forces, comments by governments on ILC drafts and corresponding commentaries, legislation, international and national judicial decisions,

99. W. Michael Reisman & Eric E. Freedman, *The Plaintiff's Dilemma: Illegally Obtained Evidence and Admissibility in International Adjudication*, 76 AM. J. INT'L L. 737, 752 (1983).

100. TALLINN MANUAL 2.0, *supra* note 25, at 229.

101. *See* Colombian-Peruvian Asylum Case (Colom. v. Peru), Judgment, 1950 I.C.J. 266, 276–77 (Nov. 20).

102. *See* Case of the S.S. Lotus, *supra* note 46, at 28. Aspects of this section are drawn from BUCHAN, *supra* note 10, chapter 7.

103. *See* Wood, *supra* note 89, ¶ 37.

recitals in treaties and other international instruments (especially when in 'all States' form), extensive patterns of treaties in the same terms, practice of international organs, and resolutions relating to legal questions in UN organs, notably the General Assembly.[104]

State practice contains several distinct features. As the ICJ stipulates, State practice must be of a certain (a) duration and (b) generality and uniformity to establish this element of CIL.[105] This Article argues (c) that another element must also be present, namely, that State practice must be of a *public character*. This is significant in the case of peacetime espionage.

A. Duration

The traditional view is that it is inherent to the notion of *customary* international law that time must pass in order for a norm to transition into a binding rule; said otherwise, the State practice attendant to the putative rule must extend over a period of time.[106] Writing in 1961, Hart explained that customary law forms after a "slow process of growth, whereby courses of conduct once thought optional become first habitual or usual, then obligatory, and the converse process of decay, when deviations, once severely dealt with, are first tolerated and then pass unnoticed."[107] Yet, the modern formulation of the doctrine of customary international law has come to accept that customary rules can develop instantaneously.[108] For example, in the 1996 *Nuclear Weapons* advisory opinion the ICJ appeared sympathetic to the view that CIL can form where States vote overwhelmingly in favor of a General Assembly resolution that endorses or denounces a particular activity,[109] providing of course that this surge in State practice is accompanied by the belief that it is accepted as law. Consequently, the elements of generality, uniformity and public character are more important to the constitution of state practice than duration.

There is no doubt that most forms of espionage have a long history in international relations and according to one commentator "[e]spionage has existed since the dawn of human history."[110] Indeed, there are references to espionage in the Bible[111] and in the works of scholars writing in ancient Greece[112] and ancient China.[113] More to the point, States have performed

104. *Report of the International Law Commission: Seventieth Session*, *supra* note 88, Conclusion 6(2).

105. *See* North Sea Continental Shelf Cases (Federal Republic of Ger. v. Den.; Federal Republic of Ger. v. Neth.), Judgment, 1969 I.C.J. 4, ¶ 73 (Feb. 20).

106. *See* Robert Jennings, *Customary Law and General Principles of Law as Sources of Space Law*, *in* ENVIRONMENTAL ASPECTS OF ACTIVITIES IN OUTER SPACE: STATE OF THE LAW AND MEASURES OF PROTECTION (Karl-Heinz Böckstiegel ed., 1988).

107. HERBERT L.A. HART, THE CONCEPT OF LAW 92 (1961).

108. *See* CHENG, *supra* note 31, at 147.

109. *See* Legality of the Threat or use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 70 (July 8).

110. Ziolkowski, *supra* note 10, at 425. *See also* Scott, *supra* note 95, at 218 ("[E]spionage has been practised by the nations of the world for centuries.").

111. *See Joshua* 2:1.

112. *See* J. A. Richmond, *Spies in Ancient Greece*, 45 GREECE AND ROME 1, 1 (1998).

113. *See* Sun Tzu, THE ART OF WAR 144 (1981).

acts of espionage in violation of the principle of territorial sovereignty since this principle's inception at the Peace of Westphalia in 1648 and this practice has continued unabated into the contemporary era.[114] Similarly, the use of vessels for espionage purposes within the territorial sea of other States has been a common feature of international relations since the adoption of UNCLOS in 1982.[115] Also, States have conducted espionage against and from within diplomatic and consular missions for many centuries and especially since the codification of diplomatic and consular law in the 1961 VCDR and the 1963 VCCR.[116]

B. Generality and Uniformity

Next, acts of peacetime espionage must be of a certain generality and uniformity.[117] Given their overlap, the requirements of generality and uniformity can be considered together.[118] *Generality* contains two constituent elements. First, a precondition for the development of CIL is that State practice is "widespread"[119] within the international society. International law does not prescribe a specific number (or percentile) of States that must engage in an activity for it to be regarded as widespread. This being said, it is clear that a putative rule "need not pass the test of universal acceptance" for it be classified as CIL.[120] What is decisive is whether "[t]he practice must have been applied by the overwhelming majority of states which hitherto had an opportunity of applying it"[121] and that "[t]he available practice . . . [will be] so widespread that any remaining inconsistent practice will be marginal and without direct legal effect."[122] Thus, in the *North Sea*

114. *See* U.N. SCOR 858th mtg., *supra* note 28, at 12 (As China stated, espionage "has been practised from the beginning of organized society.").

115. *See* JAMES KRASKA, MARITIME POWER AND THE LAW OF THE SEA: EXPEDITIONARY OPERATIONS IN WORLD POLITICS 270–71 (2011); *See also* James Kraska, *Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters*, 54 COLUM. J. TRANSNAT'L L. 164, 164 (2015).

116. *See* Victor Colonieu, L'Espionnage au point de vue du droit international et pénal français [Espionage Under International Law and French Criminal Law] (our translation) (Dec. 27, 1888) (Doctoral Thesis, Lyon Faculty of Law, Paris, Librairie Nouvelle de Droit et de Jurisprudence), at 137 (observing as early as 1888 that diplomatic espionage was commonplace) (Fr.).

117. *North Sea Continental Shelf Cases*, *supra* note 105, ¶ 73. Article 38(1)(b) of the ICJ Statute also expressly defines CIL as a "general" practice accepted as law.

118. *See* David P. Fidler, *Challenging the Classical Concept of Custom: Perspectives on the Future of Customary International Law*, 39 GERMAN Y.B. INT'L L. 198, 202 (1996) (explaining, these requirements "meld together in a unitary analytical process. International lawyers cannot, for example, analyse whether State practice is general without having identified a practice that is uniform.").

119. Maritime Delimitation and Territorial Questions between Qatar and Bahrain (Qatar v. Bahr.), Judgment, 2001 I.C.J. 40, ¶ 205 (Mar. 16); *North Sea Continental Shelf Cases*, *supra* note 105, ¶ 73.

120. *See North Sea Continental Shelf Cases*, *supra* 105, at 229 (Dissenting Opinion of Judge Lachs).

121. Josef L. Kunz, *The Nature of Customary International Law*, 47 AM. J. INT'L L. 662, 666 (1953).

122. MARK E. VILLIGER, CUSTOMARY INTERNATIONAL LAW AND TREATIES: A MANUAL ON THE THEORY AND PRACTICE OF THE INTERRELATION OF SOURCES 30 (2d ed. 1997).

Continental Shelf Cases the ICJ rejected the existence of a customary rule on the basis that there were only 15 examples of State practice in support of the rule, which it said represented "a very small proportion . . . [of] the world as a whole."[123] Second, even where a State practice is widespread within the international society, it must also be "representative"[124] of its members for CIL to crystalize; "namely that States with different political, economic and legal systems, [and] States of all continents, [must] participate in the process."[125]

Uniformity requires States to formulate their claims to customary law in a manner that is materially analogous. This does not mean that "in the practice of States the application of the rules in question should have been perfect";[126] indeed, the ICJ has stressed "too much importance need not be attached to the few uncertainties or contradictions in state practice."[127] Rather, what is important is that State practice is "consistent"[128] and "concordant"[129] with the putative rule.

The inherently secretive nature of espionage makes it difficult to determine whether State practice of territorially intrusive forms of espionage satisfies the requirements of generality and uniformity.[130] However, the available evidence certainly points to this conclusion. Indeed, one commentator explains that there is a "tidal wave"[131] of State practice in favor of these forms of espionage. This claim is supported by the fact that States have on various occasions admitted that espionage is an integral feature of their relations. For example, in a Security Council meeting that was convened to discuss the legality of the US's use of spy planes within the territorial airspace of the USSR, Poland explained that "such activities are

123. *North Sea Continental Shelf Cases*, *supra* note 105, ¶ 75.

124. *Id.* ¶ 73.

125. *Id.* at 227 (Dissenting Opinion of Judge Lachs).

126. *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13, ¶ 186.

127. Fisheries Case (U.K. v. Nor.), 1951 I.C.J. 116, 138 (Dec. 18).

128. *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13, ¶ 186.

129. Fisheries Jurisdiction (U.K. v. Ice.), Judgment, 1974 I.C.J. 3, ¶ 16 (July 25). As an illustration, in the *Newfoundland* case the Supreme Court of Canada had to determine whether, by 1949, customary international law recognized that States possessed a sovereign right to explore and exploit the natural resources located in the continental shelf adjacent to their coastline. The Supreme Court identified approximately 15 examples of States claiming such a right. However, the Court was unable to conclude that this right had crystallized as customary law because the available State practice was not sufficiently large and, more importantly in the context of the present discussion, these claims were "far from uniform." For the Court, what was problematic was that while these States claimed a sovereign right to explore and exploit in the continental shelf, they differed as to the scope and depth to which this right extended. In the words of the Court, "[a] majority claimed not only the continental shelf, but also the superjacent waters. Some States claimed the geographic shelf to a limited depth; others claimed a limit of 200 miles from the coast, whatever the depth." In re Newfoundland Continental Shelf, [1984] 1 S.C.R. 86, 119 (Can.).

130. *See* Brown & Poellet, *supra* note 10, at 133 ("Despite the 'ungentlemanly' nature of espionage, it is an open secret that countries spy on friends and foes alike.").

131. Scott, *supra* note 95, at 221.

unfortunately the normal practice. Is there any country which is not involved and which would be entitled to cast the first stone?"[132] At the same meeting, China explained that "[e]spionage is not a new phenomenon; nor is it a rare phenomenon."[133]

While on the topic of spy planes that operate within the territorial airspace of other States, in the *Nicaragua* case Nicaragua accused the United States of violating its airspace on more than 900 occasions.[134] Similarly, in 1995 Libya officially complained before the Security Council that between 1975 and 1980 its airspace was exploited for the purpose of espionage over 150 times.[135] With regard to spying within the territorial sea, the case of Sweden stands out because it was reported that foreign submarines violated its territorial waters on at least 93 occasions between 1962 and 1980.[136]

In the cyber context, the Snowden leaks revealed that the United States and a number of other States had been engaged in a massive global cyber espionage campaign against various State and non-State actors.[137] It is telling that former French Foreign Minister Bernard Kouchner admitted that he was shocked by the international furor caused by the leaks, explaining "let's be honest, we [France] eavesdrop too. Everyone is listening to everyone else."[138] Also, in response to the Snowden leaks, President Obama explained: "Now let me be clear: our intelligence agencies will continue to gather information about the intentions of governments—as opposed to ordinary citizens—around the world, in the same way that the intelligence services of *every other nation does*."[139]

---

132. U.N. SCOR 858th mtg., *supra* note 28, at 2.

133. *Id.* at 12.

134. *Military and Paramilitary Activities in and against Nicaragua* (Nicar. v. U.S.), Memorial of Nicaragua, 1986 I.C.J. Pleadings, Oral Arguments, Docs. IV, 31, ¶ 120 (Apr. 30) ("[s]uch overflights have been conducted on a regular basis. During the preceding 10 months of 1984 alone, 996 overflights took place.").

135. *See* Letter Dated Aug. 1, 1980 from the interim Chargé d'Affaires of the Permanent Mission of the Libyan Arab Jamahiriya to the United Nations Addressed to the President of the Security Council, U.N. Doc. S/14094 Annex, at 3–4 (Aug. 6, 1980) (speaking of numerous "airspace violations and American terror and spying missions"); *see also* Address by the H.E. General Michel Aoun, President of the Republic of Lebanon, at the 72d session of the UN General Assembly (Sept. 21, 2017), available at https://goo.gl/ob2dyY [https://perma.cc/2UV9-7HS2] (condemning Israel for espionage and "at least 100 land, sea and air, violations to the Lebanese sovereignty each and every month.").

136. *See* Roma Sadurska, *Foreign Submarines in Swedish Waters: The Erosion of an International Norm*, 10 YALE J. INT'L L. 34, 35 (1984).

137. *See generally* Ed Pilkington, *Time Berners-Lee: Spies' Cracking of Encryption Undermines the Web*, THE GUARDIAN (Dec. 2, 2013), https://www.theguardian.com/technology/2013/dec/03/tim-berners-lee-spies-cracking-encryption-web-snowden [https://perma.cc/CM7U-BTYF] (providing an overview of the Snowden revelations).

138. Brett LoGiurato, *Former French Foreign Minister Nails it on the Outrage over US Spying on Foreign Leaders*, BUSINESS INSIDER (Oct. 24, 2013), https://www.businessinsider.com/nsa-spying-outrage-merkel-germany-obama-france-hollande-2013-10?IR=T [https://perma.cc/FN3T-YVRV].

139. Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) (emphasis added).

With specific regard to espionage against and from within diplomatic and consular missions, one document disclosed by Snowden listed 38 diplomatic missions and consular posts that the United States had identified as targets for espionage.[140] These reports were followed in October 2013 by allegations that Australian diplomatic and consular missions in Bangkok, Beijing, Dili, Hanoi, Kuala Lumpur and Port Moresby were engaged in cyber espionage activities.[141] In defense of these allegations, Australian Prime Minister Tony Abbott explained that "every government gathers information and . . . every government knows that every other government gathers information".[142] All in all, "[r]ecent news reports are rife with descriptions of spying conducted from within diplomatic posts."[143]

C. Public Character

So far, we have demonstrated that there is, at the very least, patchy and anecdotal evidence of extensive State practice of different forms of espionage in violation of different international law rules. But the fact remains that, because of its *inherent nature*, spying is a secret State practice. This is problematic in the context of custom because, as we will see, State practice must be public in character to inform the development of CIL.

International tribunals have recognized the difficulty of identifying CIL when State practice is conducted secretly. In the *Tadić* case, the International Criminal Tribunal for the former Yugoslavia (ICTY) sounded a word of caution regarding the identification of CIL in the context of armed conflict:[144]

> When attempting to ascertain State practice with a view to establishing the existence of a customary rule or a general principle, it is difficult, if not impossible, to pinpoint the actual behaviour of the troops in the field for the purpose of establishing whether they in fact comply with, or disregard, certain standards of behaviour. This examination is rendered extremely difficult by the fact that not only is access to the theatre of military operations normally refused to independent observers (often even to the ICRC) but information on the actual conduct of hostilities is withheld by the parties to the conflict; what is worse, often recourse is had to misinformation with a view to misleading the enemy as well as public opinion and foreign Governments.[145]

---

140. *See* Ewen MacAskill & Julian Borger, *New NSA Leaks Show How US is Bugging its European Allies*, THE GUARDIAN (June 30, 2013), https://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies [https://perma.cc/ZFM3-NETM].

141. *See* Philip Dorling, *Exposed: Australia's Asia Spy Network*, SYDNEY MORNING HERALD (Oct. 31, 2013), https://www.smh.com.au/politics/federal/exposed-australias-asia-spy-network-20131030-2whia.html [https://perma.cc/2BNZ-GZGX].

142. Tony Abbott, *Speech to Australian House of Representatives* (Nov. 19, 2013).

143. Deeks, *supra* note 10, at 312.

144. *See* Prosecutor v. Duško Tadić, Case No. IT-94-1-AR72, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, 55 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

145. Prosecutor v. Tadić, Case No. IT-94-AR72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 55 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

Given "the inherent nature of this subject-matter," the Court was of the view that customary international humanitarian rules must be extracted from more reliable forms of State practice and *opinio juris* such as official military documents produced by States.[146]

Reports produced by authoritative bodies have reached the same conclusion. For example, Principle 5 of the International Law Association's report into the formation of custom explains that "[a]cts do not count as practice if they are not public."[147] In the cyber context specifically, then Legal Advisor to the U.S. State Department Brian Egan explained that "States should publicly state their views" on how international law applies to cyberspace and that "[s]tating such views publicly will help give rise to more settled expectations of State behaviour and thereby contribute to greater predictability and stability in cyberspace."[148] That State practice must be of a public character to contribute towards the development of CIL was a recurrent theme in his speech.[149]

The rationale for this requirement is that customary rules develop according to an "iterative process of claim and response"[150] (or, in Shaw's words, "the process of claims and counter-claims")[151] between States.[152] When a State maintains that a norm has crystallized as CIL, it presents a claim to the international society that the practice in question is lawful. States are then provided with the opportunity to express their sovereignty and react to that claim. In particular, States can either accept the claim and contribute to the norm's customary development or reject the claim and frustrate its transposition into customary law. Even if the claim is accepted by a significant number of States and the norm crystalizes as customary law, a State can nevertheless identify itself as a persistent objector during that rule's development and thus opt out of the legal covenant that

146. *Id.* On the difficulty of identifying customary rules where State practice is conducted in secret, see *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13, ¶ 57 (June 27).

147. COMM. ON FORMATION OF CUSTOMARY (GEN.) INT'L LAW, INT'L LAW ASS'N, FINAL REPORT OF THE COMMITTEE: STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW 15 (2000). *See also* Wood, *supra* note 89, ¶ 47 (The Report on the identification of customary law notes that "[i]t is difficult to see how [secret state] practice can contribute to the formation or identification of general customary international law."); 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW xl (2005) (noting that acts do not "contribute to the formation of customary international law if they are never disclosed.").

148. Brian Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L LAW 169, 172 (2017).

149. *Id.*

150. Alexandra H. Perina, *Black Holes and Open Secrets: The Impact of Covert Action on International Law*, 53 COLUM. J. TRANSNAT'L L. 507, 567 (2015).

151. MALCOLM N. SHAW, INTERNATIONAL LAW 62 (8th ed. 2017).

152. *See* COMM. ON FORMATION OF CUSTOMARY (GEN.) INT'L LAW, *supra* note 147, at 10 ("It is often helpful to think of customary rules as emerging, in the typical case, from a process of express or implied claim and response."). *See also* Myres S. McDougal & N. A. Schlei, *The Hydrogen Bomb Tests in Perspective: Lawful Measures for Security*, 64 YALE L.J. 648 (1955) (explaining that the process of customary international law formation is one of continuous claim and response by sovereign equals).

is otherwise binding upon all other States.[153]

For these processes to occur, State practice must be committed publicly because it is only where State practice is "conspicuous"[154] and "detectable"[155] that States are able "to respond to [a putative customary rule] positively or negatively."[156] In consequence, it can be concluded that secret State practice is methodologically irrelevant[157] to the development of CIL,[158] unless it is subsequently disclosed to the international society.

Thus, *physical acts* of espionage committed in secret on the ground cannot be classified as State practice for the purpose of CIL formation.[159]

153. *See* Fisheries Jurisdiction (U.K. v. Nor.), Judgment, 1951 I.C.J. 116, 128 (Dec. 18). *See generally* JAMES A. GREEN, THE PERSISTENT OBJECTOR RULE IN INTERNATIONAL LAW (2016).

154. Shaw, *supra* note 151, at 59.

155. François Gény, *Méthode d'interprétation et Sources en Droit Privé Positif*, section 110 (1899), *quoted in* ANTHONY D'AMATO, THE CONCEPT OF CUSTOM IN INTERNATIONAL LAW 49 (1971).

156. Yoram Dinstein, *The Interaction between Customary Law and Treaties*, 322 COLLECTED COURSES OF THE HAGUE ACADEMY OF INT'L L. 1, 275 (2007) ("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."); Daniel Bethlehem, *The Secret Life of International Law*, 1 CAMBRIDGE J. INT'L & COMP. L. 23, 35–36 (2012) (explaining that State practice "must be public, at one level, for reasons of predictability, for reasons of accountability, for reasons of opposability, and for reasons of objection. So, at one level conduct must be public in order to be appreciable for reasons of the law."); Herman Meijers, *How is International Law Made? The Stages of Growth in International Law and the Use of Its Customary Rules*, 9 NETH. Y.B. INT'L L. 3, 19 (1978) ("States concur in the creation of law by not protesting, that is to say, by not reacting. If that is so, the states concerned must get an opportunity to react. From this there flow two further requirements for the formation of law: it must be possible to indicate at least one express manifestation of the will to create a law, and this express manifestation of will must be cognoscible for all states which will be considered as wishing to concur in the creation of the new rule if they do not protest."); Michael N. Schmitt & Liis Vihul, *The Nature of International Law Cyber Norms*, 5 THE TALLINN PAPERS 26 (2014) (Discussing CIL formation in cyberspace and observing "[u]ndisclosed acts cannot, as a practical matter, amount to state practice contributing to the emergence of customary international law.").

157. It is important to stress that secrecy does not mean that State conduct is illegal under international law, only that it cannot contribute towards the development of CIL. Whether secret State practice is lawful will depend upon the primary rules of international law that are implicated.

158. *See* COMM. ON FORMATION OF CUSTOMARY (GEN.) INT'L LAW, *supra* note 147, at 3 (explaining that, up until the end of the 19th Century customary law evolved incredibly slowly because diplomacy was largely conducted bilaterally and in secret). Reports suggest that States enter into 'spy agreements,' such as the Five Eyes agreement between the USA, Canada, Australia, New Zealand and the UK; Julian Borger, *'NSA Files: What's a Little Spying Between Old Friends?'*, THE GUARDIAN (Dec. 2, 2013), https://www.theguardian.com/world/2013/dec/02/nsa-files-spying-allies-enemies-five-eyes-g8 [https://perma.cc/H47W-L3R4]. These agreements are invariably concluded in secret. It is our contention that this type of State conduct does not constitute State practice for the purpose of CIL formation precisely because of its secret (that is, non-public) character. However, we express no view on whether secret treaties are permissible under international law. For further discussion, see generally Megan Donaldson, *'The Survival of the Secret Treaty: Publicity, Secrecy, and Legality in the International Order*,' 111 AMERICAN J. INT'L L. 575 (2017).

159. *But see* Lotrionte, *supra* note 12, at 475 (explaining that "[i]n the practice of states . . . as the Cold War evolved, espionage became a systematic, publicly recognized

As the International Law Association's report into customary law explains, "a secret physical act (e.g., secretly 'bugging' diplomatic premises) is probably not an example of the objective element [of State practice]."[160] In a similar vein, Khalil contends that "[acts of States] do not contribute [to the formation of international law] if they are conducted in secrecy and not communicated to other states, as is the case with spying".[161] On the inadmissibility of secret State practice in the context of espionage the views of Ratner are also edifying:

> With intelligence gathering . . . all the evidence is secret. How can we possibly even know how states are interpreting a treaty, or what they regard as a norm of custom, if they will not acknowledge what they are doing or whether and how they believe it is legal? Even if a state has an interest in acting according to law, it will not publicly reveal its interpretation and in many cases will have reasons to avoid public protest of claims by other states that it rejects.[162]

In sum, peacetime espionage is a practice that is often committed in secret, i.e., it is not disclosed to the international society. As a consequence, the *inherent nature* of this practice means that most of its manifestations cannot contribute to CIL formation. This being said, other forms of public State practice may exist to support the existence of customary exceptions.

1. Domestic Law Authorizing Acts of Peacetime Espionage

For many years States were able to cite and rely upon the threats and dangers that were prevalent within the world order to justify the secrecy that surrounded their espionage activities.[163] Due largely to the scale and pervasiveness of cyber-enabled espionage, in recent years the view has emerged that state-sponsored spying is "out of control"[164] and this has put pressure upon States—and in particular liberal democratic States—to ensure that the activities of their intelligence agencies are more transparent and subject to greater oversight.[165]

---

form of state activity essential to the conduct of international relations, with almost all countries actively engaging in the practice.").

160. COMM. ON FORMATION OF CUSTOMARY (GEN.) INT'L LAW, *supra* note 147, at 15. *See also id.* (noting that "[i]nternal memoranda are therefore not, as such, forms of State practice, and the confidential opinions of Government legal advisers, for instance, are not examples of the objective element of custom."); Andrea da Rocha Ferriera, et al., *Formation and Evidence of Customary International Law*, 1 UFRGS MODEL U.N. J. 182, 201 (2013) (Arguing "acts such as secret military instruction and internal memoranda would not count as State practice".).

161. Khalil, *supra* note 10, at 939.

162. Steven Ratner, *Introduction*, 28 MICH. J. INT'L L. 539, 539 (2007).

163. Remarkably, it was not until 1986 that the United Kingdom was prepared to publicly admit that MI6—its foreign intelligence agency—existed. *See* Luke Jones, *The Time When Spy Agencies Officially Didn't Exist*, BBC NEWS (Nov. 8, 2004), http://www.bbc.co.uk/news/magazine-29938135 [https://perma.cc/FH8X-HKZQ].

164. Jon Moran & Clive Walker, *Intelligence Powers and Accountability in the U.K.*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 289, 289 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016).

165. *See* Zachary K. Goldman & Samuel J. Rascoff, *Introduction*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY xvii (Zachary K.

Although actual instances of espionage on the ground have continued to be conducted in secret, States have adopted a plethora of measures to enhance the accountability of their intelligence agencies. In relation to this Article, the most important of these is that States have sought to provide a clear legal basis for the functions of their intelligence agencies and to delineate the extent of their powers within national law.[166] This has allowed for the—perhaps unique—emergence of public State practice concerning espionage.[167]

It is important to identify whether States have adopted publicly promulgated laws that provide their intelligence agencies with the legal authority to conduct espionage against other States because it is well accepted that "legislation is an important aspect of State practice."[168] According to the ILC, "[t]he term legislation is here employed in a comprehensive sense; it embraces the constitutions of States, the enactments of their legislative organs, and the regulations and declarations promulgated by executive and administrative bodies."[169]

Scholars have increasingly argued that public State practice in support of customary exceptions can be established on the basis that States have adopted domestic laws that authorize their intelligence agencies to engage in this conduct. Lotrionte, for example, explains that "[t]oday, many states have open laws that provide explicit details about the authorities and limitations that have been granted to intelligence organizations within the state."[170] Similarly, the Tallinn Manual 2.0 notes that "a number of States have by domestic law authorised their security services to engage in espionage, including cyber espionage."[171]

The terminology utilized by the Tallinn Manual 2.0 is startling because, to the best of our knowledge, no State has adopted domestic laws that explicitly invoke the concept of peacetime espionage when delineating the permissible functions of its intelligence services. This is a sharp contrast to the national (usually criminal) laws of many States that often use the term espionage to describe foreign nationals that collect confidential

---

Goldman & Samuel J. Rascoff eds., 2016) (arguing that "the oversight of intelligence agencies is undergoing major transformation."). *See generally* Alan Travis, *Snowden leak: governments' hostile reaction fuelled public's distrust of spies*, THE GUARDIAN (June 15, 2015), https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies [https://perma.cc/4GCN-ZLWV].

166. *See* Zachary K. Goldman & Samuel J. Rascoff, *Introduction*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY xvii–xviii (Zachary K. Goldman & Samuel J. Rascoff eds., 2016).

167. Further examples of public State practice relating to peacetime espionage could possibly be found in cases of exchange of spies and spying in international spaces. These will be the subject of future work.

168. Int'l Law Comm'n, Rep. of the International Law Commission covering its Second Session, U.N. Doc. A/1316, at 370 (1950).

169. *Id.*

170. Lotrionte, *supra* note 12, at 478. *See id.* ("Most domestic legal systems . . . seek to prohibit intelligence gathering by foreign agents while protecting the state's own capacity to conduct such activities abroad"); Chesterman, *supra* note 4, at 1072.

171. TALLINN MANUAL 2.0, *supra* note 25, at 169.

political information within their borders.[172]

Of course, espionage is merely a concept. What is important is that we look at the substance of domestic laws and determine whether States have clearly authorized internationally wrongful acts of espionage. The United States provides a vivid illustration of a State that confers upon its intelligence agencies ample legal authority to collect foreign intelligence. For example, Section 102 of the Foreign Intelligence Surveillance Act of 1978 (FISA) provides that, "[*n*]*otwithstanding any other law*, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information" from persons, facilities or property located within the US.[173]

This provision is interesting in the context of this Article because, when the FISA bill was being debated by the Senate Committee on Intelligence before it was enacted as law, the Committee recognized the view that the activities authorized by Section 102 may violate the US's international legal obligations under the VCDR, such as where United States intelligence services collect intelligence from diplomatic missions located within the US.[174] In response, the Committee noted that "the 'notwithstanding any other law' language is intended to make clear that, notwithstanding the Vienna Convention [on Diplomatic Relations], the activities authorized by this bill may be conducted."[175] Thus, as far as the Committee was concerned, Section 102 provides intelligence agencies with clear legal authority to conduct electronic surveillance against diplomatic missions notwithstanding the fact that such conduct contravenes the VCDR.

Whereas "traditional FISA"[176] authorizes and regulates the collection of foreign intelligence within the US, Executive Order 12333 (issued in 1981) authorizes intelligence agencies to collect intelligence from targets located outside of the US.[177]

In 2008 the FISA Amendments Act (FAA) was adopted.[178] Sections 703 and 704 FAA provide intelligence agencies with the legal authority to target U.S. persons located outside of the United States whereas Section 702 provides legal authority to target non-U.S. persons located outside of the United States with the compelled assistance of communications service providers.[179] The FAA has therefore expanded the scope of FISA, incorporating within its framework intelligence activities that had previously been conducted pursuant to Executive Order 12333. Thus, Executive Order 12333 now operates residually, only applying in those circumstances that

172. *See, e.g.*, U.S. Espionage Act, H.R. 291, 65th Cong. (1917) (enacted); Criminal Code Amendment (Espionage and Related Matters) Act 2002 (Austrl.)

173. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1802 (1978) (emphasis added).

174. H.R. Rep. No. 95-1283, pt. 1, at 70 (1977).

175. *Id.*

176. "Traditional FISA" is the name given to FISA before it was amended in 2008. *See* Director of National Intelligence, The FISA Amendments Act: Q&A (Apr. 18, 2017), at 1.

177. Exec. Order No. 12,333, 46 Fed. Reg. 59, 941 (Dec. 4, 1981).

178. FISA Amendments Act of 2008, Pub. L. No. 110-261, 112 Stat. 2436(2008).

179. *Id.* §§ 702–04.

are not covered by FISA and FAA,[180] such as the collection of information from targets outside of the United States without the compelled assistance of communications service providers.[181]

In addition, legislative developments in Canada provide the Canadian Security Intelligence Service (CSIS) with clear legal authority to collect confidential information. The Canadian example is particularly interesting given that in 2008 the Federal Court of Canada held that the CSIS could not undertake espionage operations within the territory of another State because it was internationally wrongful and the authorizing legislation did not set aside Canada's international legal commitments.[182] Partly in response to that decision,[183] in 2015 Canada introduced various amendments to the *Canadian Security Intelligence Service Act* 1984.[184] Section 12(1) of this Act was amended to read that "[t]he Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada," and under Section 12(2) the intelligence agency is expressly authorized to perform this function "within or outside Canada."[185] Section 21(3.1) was amended to permit the CSIS to seek and obtain a warrant from the Federal Court for surveillance in foreign States, which reads, "[*w*]*ithout regard to any other law, including that of any foreign state,* a judge may, in a warrant issued under subsection (3), authorize activities outside Canada to enable the Service to investigate a threat to the security of Canada."[186]

---

180. THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 70 (Dec. 12, 2003).

181. Mention should be made here of Presidential Policy Directive 28, which was issued by President Obama in response the fallout from the Snowden revelations. PPD-28 does not provide new legal authority for the collection of signals intelligence but instead reiterates that such conduct can only be pursued where it is authorized by law. *See* Press Release, White House Office of the Press Secretary, Presidential Policy Directive—Signals Intelligence Activities (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/LMW8-K7HZ] (The contribution of PPD-28 is that it sets "new limits . . . [which] are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside." These limits restrict the use of signals intelligence to detecting and countering six types of actual threats: (1) espionage; (2) terrorism; (3) weapons of mass destruction; (4) cyber security; (5) threats to U.S. or allied military personnel; and (6) transnational criminal threats.").

182. *See* Canadian Security Intelligence Service Act (Re), [2008] F.C. 301 (Can.). *See also* Craig Forcese, *The Federal Court's Prescience: Spying and International Law*, NAT'L SECURITY L.: CANADIAN PRACTICE IN COMPARATIVE PERSPECTIVE (Nov. 21, 2013), http://craigforcese.squarespace.com/national-security-law-blog/2013/11/21/the-federal-courts-prescience-spying-and-international-law.html [https://perma.cc/XW4J-E8LK].

183. Protection of Canada from Terrorists Act, 2014-15, H.C. Bill C-44, c. 9. For an overview of these legislative developments, see CRAIG FORCESE & KENT ROACH, FALSE SECURITY: THE RADICALIZATION OF CANADA'S TERROR LAWS 3-7 (2015).

184. *See id.*

185. *See id.*

186. *See id.* (emphasis added). In response to these developments, Forcese explains that "I have never seen (and I have started looking in earnest) a state codify so clearly in

Other States have also implemented laws that permit the collection of information abroad—which also presumably includes information from closed sources—where necessary to maintain national security.[187] This was recognized by the UN Special Rapporteur on the Right to Privacy when he explained that "a number of States have begun to adopt laws that purport to authorize them to conduct extra-territorial surveillance or to intercept communications in foreign jurisdictions";[188] the Special Rapporteur went on to note that "[t]hese developments suggest an alarming trend towards the extension of surveillance powers beyond territorial borders."[189]

The language employed by the Special Rapporteur is significant and requires emphasis: for now, there is only a "trend" being set by "a number of States" towards the adoption of domestic laws that authorize espionage abroad. It is also apparent that the majority of States that have adopted these types of laws are organized upon a liberal democratic basis, indicating that the available State practice is far from representative of all segments of the international society. The Tallinn Manual 2.0 also records that "a number of States" have adopted domestic laws that authorize their intelligence agencies to conduct espionage abroad but, tellingly, it only cites 6 examples to support this contention, all of which are liberal democracies from Europe (namely, Austria, Germany, the Netherlands, the United Kingdom, Sweden and Switzerland).[190]

The takeaway point is that mere trends in State practice do not give rise to customary rules.[191] Of course, if other States adopt domestic laws authorizing espionage abroad, public State practice will accumulate. But it

---

its law books that it's organs will authorize spying in another state, regardless of the law of that state. States spy all the time, of course. But this is real Canadian honesty. I think I admire that." Craig Forcese, *A Longer Arm for CSIS: Assessing the Extraterritorial Spying Provisions*, NAT'L SECURITY L.: CANADIAN PRACTICE IN COMPARATIVE PERSPECTIVE (Oct. 28, 2014), http://craigforcese.squarespace.com/national-security-law-blog/2014/10/28/a-longer-arm-for-csis-assessing-the-extraterritorial-spying.html/ [https://perma.cc/NGH9-GLGM].

187. *E.g.*, New Zealand Security Intelligence Service Act 1969, s 4AA (N.Z.); *Intelligence Services Act 2001* (Cth) ss 6–7 (Austl.); Security Authorities Act 2000, § 7(1)(1) (Est.); Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, § 2(a) (B.O.E. 2002, 8628) (Spain); Legge 3 agosto 2007, n.124, in G.U. Aug. 13, 2007, n.187, § 6(2) (It.); Denmark Act, No 602, § 3(2), 12 June 2003 (Den.).

188. Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶ 64, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013).

189. *Id.* ¶ 64.

190. TALLINN MANUAL 2.0, *supra* note 25, at 169.

191. An analogy can be made to the *In re Newfoundland Continental Shelf* case. As explained above, in this case the Supreme Court had to determine whether CIL conferred upon States the right to explore and exploit in the continental shelf that runs along their coastline. The Court found that national laws can constitute instances of State practice for the purpose of CIL formation and proceeded to identify around 15 national laws where States had claimed the right to explore and exploit in the continental shelf. Importantly, the Court rejected the customary status of this right on the basis that the sample of available State practice was too small or, in the words of the Court, '[not] sufficiently widespread to constitute a general practice'; *In re Newfoundland Continental Shelf*, *supra* note 129, at 124. In light of this, at present there are too few

is only where this State practice becomes widespread within, and representative of, the international society that it can support the existence of customary espionage exceptions.

IV. *Opinio Juris*

Even if there is widespread and representative public State practice of espionage, it is still necessary to show that this practice is coupled with "evidence of a belief that this practice is rendered obligatory by the existence of a rule of [customary] law requiring it" (*opinio juris*).[192] This "psychological factor"[193] is critical in order to "distinguish between those practices of States that result merely from political expedience, diplomacy, domestic policy, or habit—that is, those practices that neither create nor evidence legal obligations—and those that flow from legal obligations."[194] In the absence of *opinio juris* there is no CIL but mere "usage."[195] Evidence of *opinio juris* can be gleaned from a variety of sources, including diplomatic correspondence, case law of national courts, opinions of government legal advisers, treaty practice and their *travaux préparatoires*, diplomatic protests or claims in legal briefs before courts and tribunals.[196]

In the *Nicaragua* case the ICJ considered under what circumstances CIL can give rise to customary exceptions, which is the issue under examination here. The ICJ noted that where,

> A state acts in a way prima facie incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State's conduct is in fact justifiable on that basis, the significant of that attitude is to confirm rather than to weaken the rule.[197]

The Court accepted, however, that customary exceptions to primary rules could form if the pioneer State *expressly claims* that its conduct creates a new legal right under customary law and this claim is "shared in principle by other States."[198] In essence, the ICJ is saying that pioneer States must explicitly claim new rights under CIL before customary exceptions to primary rules can be carved out.

---

instances of domestic laws authorizing espionage abroad to conclude that there is a general practice in favor of this activity.

192. *Id.* ¶ 77.

193. Shaw, *supra* note 151, at 55.

194. JOHN H. CURRIE, PUBLIC INTERNATIONAL LAW, ESSENTIALS OF CANADIAN LAW 170 (2001). *See also Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13, ¶ 206 (The ICJ noted that "[t]he United States authorities have on some occasions clearly stated their grounds for intervening in the affairs of a foreign State for reasons connected with, for example, domestic policies of that country, its ideology, the level of its armaments, or the direction of its foreign policy. But there were statements of international policy, and not assertions of rules of existing international law.").

195. *Id.* at 170.

196. *See Report of the International Law Commission: Seventieth Session*, *supra* note 88, Conclusion 10(2).

197. *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13, ¶ 186.

198. *Id.* ¶ 207.

Little to no *opinio juris* supports the existence of customary espionage exceptions. In considering *opinio juris*, we first (a) outline States' view towards peacetime espionage generally before turning (b) to States' reactions to specific spying incidents which violate international law; we will treat the subject from an historical standpoint, since the un-crystalized state of CIL on espionage can only be understood in light of the discrete treatment it has undergone in centuries past; and (c) we will complete this discussion by looking at other sources of *opinio juris*.

A. The Policy of Silence

Few scholars have explored the attitude of States towards espionage and, of those that have, they have tended to find *opinio juris* in mere policy statements rather than legal assertions.[199] This is a significant misstep because, as one of the present authors has contended elsewhere, States have adopted a *policy of silence* (POS) when it comes to their espionage activities.[200] POS is the name given to a discrete process whereby States circumvent the resolution of incidents arising from acts of espionage by pursuing solutions in multiple branches of international law rather than pursuing a CIL of espionage. This stifles *opinio juris* on the subject.

States' silence about spying is remarkable and evidenced in at least two ways. First, States have had the opportunity to express *opinio juris* on peacetime espionage on multiple occasions. Given the number of times the issue has arisen—before UN bodies such as the General Assembly and the Security Council, in cases before the ICJ or discussions within the ILC—one would expect States to have set forth their views on the matter, even if they fell short of regulating espionage conventionally. The fact is, States have very much shied away from this discussion, thereby precluding customary espionage exceptions from emerging.

Second, States have been careful to regulate peacetime espionage through a *patois* of legal euphemisms ('acts incompatible with the diplomatic function'; 'non-innocent passage'; 'flights inconsistent with the aims of the Convention'; 'peaceful purposes', etc.)—that is, States have made "an almost conscious effort to avoid a solution in *terms of espionage*."[201] The practical effect of this *patois* is to allow States to discuss and even condemn espionage activities without making public their *opinio juris* about espionage conducted through different means. The following section will illuminate the existence of this POS and show how it stifles the emergence of customary espionage exceptions.

---

199. For further discussion on *opinio juris see* Navarrete, *supra* note 10, at 17.

200. *See id.* (noting that "[l]a politique du silence ne permet pas de développer des normes prohibitives ou permissives incrémentales.") ["[t]he policy of silence does not permit the incremental development of prohibitive or permissive legal rules relating to espionage."] (our translation); Forcese, *supra* note 14, at 68.

201. Edmondson, *supra* note 28, at 446 (emphasis added).

1. Air Law

Air law offered the first possibility to deal with peacetime espionage. At the beginning of the twentieth century, States considered the possibility of protecting their sovereignty through a sovereign right granted expressly for the repression of espionage[202] in a regime of free, open skies. Instead, they ultimately created a highly restricted regime of air law in which any trespass into a nation's airspace violates international law.[203] Injured States are thus free to condemn solely unauthorized entries, or to brand them in terms of espionage to obtain diplomatic gains.[204] In the wake of the 1983 KAL 007 incident, States had the chance to revisit the question of whether they should address espionage explicitly within the context of air law. The Korean plane—allegedly a spy-plane working on behalf of the USA[205]—was shot down by the USSR when it deviated into USSR airspace for unknown reasons, resulting in the loss of 269 civilian lives.[206] As a result, States adopted an amendment to the Chicago Convention, according to which States must refrain from using force against civil aircrafts in flight and are entitled to require their landing when the aircrafts are being used for "any purpose inconsistent with the aims of the Convention."[207]

202. The first important proposal on the subject of the legal status of the airspace above national territory came from French legal scholar Fauchille, who proposed a doctrine of freedom of the air, subject to conservation rights in subjacent States, including a right to suppress espionage. *See* Paul Fauchille, *Régime juridique des aérostats*, 19 ANNUAIRE DE L'INSTITUT DE DROIT INT'L 19 (1902). *See also* Note, *Legal Aspects of Reconnaissance in Airspace and Outer Space*, 61 COLUM. L. REV. 1074, 1076 (1961); Institut de Droit International, *Resolution on the Law of the Air*, 19 INSTITUT DE DROIT INT'L Y.B. 32, art. 7 (1902); Michel Tremblay, The Legal Status of Military Aircraft in International Law (Nov. 2003) (thesis submitted to McGill University, Faculty of Law, Institute of Air and Space Law), at 22.

203. Chicago Convention on International Civil Aviation, *supra* note 44 (reaffirming the principle of State sovereignty of national airspace). On the history of the Convention, see DEP'T OF DEF., OFF. GEN. COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 2 (1999).

204. *See* Fabien Lafouasse, *L'espionnage en droit international*, 47 ANNUAIRE FRANÇAIS DE DROIT INT'L 63, 123 (2001).

205. *See generally* John T. Phelps II, *Aerial Intrusions by Civil and Military Aircraft in Time of Peace*, 107 MIL. L. REV. 255, 302 (1985); Suzette V. Suarez, *Korean Air Lines Incident (1983)*, OXFORD PUB. INT'L L. (Dec. 2007), http://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e1183?rskey=LQLRHI&result=13&prd=EPIL [https://perma.cc/JZP6-3QKE]; Dale Stephens & Tristan Skousgaard, *Military Reconnaissance*, OXFORD PUB. INT'L L. (May 2009), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e335 [https://perma.cc/S5E9-E493]; Emilia Chiavarelli, The KAL 007 Incident: The Legal Effects of ICAO Decisions 49 (1984) (thesis Submitted to McGill University, Faculty of Law, Institute of Air and Space Law), at 49.

206. Chiavarelli, *supra* note 205, at 200.

207. Chicago Convention on International Civil Aviation, *supra* note 44, art. 3bis. *See also* Robin Geiβ, *Civil Aircraft as Weapons of Large-Scale Destruction: Countermeasures, Article 3BIS of the Chicago Convention, and the Newly Adopted German "Luftsicherheitsgesetz"*, 27 MICH. J. INT'L L. 227, 239 (2005) ("The events which led to the adoption of article 3bis were largely interstate incidents in which civil aircraft had trespassed sovereign airspace, overflown military sensitive areas, and were suspected of being engaged in espionage on behalf of their state of registration.").

Unsurprisingly, this new phrase on 'inconsistent purposes' became the proxy by which States alluded to espionage activities during meetings. At least one State felt compelled to tackle the issue of espionage expressly by defining the phrase with a list of prohibited activities, including "acts of espionage,"[208] but States did not retain this proposal. Taking up this point, one delegate expressly referred to POS, noting that "[a]ll the proposed amendments [are] one sided in the sense that almost no emphasis [is] laid on the prohibition of States from resort to the use of aviation for espionage."[209] In the delegate's view, it was important that the amendment deter States from spying, otherwise "any amendment, no matter how beautifully it might be framed, [would be] nothing but a toothless bulldog."[210] Yet, most States remained impervious to this outcry.

2. Law of the Sea

States displayed a similar attitude in sketching the notion of 'innocent passage' in territorial waters. Article 19(2)(c) UNCLOS makes espionage inherently non-innocent.[211] Importantly, however, States avoided discussing peacetime espionage.[212] The history of the drafting of Article 19(2)(c) is more than revealing on this point. In 1973, Fiji presented a series of draft articles that supplied a list of "activities" that could render the passage non-innocent, including a new paragraph (f) describing "any act of *espionage* affecting the defence or security of the coastal State."[213] But interestingly, States opted for the wording "any act aimed at collecting information," which was later enshrined into UNCLOS in preference to the term 'espionage.' Presumably, States intentionally left the terms ambiguous to paper over the differences in their views, or perhaps, simply because they did not wish to discuss espionage. At any rate, this language allows States to condemn "non-innocent" passages in territorial waters[214] (a clear

208. During the 25th (extraordinary) Session of the ICAO Assembly on April 30, 1984, Cuba defined 'acts inconsistent with the aims of the Convention' as "[a]cts of aggression, infiltration or espionage involving discharge of harmful substances or pathogenic agents; transport of contraband or prohibited traffic using the airspace of another State, even with destination to a third State or with any other purpose inconsistent with the aims of the Convention." *See* Int'l Civil Aviation Org. [ICAO], *Minutes of the Sixth Meeting. Monday, 30 April 1984*, at 9, ICAO Doc. A25-Min. EX/6 (1984). *See also* RUWANTISSA ABEYRATNE, CONVENTION ON INTERNATIONAL CIVIL AVIATION: A COMMENTARY 75 (2014).

209. ICAO, *Minutes of the Seventh Meeting. Tuesday, 1 May 1984*, at 11, ICAO Doc. A25-Min. EX/7 (1984).

210. *Id. But see*, ICAO, *Minutes of the Sixth Meeting*, *supra* note 208, at 13 (Chief delegate of the USSR stating that acts of intelligence gathering should be included in the definition of intruder aircraft).

211. *See* Kraska, *supra* note 67, at 219.

212. *See* GEORGE K. WALKER, DEFINITIONS FOR THE LAW OF THE SEA: TERMS NOT DEFINED BY THE 1982 CONVENTION 228 (2011).

213. *See* Navarrete, *supra* note 10, at 6. *See also* CARLOS ESPALIÚ BERDUD, LE PASSAGE INOFFENSIF DES NAVIRES DE GUERRE ÉTRANGERS DANS LA MER TERRITORIALE 42 (2007).

214. That is, the exercise of a conditional right. *See* Sam Bateman, *Security and the Law of the Sea in East Asia: Navigational Regimes and Exclusive Economic Zones*, *in* THE LAW OF THE SEA: PROGRESS AND PROSPECTS 365, 367 (David Freestone, Richard Barnes & David M. Ong eds., 2006).

legal euphemism) without having to discuss espionage.

How does this translate into practice? On the rare[215] occasion that a coastal State takes the necessary steps to prevent the passage of a foreign ship conducting espionage in its territorial sea,[216] "[t]he spying state is compelled to justify the innocence of its passage and the aggrieved state minimizes the risk that it will be estopped from raising the issue by its own espionage that is conducted in a different manner."[217] The outcome, then, is that States have remained silent on the thorny question of espionage and employed a *patois* that shuns a legally loaded label.

3. *Diplomatic and Consular Law*

Diplomatic relations have always been the playground of euphemisms. As noted earlier, the VCDR "both implicitly accept[s] limited intelligence gathering as an inevitable element of diplomacy and explicitly grant[s] an absolute discretion to terminate that relationship at will."[218] The key point is that when States are caught spying, it is dealt with entirely within what the ICJ, in its *Tehran Hostages* dictum, described as a "self-contained regime."[219] Much like the innocent-passage regime, this regime provides its own remedies and legal euphemisms, thus allowing the emergence of a practice where States justify their actions with reference to appropriate and inappropriate activities—and not espionage.[220] As such, receiving States can, and often do, declare diplomats *persona non grata* for "activities incompatible with their diplomatic status" (another euphemism for spying).[221]

Additionally, States have shown an unmistakable POS when discussing diplomatic espionage, even though routine abuse of the VCDR may lead to its desuetude.[222] Thus, during a 1984 meeting of the ILC on the status of the diplomatic bag and courier, one delegate noted that he "had been struck by the fact [that the discussion on espionage] had come up for con-

215. *See id.* at 368 (as Bateman notes, the covert nature of these acts makes them difficult to detect for coastal states).

216. *See* UNCLOS, *supra* note 42, art. 25.

217. Edmondson, *supra* note 28, at 446.

218. Simon Chesterman, *Secret intelligence*, OXFORD PUB. INT'L L. (Jan. 2009), ¶ 11, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e992 [https://perma.cc/GT62-F3BA].

219. Case Concerning United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, ¶ 86 (May 24). While the particular wording of the ICJ's dictum has been severely criticized by some as a jurisprudential 'overkill,' the fact remains that the VCDR provides special remedies in reaction to abuses of the diplomatic function. For a critique of the Court's dictum, see Bruno Simma & Dirk Pulkowski, *Of Planets and the Universe: Self-contained Regimes in International Law*, 17 EUR. J. INT'L L. 484 (2006).

220. *See* Chesterman, *supra* note 4, at 1089.

221. VCDR, *supra* note 26, art. 9(1); *see* Robert Windrem, *How does the U.S. decide which Russians to throw out of the country?*, NBC NEWS (Mar. 29, 2018), https://www.nbcnews.com/news/us-news/how-does-u-s-decide-which-russians-throw-out-country-n860916 [https://perma.cc/R4VQ-TVPG] (explaining common terms relating to espionage).

222. *See* Navarrete, *supra* note 10, at 7, 44.

sideration *only at the present time*. The international community *had obviously been avoiding any discussion . . . for a long time*," adding that this was understandable because "[n]o one was completely innocent. . . . Everyone was trying to find out what others were doing; everyone engaged in that exercise, but everyone denied it."[223]

Regarding consular relations, it would seem that the subject of espionage never even raised its head in the *travaux préparatoires* of the VCCR. At least, that is what a Pakistani Agent asserted in a rare statement before the ICJ in the *Jadhav* case.[224] Discussing the elaboration of the VCCR, the Agent argued that "[t]here is no reference to espionage [or] spying . . . in the *travaux* [because] not that long ago [the] Soviet Union and the United States of America were engaged in what is known as the Cold War, and *we all accepted the fiction that there were no spies*."[225] If this bold remark was made in the context of the applicability of consular rights to an alleged spy,[226] the POS is explicit. This statement reinforces the idea that States have long regarded espionage as a "dirty word."[227]

4. Space Law

With the making of the *Outer Space Treaty*,[228] States once again had the opportunity to express their views about espionage and reconnaissance conducted in outer space. It is telling that many States expressed unease in discussing espionage during meetings and explained that prohibiting such

223. Int'l Law Comm'n, *Status of the diplomatic courier and the diplomatic bag not accompanied by the diplomatic courier*, Summary Record 1845th Meeting, U.N. Doc. A/CN.4/SR.1845, at 185–186 (1984).

224. *See* Jadhav (India v. Pak.), Provisional Measures, 2017 I.C.J. 231, 242 (May 18).

225. Jadhav Case (India v. Pak.), Verbatim Record, 2017 I.C.J. 168 (May 15, 2017, 3 p.m), at 20, available at http://www.icj-cij.org/files/case-related/168/168-20170515-ORA-02-00-BI.pdf [https://perma.cc/BGK4-2X75]. *But see, e.g.*, Int'l Law Comm'n, Documents of the Twelfth Session, U.N. Doc. A/CN.4/131, A/CN.4/L.86, at 58, *reprinted in* [1960] 2 Y.B. INT'L L. COMM'N 52, U.N. Doc. A/CN.4/SER.A/1960/ADD.1 (where members of the ILC considered whether it might be desirable that local authorities not be obligated to inform the consul in cases of espionage). This point was further developed in the oral proceedings. *See* Jadhav Case (India v. Pak.), Verbatim Record, 2019 I.C.J. (Feb. 19, 2019, 10 a.m.), at 41 (noting that States had adopted a position of "studied ambiguity," with the consequences that it cannot be said that there is a general practice accepted as law by States to provide consular access in cases where espionage was reasonably suspected), available at https://www.icj-cij.org/files/case-related/168/168-20190219-ORA-01-00-BI.pdf [https://perma.cc/9XD5-T4M3].

226. It is argued that Article 36 VCCR provides for a customary international law exception with regards to espionage, i.e., that receiving States do not have to provide consular access in cases of espionage. Given that no express reservation was made in Article 36 VCCR for charges of espionage, and the apparent lack of consistent State practice in this regard, the existence of such an exception is open to question. *See generally* Nicole M. Howell, *A Proposal for U.S. Implementation of the Vienna Convention's Consular Notification Requirement*, 60 UCLA L. REV. 1324, 1336 (2013); Cindy Galway Buys, *Reflections on the 50th Anniversary of the Vienna Convention on Consular Relations*, 38 S. ILL. U. L.J. 57, 63 (2013).

227. Chesterman, *supra* note 4, at 1076.

228. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

activity was a top-level political decision.[229] States found a way out of this awkward discussion through artful ambiguity. Until 1963, the USSR and other Soviet Bloc countries[230] held that reconnaissance activities conducted in outer space were illegal under international law. Indeed, the USSR took the lead on at least two occasions to prohibit[231] or regulate[232] these activities. (This was, of course, only lip service, as the USSR ultimately used its 'scientific' satellites to spy). By contrast, the United States held that reconnaissance from points outside the territory of any state was legal, a view shared by its allies such as Australia[233] and the United Kingdom.[234] Evidently, the problem for States, then, was how to frame the issue so as to not forestall ratification of the Treaty, while allowing the two superpowers to uphold their opposing views about espionage.

States found the answer in Article IV of the Treaty, which has been dubbed a "masterpiece of legal *trompe-l'oeil*."[235] It provides that "[t]he

229. *See* Comm. on the Peaceful Uses of Outer Space, 17th Sess., 11th mtg. at 5, 234, U.N. Doc. A/AC.105/C.2/SR.11 (Aug. 21, 1962) ("A decision to alter the law [on espionage] in that regard, by requiring all states to wave their legal rights, would be a top level political decision and therefore all together outside the competence of the Legal Sub-Committee to take on its own initiative. . . . The Legal Sub-Committee . . . should not allow itself to be tempted by the ambition to take up subjects that were beyond its competence or that had already been referred to other international bodies, as for example the question of . . . so called 'intelligence' activities.").

230. *See, e.g.*, U.N. GAOR, 17th Sess., 1294th mtg. at 238, U.N. Doc. A/C.1/SR.1294 (Dec. 7, 1962) (where the delegate of Czechoslovakia stated that "[i]nternational law could not, indeed, authorize in outer space acts which it prohibited on earth or in the atmosphere"); *id.* at 240 (where the delegate of the Ukrainian Soviet Socialist Republic considered that the use of space for obtaining intelligence data was inadmissible).

231. *See* Comm. On the Peaceful Uses of Outer Space, USSR: Draft Declaration of the Basic Principles Governing the Activities of States Pertaining to the Exploration and Use of Outer Space, U.N. Doc. A/AC.105/L.02 (Sept. 10, 1962), art. 8 ("The use of artificial satellites for the collection of intelligence information in the territory of foreign States is incompatible with the objectives of mankind in its conquest of outer space."). *See also* McMahon, *supra* note 32, at 373.

232. The USSR introduced a proposed agreement for assistance to astronauts and spacecraft landing in foreign territory in the Legal Subcommittee. *See* Comm. on the Peaceful Uses of Outer Space, USSR: Draft International Agreement on the Rescue of Astronauts and Spaceships Making Emergency Landings, U.N. Doc. A/AC.105/12 (May 6, 1963), art. 7 ("Space vehicles aboard which devices have been discovered for the collection of intelligence information in the territory of another State shall not be returned."). *See also* John Cobb Cooper, *Current Developments in Space Law*, 41 N.C. L. REV. 339, 343 (1963).

233. *See* Comm. on the Peaceful Uses of Outer Space, 17th Sess., 11th mtg., *supra* note 229, at 5 ("It would seem absolutely clear that to obtain information about the earth by means of a space vehicle did not *per se* involve any breach of international law.").

234. *See* Comm. on the Peaceful Uses of Outer Space, 17th Sess., 10th mtg. at 4, U.N. Doc. A/AC.105/C.2/SR.10 (Aug. 21, 1962) ("[T]he United Kingdom held that observation from points outside the territory of any State was not contrary to international law.").

235. Bin Cheng, *Properly Speaking, Only Celestial Bodies Have Been Reserved for Use Exclusively for Peaceful (Non-Military) Purposes, but Not Outer Void Space*, *in* INTERNATIONAL LAW ACROSS THE SPECTRUM OF CONFLICT: ESSAYS IN HONOUR OF PROFESSOR L.C. GREEN ON THE OCCASION OF HIS EIGHTIETH BIRTHDAY 81, 88 (Michael N. Schmitt ed., 2000).

moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes."[236] With this piece of legal acrobatics, the issue became not whether "espionage" was legal, but whether the use of reconnaissance satellites from outer space fell within the realm of "peaceful purposes." The sticking point of the analysis thus became defining "peaceful purposes." States were of course content with ambiguity,[237] as they were able to uphold their respective views on the legality (peaceful means "non-aggressive") or illegality (peaceful means "non-military") of intelligence gathering in outer space while not discussing espionage generally.[238] As time wore on, States agreed this to be a peaceful use protected by international law.[239]

In sum, espionage has come to represent a "dirty word" within international relations.[240] States have had the opportunity to discuss specific acts of espionage or espionage generally on multiple occasions; and yet they have offered no granular expressions on the subject. Taking a closer look, we must also realize that States have purposively constructed the necessary *patois* to preclude the formation of *opinio juris* on espionage. This suggests that States have been assiduously careful that conventional developments in peacetime espionage did not spill over into CIL. This is significant because customary exceptions cannot emerge from mere silence.

Does this silence mean that States deem most forms of espionage unlawful? To be sure, it is difficult to make assumptions based on this POS because silence may denote "indifference, conscious non-participation in something considered illegal, lack of technical capacity, political maneuver or whatever."[241] It is therefore necessary to turn to States' reactions to international incidents involving espionage.

B. The Process of Claims and Counterclaims

As we have seen in the *Nicaragua* case, for a customary exception to emerge, pioneer States must have formulated their claim in *legal* terms and other States must have accepted that claim as law.[242] This process is some-

236. *See id.* at 95.

237. *See* Frans G. von der Dunk, *Customary International Law and Outer Space*, *in* REEXAMINING CUSTOMARY INTERNATIONAL LAW 346, 361 (Brian D. Lepard ed., 2017) (speaking of the intentional vagueness of the clause). *See also* Craig Forcese, *Creative Ambiguity– International Law's Distant Relationship with Peacetime Spying*, JUST SECURITY (Nov. 14, 2013), https://www.justsecurity.org/3168/guest-post-creative-ambiguity-international-laws-distant-relationship-peacetime-spying/ [https://perma.cc/S2R6-GZ8P]. *But see* Navarrete, *supra* note 10, at 17 (stating that creative ambiguity is only one facet of States' approach to peacetime espionage).

238. *See* Jinyuan Su, *Use of Outer Space for Peaceful Purposes: Non-Militarization, Non-Aggression and Prevention of Weaponization*, 36 J. SPACE L. 253, 254 (2010).

239. *See id.* at 258; Joseph R. Soraghan, *Reconnaissance Satellites: Legal Characterization and Possible Utilization for Peacekeeping*, 13 MCGILL L.J. 458, 489 (1967).

240. Chesterman, *supra* note 4, at 1076.

241. MARTTI KOSKENNIEMI, FROM APOLOGY TO UTOPIA: THE STRUCTURE OF INTERNATIONAL LEGAL ARGUMENT 437 (2005).

242. Of course, these claims have to be cast under international law and not national law. *See* Vienna Convention on the Law of Treaties art. 27, May 23, 1969, 1155 U.N.T.S. 331, 8 I.L.M. 679.

times referred to as the process of 'claims and counterclaims,' as States have the opportunity to claim new rights and other States are provided with the opportunity to respond to those claims. As it is, States have rarely, if ever,[243] claimed a "right to spy" in exception to international law. Quite the contrary, upon discovery acts of espionage have historically led to a legal hat trick of plausible deniability, responding with (i) a denial; (ii) 'Neither Confirm Nor Deny'; or (iii) an attempt to excuse its behavior on the basis of mistake. As we shall see, the consequence of these types of response is to stall or rather cancel the emergence of customary exceptions. Further, customary exceptions cannot emerge from (iv) extra-legal justifications or (v) mere silence on the basis that espionage is an indecorous subject.

1. Denials

States have consistently refused to acknowledge their participation in espionage activities.[244] Denials have been particularly prevalent in the context of diplomatic espionage, where agents under diplomatic cover conduct espionage abroad in breach of the VCDR, and receiving States are known to bug the embassies of the sending States:[245] "[w]hen microphones have been found in embassies, protests have of course been made, but the receiving State has never, so far as one knows, admitted that is had

243. *See* Wrange, *supra* note 30, at 321 (observing that no State "has publicly claimed that espionage in all its forms is legal. On the contrary, states generally deny being involved in illegal espionage, and admit only when there is full proof"). *See also* EILEEN DENZA, DIPLOMATIC LAW: COMMENTARY ON THE VIENNA CONVENTION ON DIPLOMATIC RELATIONS 187 (4th ed. 2016) (observing that despite routine violation of the VCDR there is "no indication whatsoever from public diplomatic exchanges of any attempt to justify any forms of surveillance of diplomatic communications on any legal basis."); Forcese, *supra* note 14, at 202 ("[S]pying is a poor candidate for a customary international law exception to sovereignty—whatever state practice exists in the area is hardly accompanied by *opinio juris*."); Terry, *supra* note 10, at 191; Schmitt & Vihul, *supra* note 41, at 1645 (similarly noting the absence of *opinio juris* supporting the existence of a customary exception to the principle of territorial sovereignty in the context of cyber espionage); Ian Brown & Douwe Korff, *Foreign Surveillance: Law and Practice in a Global Digital Environment*, 3 EUR. HUM. RTS. L. REV. 243, 250 (2014).

244. *See* 1 LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE 619 (Ronald Roxburgh ed., 1920) (stating that in regards to its spies under criminal prosecution, a State will "never interfere, since it cannot officially confess to having commissioned a spy"); Edmondson, *supra* note 28, at 445–46 ("The law of peace seems to be settled in only one situation: a secret agent captured within the interior of another state, under circumstances uncomplicated by a separate violation of international law, gives rise to an exchange of notes, a protest and a denial."); Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 340 (1996) ("Plausible denial was the universal international posture regarding spies; intelligence overflights seemed to merit the same response."); Perina, *supra* note 150, at 542 ("Historically, governments were loath even to acknowledge that they engaged in covert activity, especially in peacetime."). *But see* Beresford, *supra* note 12, at 114.

245. *See* DENZA, *supra* note 243, at 186 ("The usual response has rather been for the facts to be denied by the State accused of surveillance and for the other to resort to more effective particle and technological methods of protecting the secrecy of its own communications.").

installed them."[246] This protest-denial ritual is alive and well today. In the case of cyber espionage, for instance, the United States pressed China to provide an explanation for its clandestine entry into Google's servers in 2010—a cyber operation termed "Aurora."[247] The Chinese government denied any involvement, wrapping this claim up with a call for increased cooperation between States to combat Internet hacking.[248]

Denials are not of a nature to yield an exception to international law. Unlawful acts of espionage will not carve out an exception "as long as this contrary practice is condemned by other States or denied by the government itself and therefore does not represent its *official* practice."[249] Unless and until a State acknowledges its conduct, there is, in the process of custom, no "claim,"[250] and certainly no expression of *opinio juris*.

2. *Neither Confirm Nor Deny*

A second standard response by States is to "Neither Confirm Nor Deny" (NCND) spying accusations.[251] In 2003, for instance, Pakistan

246. *Id.*

247. *See generally* Ellen Nakashima, *Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, WASH. POST (May 20, 2013), https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html?noredirect=on&utm_term=.db13dcbd17ef [https://perma.cc/UK28-G2EQ].

248. *See* EMBASSY OF THE PEOPLE'S REPUBLIC OF CHINA IN THE UNITED STATES, *Foreign Ministry Spokesperson Ma Zhaoxu's Remarks on China-related Speech by US Secretary of State on "Internet Freedom"* (Jan. 22, 2010), http://www.china-embassy.org/eng/fyrth/t653351.htm [https://perma.cc/QQ76-XD6G] ("We resolutely oppose such remarks and practices that contravene facts and undermine China-US relations. . . . As a major victim of hacking in the world, China believes that the international community should intensify the cooperation in jointly combating internet hacking so as to safeguard internet security and protect the privacy of citizens in accordance with law."). *See also* Aaron Shull, Cyber Espionage and International Law (Oct. 21, 2013) (paper presented at the GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013, Bali) (noting that China's denial stifles the development of CIL about cyber espionage).

249. HENCKAERTS & DOSWALD-BECK, *supra* note 147, at xliii.

250. *Id. See* Khurts Bat v. Investigating Judge of the German Federal Court, 147 I.L.R. 633, 661 (Eng. High Ct. 2011) (explaining that because States usually deny that spying has been undertaken on their behalf by diplomats, "the absence of such claims diminishes the prospect of establishing State practice on which customary international law must depend".); Elizabeth H. Franey, Immunity, Individuals and International Law: Which Individuals are Immune from the Jurisdiction of National Courts under International Law 236 (June 2009) (Thesis to the Department of Law of the London School of Economics) (stating that "[e]xchange of spies who have been arrested in foreign states are often arranged. States do not accept that their agents have been collecting information for them. Usually the agent has a legitimate business reason for being in the foreign state, and their state denies that they have been spying.").

251. Perina, *supra* note 150, at 542 ("Historically, governments were loath even to acknowledge that they engaged in covert activity, especially in peacetime."); Marty Lederman, *Major Development Concerning Transparency of the Use of Force in Yemen*, JUST SECURITY (May 14, 2014) https://www.justsecurity.org/10821/major-development-transparency-force/?print [https://perma.cc/HHZ9-Z3SC] (noting that in the context of the use of force, "the norm has become to neither confirm nor deny" rather than to issue specific denials); *see also* Richard Norton Taylor, *Why "Neither Confirm Nor Deny" Has Become Untenable for British Spies*, THE GUARDIAN (July 15, 2014), https://

sought categorical assurances that the British Government had not authorized any activity "inconsistent with the Vienna Convention"[252] in its embassy, namely, the installation of covert bugging devices when the building was being refurbished.[253] No assurances were given, but it is reported that the United Kingdom contacted Pakistan's Foreign Minister, "underlining the importance of maintaining good relations between the two countries, while neither confirming nor denying that an authorized bugging operation had taken place."[254] In 2013, the Australian Prime Minister responded to Indonesia's spying allegations by saying that "the Australian government never comments on specific intelligence matters. This has been the long tradition of government of both political persuasions and I don't intend to change that today."[255]

For obvious reasons, NCND maintains a special relationship with espionage. The response protects the identity of those engaged in spying abroad and the nature of the operations in which they are engaged. NCND has therefore been recognized as a legitimate practice by international tribunals,[256] and perhaps even as a plausible right in the recent *Timor-Leste v Australia* case.[257] Timor-Leste asserted that Australia had committed an act of espionage against it in Narrabundah in 2004, and an Agent of Australia replied that Australia NCND and requested the Court to dismiss the matter.[258] Pressed again to explain Australia's conduct, the Agent hinted to the fact that the question of whether there was some international law norm that States cannot collect intelligence, without making public the particular security issue, was inseparable from the question of espionage, an issue that was not before the Court.[259] While the ICJ rendered no con-

www.theguardian.com/commentisfree/2014/jul/15/neither-confirm-nor-deny-british-spies-edward-snowden-revelations [https://perma.cc/5VPS-X9HV] ("For decades, ministers and officials have come up with the pat response, 'We can neither confirm, nor deny', when asked about operations by MI5, MI6 and GCHQ.").

252. DENZA, *supra* note 243, at 186.

253. *Id.*

254. *Id.*

255. CNN Staff, *Indonesia voices anger at Australia alleged spying*, CNN (Nov. 18, 2013), https://edition.cnn.com/2013/11/18/world/asia/indonesia-australia-spy-allegations/index.html [https://perma.cc/Z7ZR-PNPC].

256. *See, e.g.*, Kennedy v. U.K., App. No. 26839/05, Eur. Ct. H.R. ¶ 137 (2010) (The court approved the government's "policy to 'neither confirm nor deny' [because this] was important to ensure the overall effectiveness of surveillance operations."); Liberty v. U.K., App. No. 58243/00, Eur. Ct. H.R. ¶ 47 (2008) (where the Government adopted a general policy of NCND with regards to allegations made in respect of surveillance); Perina, *supra* note 150, at 542 ("Some states, including the United States and Israel, typically offer 'no comment' in responding to specific allegations of intelligences activities or certain military conduct.").

257. *See* James R. Van de Velde, "*Neither Confirm nor Deny" at Sea Still Alive and Consistent with International Law*, 45 NAVAL L. REV. 268, 268 (1998) (arguing that "NCND reflects an international right that is one hundred and eighty-three years old and is consistent with both customary and conventional international law.").

258. *See* Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Austl.), Provisional Measures Order, 2014 I.C.J. 147, ¶ 2 (Mar. 3).

259. *Id.* ¶ 25.

clusive ruling on the matter, some Judges looked favorably at NCND.[260]

Be that as it may, NCND is not a breeding ground for customary espionage exceptions. Again, by declining to endorse or defend their conduct, spying States are undercutting the claim process of CIL.[261] Such response is possible because, as alluded to by the Australian Agent, there is no international legal obligation to reveal the reasons for why espionage has been conducted.[262] States may have a general right to plead the Fifth but, if they want their actions to be law creating, they must forfeit this response and present their claim unambiguously to the international society.

3. Mistakes

Where States are caught spying abroad, they often seek to excuse their involvement in this activity on the basis of mistake. As Dubuouis notes, aerial intrusions for espionage purposes are a remarkable illustration of this trend,[263] where States have historically been very careful to excuse their violation of the territorial sovereignty of other States on the grounds of "navigational mistakes."[264] For example, during the Cold War the USSR frequently alleged that the US's use of spy planes within its national airspace violated its right to territorial sovereignty.[265] Rather than admitting espionage, the typical American response was that the pilot had simply lost

260. *See id.* ¶ 31 (dissenting opinion by Callinan, J.) ; *id.* ¶ 28 (dissenting opinion by Greenwood, J.) (stating that Australia's right "to protect the safety of its officials must also be regarded as plausible.").

261. *See* Perina, *supra* note 150, at 574.

262. Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 177 (2017) (stating that "[D]espite the suggestion by some States to the contrary, there is *no* international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action."); Eric Donnelly, *The United States-China EP-3 Incident: Legality and Realpolitik*, 9 J. CONFLICT & SECURITY L. 25, 34 (2004) ("[S]tates have argued that states have no 'right' to request *any* flight details of aircraft over-flying the high seas."); similarly, see Wright, *supra* note 56 (who stated that "There is no legal obligation requiring a state to publicly disclose the underlying information on which its decision to attribute hostile activity is based, or to publicly attribute hostile cyber activity that it has suffered in all circumstances.").

263. *See* Louis Dubuouis, *L'erreur en droit international public*, 9 ANNUAIRE FRANÇAIS DE DROIT INTERNATIONAL 191, 215 (1963) (stating further that intrusive spy flights violate international law). This has been a longstanding practice. *See, e.g.*, *"Force majeure" and "Fortuitous Event" as Circumstances Precluding Wrongfulness: Survey of State Practice, International Judicial Decisions and Doctrine– Study Prepared by the Secretariat*, [1978] 2 Y.B. INT'L L. COMM'N 61, 102–03, U.N. Doc. A/CN.4/315 (arguing that "[b]ad weather, the malfunctioning of navigational instruments and other conditions of force majeure are frequently invoked in diplomatic correspondence concerning aerial incidents" and substantiating the assertion with the statements of German nationals involved in the 1913 incident between France and Germany, reporting that the airship "has lost the direction owing to foggy weather" and was "in no way engaged in acts of espionage."); *Note to the Hungarian Government of March 17, 1953*, *in* I.C.J. PLEADINGS, TREATMENT IN HUNGARY OF AIRCRAFT OF UNITED STATES OF AMERICA (U.S. V. HUNGRY; U.S.A. V. U.S.S.R.) (1954); Oliver J. Lissitzyn, *The Treatment of Aerial Intruders in Recent Practice and International Law*, 47 AM. J. INT'L L. 559, 581 (1953) (discussing the C-47 incident between the United States and Hungary).

264. Dubuouis, *supra* note 263, at 215 (speaking of "erreur de navigation excusable") ["excusable navigation mistake"] (our translation).

265. *Id.*

his or her bearings.[266] Similarly, when a Soviet submarine strayed into a restricted military area within Sweden's territorial sea in 1981, the USSR claimed that "while making a routine training cruise in the Baltic Sea, [a submarine] went off course in conditions of poor visibility and ran aground."[267] More recently, China alleged that its submarine entered Japan's territorial sea "by mistake from a technical cause during its normal training course."[268] Political expedience readily explains this practice. By justifying their actions on these grounds, States seek to negate their intention to spy and thereby shield themselves from embarrassment and international legal responsibility.[269]

The process of CIL formation is averse to mistakes. As just noted, State conduct matters for custom formation only insofar as it "provides clear evidence of how one State views the law."[270] Therefore, for such practice to be relevant, it must be "deliberate or, at least, conscious."[271] This logically excludes mistakes, accidents and other inadvertent acts.[272] Inadvertent repetition of mistakes can hardly lead to a settled practice accompanied by a legal *conviction*.[273] Thus, when a spying State excuses its actions as a mistake, it vitiates that conduct's contribution to possible customary espionage exceptions.

4. Extra-Legal Justifications

When confronted with compelling evidence pointing towards their participation in espionage activities, at least one State, the United States, has, on rare occasions, formally acknowledged its involvement in espio-

266. Edmondson, *supra* note 28, at 445 (noting that "the popular American response is that the pilot lost his bearing.").

267. Sadurska, *supra* note 136, at 35 (further adding that the Swedish authorities did not believe this statement and immediately delivered a protest to the Soviet Ambassador).

268. Kraska, *supra* note 67, at 211.

269. Mistakes and material impossibility can be regarded as circumstances precluding wrongfulness. *See* Dubuouis, *supra* note 263, at 215–16 (explaining that States typically claim mistake when accused of spying).

270. *See* PATRICK DUMBERRY, THE FORMATION AND IDENTIFICATION OF RULES OF CUSTOMARY INTERNATIONAL LAW IN INTERNATIONAL INVESTMENT LAW 156 (James Crawford & John S. Bell eds., 2016).

271. *Id. See also* Right of Passage over Indian Territory (Port. v. India) Judgment, 1960 I.C.J. 6, 82 (Apr. 12) (Dissenting Opinion of Judge Armand-Ugon) ("[A] deliberate intention . . . a common awareness reflecting the conviction . . . as to [a] right."); Wood, *supra* note 89, ¶ 70 ("The motivation behind a certain practice must be discernible in order to identify a rule of customary international law."); Luigi Ferrari Bravo, *Méthodes de recherche de la coutume internationale dans la pratique des États*, 192 COLLECTED COURSES OF THE HAGUE ACADEMY OF INT'L L. 233, 261 (1985).

272. *See* COMM. ON FORMATION OF CUSTOMARY (GEN.) INT'L LAW, *supra* note 147, at 14 ("[P]hysical acts are not always formal and deliberate manifestations of State practice. For instance, a ship might be arrested by a minor official without proper instructions, but this will still count as practice if it is not 'cancelled' by some higher authority.").

273. *See* HENCKAERTS & DOSWALD-BECK, *supra* note 147, at ILIV (stating that repeated evidence of violations of that rule are not of nature to challenge the existence of a rule where "this has been accompanied by excuses or justifications by the actors and/or condemnations by other States.").

nage and has sought to justify it, thereby departing from the "old rules of the game"[274] of denying allegations of espionage, NCND, or excusing that conduct on the basis of mistake. Yet, crucially, these justifications have not been framed in terms of permissive customary exceptions.

Take for example the U-2 affair, where on May 9, 1960, the U.S. Secretary of State Herter explicitly admitted that the United States had sent spy planes into the USSR's airspace as a measure to "lessen and to overcome the danger of surprise attack."[275] Many States vehemently rejected the Herter Declaration on the basis that it amounted to an assertion of a new right in favor of aerial espionage. For example, Poland explained before the Security Council that such flights constituted a violation of international law[276] and warned the international society of the declaration's dangerous precedential value:

> The statement of the Secretary of State which we heard on 9 May was unprecedented in history, as it attributed to the United States the right of espionage flights over the territory of the USSR for reasons of security. . . . At the moment when the Secretary of State pronounced those words the case ceased to be an incident. . . . At this point what actually happened was that a great, powerful State raised the violation of international law to the rank of its official policy. . . . The new doctrine expressed in the statement of the Secretary of State is an attempt to replace international law by the law of the jungle. . . . [It] negates the fundamental principles of international law on which the whole system of international relations is based, namely, the principle of the sovereignty of States. . . . A violation of these principles cannot and should not be justified by the interest of one State or even a group of States. . . . There can be no exceptions to that rule. . . . That is why it cannot be considered as a legal formula.[277]

As is well known, States concluded the U-2 affair constituted a violation of the USSR's sovereignty, and subsequently, the United States reversed its policy and determined that it would no longer use spy planes within other States' territorial airspace.[278] Indeed, Secretary Herter had to concede that the declaration was highly unusual, admitting that he knew of no precedent in history where a State official had admitted to spying.[279] What is

274. Falk, *supra* note 5, at VII.

275. Secretary Herter, *United States Plane Downed in Soviet Union: Statement by Secretary Herter*, 42 DEP'T ST. BULL. 816, 816 (1960).

276. U.N. SCOR 858th mtg., *supra* note 28, ¶ 85 ("Any flight that takes place without the permission of the State concerned, particularly an espionage flight, is a drastic breach of treaty obligations; it is also a violation of the principle of sovereignty and of a States frontiers; and finally it is a violation of the United Nations Charter, particularly Articles 1, 2 and 78.").

277. *Id.* ¶¶ 93–96, 98–99 ; *see also Legal Aspects of Reconnaissance in Airspace and Outer Space*, *supra* note 202, at 1100.

278. *See* Senator John F. Kennedy and Vice President Richard M. Nixon: First Joint Radio-Television Broadcast, Oct. 7, 1960, available at https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/2nd-nixon-kennedy-debate-19601007 [https://perma.cc/HCE5-SGVF] (last visited Feb. 12, 2019)(during the Presidential campaign of 1960, Senator Kennedy also admitted that the U-2 flights "were not in accordance with international law.").

279. *See* SENATE FOREIGN RELATIONS COMMITTEE: EVENTS INCIDENT TO THE SUMMIT CONFERENCE 26–27 (1960) (where the following exchange happened: "The Chairman: Mr.

more, in response to a query by Senator of Louisiana at the Hearings before the Senate Committee on Foreign Relations, Secretary Herter conceded that "all espionage is a violation of sovereignty, all forms of espionage."[280]

Although not *all* forms of espionage violate international law, the U-2 incident should be understood as a crucial development for the CIL about peacetime espionage, not least because it showed that pioneer States would face significant hurdles in justifying their unilateral actions.

Again in 1982, the U.S. Ambassador to the UN explained before the Security Council that the United States conducted regular reconnaissance flights over Nicaraguan territory in order to "safeguard our own security and that of other States which are threatened by the Sandinista Government."[281] It is not clear whether Ambassador Kirkpatrick justified these acts on the basis that the Sandinista government represented a general threat to the security of the United States or, more specifically, on the international law doctrine of self-defense.[282]

A similar situation occurred in 2014 when US President Obama responded to allegations that the NSA had been engaged in a global espionage campaign. President Obama explained that, in the future, "unless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies."[283] As with the Kirkpatrick declaration, it is not clear whether Presi-

---

Secretary, you are a longtime devotee of international relations and thoroughly familiar with precedents in this field. Is the public assumption of responsibility for espionage by the head of a state the usual and customary practice among nations? Secretary Herter: No; the general practice has been, I think, for a long period of time to deny any responsibility whatever. The Chairman: Do you know of any precedent in our history or in the history of any great nation in which the head of state has assumed personal responsibility for espionage activities? Secretary Herter: No; I do not know of any firsthand.").

280. *Legal Aspects of Reconnaissance in Airspace and Outer Space*, *supra* note 202, at n.144 (quoting *Hearings Before the Senate Comm. on Foreign Relations on Events Incident to the Summit Conference*, 86th Cong., 2d Sess. 43 (1960)).

281. U.N. SCOR, 37th Sess., 2335th mtg. ¶ 132, U.N. Doc. S/PV.2335 (March 25, 1982). Nicaragua rejected this claim both before the Security Council and before the ICJ; *see id.* ¶ 86.

282. This is the view of Judge Schwebel. In his dissenting opinion, Judge Schwebel referred to the Kirkpatrick Declaration and deemed the U.S. intelligence overflights to be permissible acts of self-defense. *See Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13, ¶ 9 (dissenting opinion by Schwebel, J.) ("Are United States support of the *contras* . . . as well as other measures such as intelligence overflights, military and naval manoeuvres, and a trade embargo, unnecessary and disproportionate acts of self-defence? I do not believe so."). It is generally accepted that acts of espionage can be justified on the basis of self-defence where an armed attack occurs or is imminent. *See* Forcese, *supra* note 14, at 199 ("[S]pying in response to the proliferation of weapons of mass destruction and state-sponsored terrorism . . . is difficult to square with the doctrinal law of self-defense. It is not clear how spying in aid of self-defense is permissible where the right to self-defense is not yet triggered as a matter of international law by, among other things, a sufficiently imminent armed attack."). For a broader interpretation of when states can invoke the doctrine of self-defense to justify their espionage activities, see Asaf Lubin, *Espionage as a Sovereignty Right under International Law and its Limits*, 24 INT'L L. STUDENTS ASS'N Q. 22 (2016).

283. Obama, *supra* note 139, at 139.

dent Obama was relying upon the doctrine of self-defense[284] to justify these forms of intelligence activities or, instead, whether he is appealing to extra-legal justifications such as the need to protect national security.

For the purpose of the present discussion, it makes little difference as to what basis Secretary Herter, Ambassador Kirkpatrick and President Obama sought to justify espionage—neither ground provides evidence of *opinio juris* to support the existence of customary exceptions in favour of the permissibility of espionage. As we have explained, *opinio juris* requires that States invoke CIL to justify their actions rather than extra-legal considerations (such as security) or other legal bases (such as self-defense).[285]

All in all, the pattern of CIL formation is aptly captured by the words of Lord Denning: "Whenever a change is made, someone some time has to make the first move. One country alone may start the process. Others may follow. At first a trickle, then a stream, last a flood."[286] Thus, even if we were to accept that the United States was ready to 'make the first move' on at least a few occasions (which is doubtful as it justified its actions on extra-legal considerations) these moves were not followed by a 'trickle' of State practice, even less a 'stream' or a 'flood.'

It is not difficult to fathom why States have reacted this way. The principle of reciprocity underpins CIL. As Byers observes, reciprocity "ensures that any state claiming a right under general CIL accords that same right to every other state, [thus] States will only claim rights which they are prepared to see generalized."[287] Except for the United States, most States may be motivated to spy for their own benefit, but reluctant to see these benefits generalized to more powerful peers. We are thus led to conclude that there is a lack of *opinio juris* on espionage.

5. *Legal and Psychological 'Cannot'*

Some have criticized this conclusion for being "naïve" about the delicacies of international relations.[288] The point would be that it is naive to equate States' refusal to acknowledge or justify their spying activities with a sense of *legal* wrong. Stone perhaps captured first the notion that States' silence was not the result of a legal 'cannot' but instead a *psychological* 'can-

284. Or even on the grounds of necessity. *See* Rep. of the Comm. to the Gen. Assembly, [2001] 2 Y.B. INT'L L. COMM'N 26, art. 25, U.N. Doc. A/CN.4/SER.A/2001/Add.1.

285. *See, e.g.*, *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13, ¶ 208 (The ICJ had to determine whether the provision of assistance to rebel groups within other States had emerged as a right under CIL and which had thereby modified the scope of the non-intervention principle. The Court rejected this contention, explaining that while there was a number of instances of foreign intervention for the benefit of forces opposed to the government of another State, such conduct had never been justified on the basis of a customary right but instead "expressly and solely by reference to the 'classic' rules involved, namely, collective self-defense against an armed attack.").

286. Trendtex Trading Corp. v. Cent. Bank of Nigeria, [1977] 1 Q.B. 529, 556 (C.A.) (Eng.).

287. James Crawford, *Foreword* to MICHAEL BYERS, CUSTOM, POWER AND THE POWER OF RULES IX, X (1999).

288. *See* Lotrionte, *supra* note 12, at 487–88.

not.'[289] In so doing, Stone distinguished between the legal 'cannot' (i.e., States are unwilling to justify their spying activities because they know they are acting unlawfully under international law) and the psychological 'cannot' (i.e., States are unwilling to justify their spying activities for reasons other than acting unlawfully), and favored this latter view.[290] Stone vividly captures this idea: espionage ought to be seen "like some situations that occasionally arise between friends . . . when one of them does the sort of thing about which it isn't really any use for them to talk."[291]

This was recently echoed by Lotrionte, who argues that "[i]n not acknowledging the spy, the sending state is not doing so necessarily because of a sense that its actions are illegal, but rather in order to put off what would be a very tense diplomatic conversation, but not necessarily a violation of international law."[292]

These observations inject a healthy dose of realism into our discussion of customary exceptions. Indeed, States might refuse to justify their spying activities for a myriad of reasons, chief amongst them is to avoid embarrassment and an indecorous subject. Another reason might be because States "hold their spying capacities as closely guarded secrets."[293] Discussing spying *per se* or methods of spying with other States would necessarily involve disclosing one's sources and capabilities. Even small "disclosure of a source's identity could well impair intelligence gathering and cause sources to 'close up like a clam.'"[294]

However, what we must not lose sight of is that on multiple occasions, international tribunals such as the ICJ have determined that for customary exceptions to form, State practice must be accompanied by *opinio juris*.[295] More to the point, the psychological 'cannot' flies in the face of clear *opinio juris* supporting the permissibility of certain intelligence collection acts.

A careful study of State practice shows that despite the psychological 'cannot,' States have not shied away from supporting the permissibility of spying conducted in the high sea,[296] in international airspace[297] or in

289. Julius Stone, *Legal Problems of Espionage in Conditions of Modern Conflict*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 29, 39 (Roland J. Stanger ed., 1962).

290. *Id.* at 40.

291. *Id.* at 39.

292. Lotrionte, *supra* note 12, at 487. Lotrionte adds: "The fact that spies are often given awards upon returning to their home country once PNGed from another state is reflective of the sending state's belief that there is nothing illegal or dishonorable in spying abroad." Respectfully, this is not the case. If anything, medals are reflective of legitimacy, but not legality.

293. Deeks, *supra* note 10, at 314.

294. CIA v. Sims, 471 U.S. 159, 175 (1985).

295. *See, e.g.*, Talmon, *supra* note 38, at 420.

296. *See, e.g.*, Sam Bateman, *Hydrographic Surveying in Exclusive Economic Zones: Is it Marine Scientific Research*, *in* FREEDOM OF SEAS, PASSAGE RIGHTS AND THE 1982 LAW OF THE SEA CONVENTION 105, 115 (Myron H. Nordquist et al. eds., 2009) (noting that the United States "reserves the right to engage in military surveys outside foreign territorial seas and archipelagic waters" and that the United Kingdom believes that States "have a right to engage in military data gathering anywhere outside foreign territorial seas and archipelagic waters without prior notice to, or permission from the coastal state."); Lissitzyn, *supra* note 70, at 569 ("[I]nternational law does not forbid electronic reconnais-

outer space.[298] While a full study of these statements cannot be undertaken here, examples of express statements are available to show that these acts are deemed legal by States.

For instance, following the RB-47 incident, the United Kingdom repeatedly asserted before the Security Council that reconnaissance activities "are internationally permissible when conducted in international air-

---

sance from the high seas."); Liacouras, *supra* note 70, at 134 ("intelligence gathering on vessels sailing in international waters is permitted in principle"); Raul Pedrozo, *Military Activities in the Exclusive Economic Zone: East Asia Focus*, 90 INT'L L. STUD. 514, 531 (2014) (speaking of "abundant evidence of State practice that permits intelligence collection beyond the territorial sea.").

297. *See, e.g.*, Raul Pedrozo, *Military Activities In and Over the Exclusive Economic Zone*, *in* FREEDOM OF SEAS, PASSAGE RIGHTS AND THE 1982 LAW OF THE SEA CONVENTION 235, 240 (Myron H. Nordquist et al. eds., 2009) ("Long-standing state practice supports the position that surveillance and reconnaissance operations conducted in international airspace beyond the 12-nm territorial sea are lawful activities. Since the end of World War II, surveillance and reconnaissance operations in international airspace have become a matter of routine."); Oliver Lissitzyn, *Some Legal Implications of the U-2 and RB-47 Incidents*, 56 AM. J. INT'L L. 135, 142 (1962) (quoting the diplomatic protest by the USSR to the French Government of February 12, 1961, in which the Soviet government stated that "the generally accepted norms of international law provide for the freedom of flight in the airspace over the high seas, and no state, if it does not wish to be a violator of international laws, has the right to limit this freedom.").

298. *See, e.g.*, U.N. GAOR, First Committee, 17th Sess., 1289th mtg. at 13, U.N. Doc. A/C.1/PV.1289 (Dec. 3, 1962) (Albert Gore, U.S. Representative stated "[o]bservation from space is consistent with international law, just as is observation from the high seas."); Comm. on the Peaceful Uses of Outer Space, 17th Sess., 11th mtg., *supra* note 229, at 5 (Australia's representative stated "[i]t would seem absolutely clear that to obtain information about the earth by means of a space vehicle did not per se involve any breach of international law."); Comm. on the Peaceful Uses of Outer Space, 17th Sess., 10th mtg., *supra* note 234, at 4 ("The United Kingdom held that observation from points outside of the territory of any State was not contrary to international law."); U.N. GAOR, Comm. on the Peaceful Uses of Outer Space, 17th Sess., 7th mtg. at 9, U.N. Doc. A/AC.105/C.2/SR.7 (June 7, 1962) ("International law imposed no prohibition on the observation of the earth from outer space, which was peaceful and did not interfere with other activities on earth or in space."); Application for Revision of the Judgment of 11 September 1992 in the Case concerning the Land, Island and Maritime Frontier Dispute (El Sal./Hond.: Nicar. intervening), Verbatim Record, ¶ 29 (Sept. 9, 2003), https://www.icj-cij.org/files/case-related/127/127-20030909-ORA-01-00-BI.pdf [https://perma.cc/S6X7-HN28] (where Agent for El Salvador stated "[s]atellite photography does not, of course, entail any breach of international law"); Arthur A. Stein, *Constrained Sovereignty: The Growth of International Intrusiveness*, *in* THE NEW GREAT POWER COALITION: TOWARD A WORLD CONCERT OF NATIONS 261, 269 (Richard Rosecrance ed., 2001) (citing Nikita Khrushchev arguing "any nation in the world who wanted to photograph Soviet areas by satellite was completely free to do so"); *see also* CHENG, *supra* note 31, at 579; Carl Q. Christol, *Remote Sensing and International Space Law*, 16 J. SPACE L. 21, 21 (1988); CARL Q. CHRISTOL, THE 1986 REMOTE SENSING PRINCIPLES: EMERGING OR EXISTING LAW 269 (1987); Ram Jakhu, *International Law Governing the Acquisition and Dissemination of Satellite Imagery*, 29 J. SPACE L. 65, 76–77 (2003); Ilias I. Kuskuvelis, *The Customary Legality of Military Space Observation and Proposals Towards its Codification*, *in* PROCEEDINGS OF THE THIRTY-THIRD COLLOQUIUM ON THE LAW OF OUTER SPACE 305, 308 (1990); Soraghan, *supra* note 239, at 489 (stating "the legal characterization of reconnaissance satellites, as is witnessed by the oftstated argument that in less than ten years state practice has determined that sovereignty does not extend to outer space.").

space or international waters."[299] The legality of spying on the high seas was again reaffirmed in 2017 during the United States presidential elections, when a Russian spy ship was spotted lurking in international waters off the United States East Coast—something even United States officials considered lawful.[300]

Stone's claim, then, that States' silence should be understood as a psychological impossibility in the face of an indecorous subject cannot be sustained when one considers that the psychological 'cannot' has not precluded States from asserting the legality of at least some forms of espionage, that is, precisely the ones that are unambiguously lawful. The psychological 'cannot' really is a legal 'cannot.'

C. Other Sources of *Opinio Juris*

The absence of express *opinio juris* in favor of espionage exceptions points towards the conclusion that peacetime espionage "appear[s] to be a case in which frequent practice has not established a rule of law because the practice is accompanied not by a sense of right but by a sense of wrong."[301] The following section explores whether other sources of *opinio juris* exist, namely (i) negative State practice by injured States and (ii) domestic law and national decisions, which can be used to evidence the existence of customary espionage exceptions.

1. Negative State Practice

A segment of the current literature turns the *opinio juris* requirement on its head and argues that the failure of *injured* States to denounce espionage activities as unlawful is reflective of their view that such conduct is lawful under CIL. The main argument is that, "[i]n terms of the actual volume of this activity . . . the number of formal protests which have been lodged have been relatively insignificant"[302] and this thus indicates "a deep but reluctant admission of the lawfulness of such intelligence gathering, when conducted within customary normative limits."[303] Said differently, this literature argues that customary espionage exceptions can be established on the basis of negative State practice, i.e. abstentions and omissions.

---

299. U.N. SCOR, 15th Sess., 883d mtg. ¶ 136, U.N. Doc. S/PV.883 and Add.1 (July 26, 1960) (remarks by U.K. representative, Pierson Dixon).

300. *See* Christine Hauser, *Trump, the Russian Ship and Suspicious Minds*, N.Y. TIMES (Feb. 16, 2017), https://www.nytimes.com/2017/02/16/us/politics/russian-ship-vessel-usa.html (according to Captain Andrew Tucci from the United States Coast Guard, "'yes, Russian vessels transit through international waters . . . and certainly American vessels transit through international waters, and it is a legitimate and lawful activity that doesn't raise any particular concerns.").

301. Wright, *supra* note 51, at 17.

302. McDougal et al., *supra* note 12, at 394.

303. *Id.*; *see also* Deeks, *supra* note 10, at 305 (arguing that "[s]tates generally refrain from characterizing spying by other states as internationally illegal, at least when that spying collects intelligence about core state activities such as military capabilities."); Lotrionte, *supra* note 12, at 475.

For instance, Cohen-Jonathan and Kovar identify six incidents between 1877 and 1946 where injured States reacted tepidly to intrusive acts of foreign secret agents.[304] Colby paints a similar picture in relation to diplomatic spying, arguing that "[w]hile such tolerance is not uniform among all participants in the international arena, and remains low, if at all in situations of intense crisis, it is nonetheless perceptible."[305] Whereas this argument was, at least historically, confined to spying by diplomats and secret agents, it has since picked up momentum and is nowadays used to establish the customary basis of other forms of espionage.[306]

This line of argument is problematic for two reasons. At the outset, it puts the cart before the horse: pursuant to *Nicaragua*, the crucial question is whether the spying States claimed to be acting pursuant to customary espionage exceptions. This being said, advocates of the toleration argument are not entirely mistaken in looking at the injured States' reaction; *opinio juris* ought to be sought with respect to "the interested States, both those who carry out the practice in question and those in a position to respond to it."[307] Inaction by injured States must nevertheless be of a certain *quality* in order to qualify as *opinio juris*. In Fitzmaurice's words,

> [c]learly, absence of opposition is relevant only in so far as it implies consent, acquiescence or toleration on the part of the States concerned; but absence of opposition per se will not necessarily or always imply this. It depends on whether the *circumstances* are such that opposition is called for because the absence of it will cause consent or acquiescence to be presumed.[308]

---

304. Gérard Cohen-Jonathan & Robert Kovar, *L'espionnage en temps de paix*, 6 ANNUAIRE FRANÇAIS DE DROIT INT'L, 239, 251–54 (1960).

305. Jonathan E. Colby, *The Developing Law on Gathering and Sharing Security Intelligence*, 1 YALE J. INT'L L. 49, 88 (1974).

306. *See, e.g.*, *id.* at 67 (noting that States "appear to tolerate the entry of each other's aircraft within the airspace above their own territorial seas for the purpose of 'passive' observation and monitoring," and that by exchanging spies, States demonstrate their toleration of espionage); Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1095 (2003) (speaking of a "widespread, international tolerance" of espionage.). *See also* Deeks, *supra* note 6, at 646 (arguing "[i]n the face of the longstanding practice by states of spying on each other . . . one can argue that states and their officials are on notice that they are subject to foreign intelligence activity and, where they have not objected to it, have tacitly consented to being the targets of that activity.").

307. Wood, *supra* note 89, ¶ 64. Such acquiescence by injured States, in the words of the ICJ in the *Gulf of Maine*, could be "equivalent to tacit recognition manifested by unilateral conduct which the other party may interpret as consent."; Delimitation of the Maritime Boundary in the Gulf of Maine Area (Can./U.S.), Judgment, 1984 I.C.J. 246, ¶ 130 (Dec. 18). *See also Report of the International Law Commission: Seventieth Session*, *supra* note 88, Conclusion 10(3) ("Failure to react over time to a practice may serve as evidence of acceptance as law (*opinio juris*).").

308. Gerald Fitzmaurice, *The Law and Procedure of the International Court of Justice, 1951-54: General Principles and Sources of Law*, 30 BRIT. Y.B. INT'L L. 1, 33 (1953) (emphasis added). *See also Report of the International Law Commission: Seventieth Session*, *supra* note 88, Conclusion 10, ¶ 8 ("it is essential that a reaction to the practice in question would have been called for").

And there is the rub for espionage. As this practice is almost always committed in secret, it is likely that States are not fully aware of the intrusive espionage acts committed on their territory, which means that they cannot protest against this conduct. Where there is no opportunity to protest, silence cannot be interpreted as acquiescence.

To be sure, all States seem *generally* aware of the widespread and longstanding nature of espionage, but as their puzzled reactions have periodically shown (following the Echelon program revelations in 2000[309] or the Snowden revelations in 2013) it is simply not the case that States are always aware of the exact nature and true extent of espionage activities conducted against them with sophisticated means.

A second circumstance that may explain inaction by injured States rests on the *tu quoque* doctrine. As a 1999 memorandum from the US Department of Defense notes, "[t]he lack of strong international legal sanctions for peacetime espionage may also constitute an implicit application of the international law doctrine called '*tu quoque*' (roughly, a nation has no standing to complain about a practice in which it itself engages)."[310] This seems particularly true for the most widespread forms of espionage amongst States, e.g., diplomatic espionage,[311] secret agents[312] and cyber

309. Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) (2001/2098 (INI)) EUR. PARL. DOC. A5-0264/2001 (July 11, 2001), at 11 (noting that many senior Community figures, including European Commissioners claimed to be unaware of the existence of the ECHELON program). *See also* Dimitri Yernault, *De la fiction à la réalité: le programme d'espionnage électronique global 'Échelon' et la responsabilité internationale des États au regard de la Convention Européenne des Droits de l'Homme*, 1 REVUE BELGE DE DROIT INT'L 137, 138 (2000).

310. *See* DEP'T OF DEF., *supra* note 203, at 46. *See also* Wrange, *supra* note 30, at 15 ("[E]spionage by one state may be considered to be an estoppel against that state if it raises a claim against another state that engages in similar conduct.").

311. Toleration is all the more understandable because, for receiving States to uncover espionage by foreign diplomats, they might have to subject those diplomats to some form of surveillance, which can violate the VCDR. A certain degree of toleration between States is thus in order. *See* Mohammed Helal, *'We're on the Air!' Michael Flynn, Sergey Kislyak and the Paradoxes of Diplomatic Immunities*, OPINIO JURIS (Feb 21, 2017), http://opiniojuris.org/2017/02/21/were-on-the-air-michael-flynn-sergey-kislyak-and-the-paradoxes-of-diplomatic-immunities/ [https://perma.cc/9BRM-FC2Q] (adding that "this, I suspect, is part of the reason why states have tolerated the practice of surveillance of diplomats. States recognize and uphold the general principles of the inviolability and immunity of diplomatic agents, while expecting and tolerating a degree of encroachment on the confidentiality of diplomatic communications as a necessary antidote to . . . spying.").

312. Espionage by undercover agents abroad is so widespread that States have proceeded under a legal fiction whereby the spy's individual responsibility is triggered *in lieu* of the sending States' responsibility. *See* Tenet v. Doe, 544 U.S. 1, 3 (2005) (holding that spies cannot enforce their secret contracts with the U.S. government); Vavilov v. Canada (Citizenship and Immigration), [2017] F.C. 132, ¶ 90 (Can.) (noting that illegal secret agents cannot be considered employees of a Foreign government even if they gather intelligence in the same way that official diplomats do). *See also* Delupis, *supra* note 84, at 70 (arguing that the responsibility of the sending States for its secret agents spying abroad almost always remain latent); Quincy Wright, *Legal Aspects of the U-2 Incident*, 54 AM. J. INT'L L. 836, 851 (1960) ("[S]ince states are acting *ultra vires* in authorizing [aerial espionage] in time of peace, they cannot protect their agents from

espionage.

This is again illustrated by the U-2 incident, where members of the international society criticized the USSR's condemnation of the United States' espionage activities given its own longstanding espionage.[313] During the incident the United States cited around 360 convictions of Soviet spies in courts around the world, and States' disapproval of the USSR was felt before the Security Council: "if the U-2 incident is to be condemned, it is certainly not for the Soviet Union to cast the first stone."[314]

But while espionage is at times tolerated by the international society, on many other occasions States have invoked the language of international law to condemn this activity, further militating against the emergence of permissive CIL exceptions. For instance, this was most recently evidenced in the cyber context by a wide array of statements by States in reaction to Edward Snowden's revelations that the United States' NSA had been engaged in a massive, global cyber espionage campaign. The Brazilian President Dilma Rousseff was clear in her view that the NSA's conduct constituted an unlawful intrusion into Brazil's territorial sovereignty.[315] Brazil's objections to this unlawful activity were communicated to the United States by "demanding explanations, apologies and guarantees that such acts or procedures will never be repeated again."[316] In the same vein, Brazilian Justice Minister described the surveillance as "an attack on [Brazil's] sovereignty."[317]

Similarly, Argentina, Bolivia, Brazil, Uruguay, and Venezuela, channeling their views through the Pro-Tempore President of MERCOSUR, submitted a *Note Verbale* to the UN Secretary-General "[c]ondemning the acts of espionage carried out by the intelligence agencies of the United States of America . . . which constitute unacceptable behaviour that violates our sovereignty."[318] Separately, the Foreign Minister of Venezuela explained before the Security Council that it rejected "the actions of global espionage

---

[criminal] prosecutions beyond the usual demand for fair trial under the municipal law of the state conducting the trial.").

313. *See* Wright, *supra* note 51, at 20. *See also* Wright, *supra* note 312, at 849.

314. *See* U.N. SCOR, 15th Sess., 858th mtg., *supra* note 28, at 15.

315. *See* Julian Borger, *Brazilian President: US Surveillance a 'Breach of International Law'*, THE GUARDIAN (Sept. 24, 2013), https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance [https://perma.cc/RQA4-LKRK] (quoting President Rousseff: "Tampering in such a manner in the affairs of other countries is a breach of international law and is an affront to the principles that must guide the relations among them, especially among friendly nations. A sovereign nation can never establish itself to the detriment of another sovereign nation.").

316. President of the Federative Republic of Brazil, Statement by H. E. Dilma Rousseff, President of the Federative Republic of Brazil, U.N. GAOR, 68th Sess., at 2 (Sept. 24, 2013), available at https://gadebate.un.org/en/68/brazil [https://perma.cc/WP5Y-2SL9].

317. *Brazil and Mexico Probe Claims US Spied on Presidents,* BBC NEWS (Sept. 2, 2013), https://www.bbc.com/news/world-latin-america-23938909 [https://perma.cc/FAL3-A6ZN].

318. Note Verbale dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations addressed to the Secretary-General, U.N. Doc. A/67/946 (July 29, 2013), at 2.

carried out by the government of the United States, which undermine the sovereignty of States" and called upon "the United Nations [to] punish and condemn this violation of international law."[319] In addition, the Bahamian Foreign Minister asked what the "high ideals of territorial integrity, sovereignty and respect for the rule of law actually mean in practice" in light of such massive espionage.[320] Lastly, before the UN General Assembly, Indonesia noted its "strong position against extraterritorial surveillance because it was a violation of international law."[321] Hence, in the words of Chesterman: "if the vast majority of States both decry it and practice it, state practice and *opinio juris* appear to run in opposite directions."[322]

2. *Domestic Law and National Decisions*

Given the absence of *opinio juris* supporting customary espionage exceptions, some scholars draw on domestic law authorizing espionage.[323] Such practice is a weak reed on which to establish *opinio juris*. For domestic law to reflect acceptance of law, States must have enacted that law with the belief that the acts of espionage were lawful under international law. It is telling that even those States that have enacted such laws harbor doubts about their validity under international law.

For example, when the United States enacted FISA in 1978 to permit electronic surveillance directed at diplomatic premises on American soil, it had to concede that the view which held that the VCDR authorized these activities was "one about which reasonable persons may harbor some

319. U.N. SCOR, 68th Sess., 7015 mtg. at 8, U.N. Doc. S/PV.7015 (Resumption 1) (Aug. 6, 2013).

320. *See* Rashad Rolle, *Lawyers to Act in N.S.A. Spy Row*, TRIBUNE 242 (June 5, 2014), http://www.tribune242.com/news/2014/jun/05/lawyers-act-ns-spy-row/ [https://perma.cc/6K2D-WEJ7].

321. Press Release, General Assembly, Third Committee Approves Text Titled "Right to Privacy in the Digital Age", as It Takes Action on 18 Draft Resolutions, U.N. Press Release GA/SHC/4094 (Nov. 26, 2013). More expressions of *opinio juris* exist in this respect. *See, e.g.*, Statement by Dr. the Honourable Ralph E. Gonsalves, Prime Minister of Saint Vincent and the Grenadines to the United Nations, General Debate of the U.N. General Assembly, 68th Sess., at 12 (Sept. 27, 2013) (rejecting electronic espionage "as illegal, a violation of diplomatic conventions, and an affront to the comity of nations."); Statement by H.E. Mr. Bruno Rodriguez Parrilla, Minister for Foreign Affairs of the Republic of Cuba, on behalf of the Community of Latin American and Caribbean States, General Debate of the U.N. General Assembly, 68th Sess., at 4 (Sept. 26, 2013) ("The global espionage against CELA member countries . . . is a violation of the principle of sovereignty of States and International Law.").

322. Chesterman, *supra* note 4, at 1072.

323. *See, e.g.*, Lotrionte, *supra* note 12, at 488 ("Given . . . that most states have passed domestic legislation establishing some form of legal authority for such clandestine activities, it would seem that there exists *opinio juris* on the practice of espionage."). For domestic law and custom, compare *Fisheries Jurisdiction*, *supra* 153, at 131 (the Court's judgment relied on the legislation of certain States having adopted the ten-mile rule concerning the delimitation of the territorial sea but could not find sufficient evidence of a "general" practice) with Jurisdictional Immunities of the State (Ger. v. It.: Greece intervening), Judgment 2012 I.C.J. 99, ¶¶ 70 & 88 (Feb. 3) (where the latter paragraph excludes the relevance of an isolated example of legislation for the purpose of establishing the existence of practice.).

doubt."[324]

Also illustrative are the 2015 legislative developments in Canada. As previously mentioned, Canada amended its *Canadian Security Intelligence Service Act* to authorize intelligence collection abroad "without regard to any other law, including that of any foreign state."[325] It is telling that in the House of Commons' debates, numerous MPs expressed serious concerns about this language, to the point that all opposition parties agreed on an amendment to delete it in order "to remove any contradiction with international law and the explicit granting of power to Canadian courts to authorize illegal activity in other States."[326] Tempers flared over this "extremely extraordinary"[327] language, while one MP argued that the "language is so broad and so offensive in many ways to international law that I cannot image the courts would look favourably upon it."[328] Conspicuously absent from the debates is the assertion that espionage abroad is a lawful international activity.

Similarly, Switzerland readily admits that extraterritorial espionage authorized by its 2017 *Loi sur le renseignement* is problematic as it may be constrained "to some extent" by several rules of international law, including the VCDR.[329] On another occasion, the Swiss *Délégations des commissions de gestion des Chambres fédérales* simply acknowledged to the Federal Council that it did not know whether technical eavesdropping abroad was regulated by international law.[330] This demonstrates that while States may

---

324. Permanent Select Comm. on Intelligence, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, H.R. Rep. No. 95-1283, pt. 1, at 70 (1978) ("Administration witnesses testified that, in their view, the activities authorized by the bill are not prohibited by the Vienna Convention on Diplomatic Relations. The committee is of the same view.").

325. Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23.

326. HC Debates, 41st Parliament, 2d session, Vol. 147, No. 166, at 10869 (Jan. 30, 2015) (Can.).

327. HC Debates, 41st Parliament, 2d session, Vol. 147, No. 157, at 10311 (Dec. 8, 2014) (Can.).

328. *Id.* at 10313.

329. *See* Conseil fédéral, 14.022 Message concernant la loi sur le renseignement, FF 2029, 2154 (2014) (Switz.). Switzerland's views are ambiguous. *See generally* Samantha Besson & Odile Ammann, *La pratique Suisse relative à la détermination du droit international coutumier*, 21 CAHIERS FRIBOURGEOIS DE DROIT EUROPÉEN 91 (2016) (citing the Legal Opinion of March 10, 2009 by the Swiss Federal Department of Justice and Police and the Directorate of International Law stating that "States generally do not react to acts of espionage with reprisals, that is, they treat espionage as inimical acts rather than acts contrary to international law") (our translation); *Id.* at 104 (citing the Note of November 1st 2013 by the Directorate of International Law to the Swiss Federal Department of Justice and Police, stating that "customary international law tolerates activities of peacetime espionage to a certain extent.") (our translation). Switzerland's method of identification of custom appears to rest mostly on negative State practice (i.e., abstentions and omissions); it does not consider other sources of State practice as it relates to spying.

330. *See* Délégations des commissions de gestion des Chambres fédérales, Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet Onyx) 1377 (Nov. 10, 2003) (Switz.) (explaining explicitly that it did not know whether technical eavesdropping abroad constitutes (a) an intrusion and thus a violation of the principles of territoriality; (b) if the interception is effectively conducted in Switzerland; or (c) rather in outer space where the communications satellites are located, in which case there would be no viola-

authorize espionage under national law, they do not necessarily believe that such conduct is permissible under international law.

In addition, a growing body of national decisions offsets contrary *opinio juris* derived from domestic laws.[331] The case law of various national courts has made it clear that territorially intrusive forms of espionage and diplomatic espionage violate international law.[332] For instance, the Dutch Special Court of Cassation in the 1949 *In Re Flesche* case, which concerns the arrest of a German spy immediately prior to the German invasion of the Netherlands, considered that peacetime espionage "constitutes an international delinquency by that State against another State for which it is answerable under international law."[333] The almost complete absence of contrary case law is also significant.[334]

Another important example is the Federal Court of Canada's decision, which recognized the absence of a customary espionage exception in 2008 when it refused to grant the CSIS a warrant to undertake espionage activities on the soil of foreign States.[335] In that case, CSIS had *explicitly* argued that State practice of territorially intrusive forms of intelligence had given rise to a customary exception, to which the Court responded that it was not persuaded that "in the national security context, the practice of 'intelligence-gathering operations' in foreign States is recognized as a 'customary practice' in international law."[336]

---

tion of the target States' sovereignty. Nonetheless, the Report considered that intelligence collection was limited by international human rights law.). French authorities seem to concur with this view. *See* Arthur Paecht, *Les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale,* at 50, 11e Assemblée Nationale Impressions, Rep. No. 2623 (Oct. 11, 2000) (noting that no international regime prohibits interception of communications between States).

331. National decisions play a dual role in relation to custom, not only as State practice and *opinio juris*, but also as subsidiary means for the determination of rules of CIL when they consider the existence of customary rules. *See* Wood, *supra* note 89, at 55; Jurisdictional Immunities of the State, *supra* note 323, ¶ 77.

332. *See supra* note 48 and accompanying text for other relevant decisions.

333. *In re Flesche*, *supra* note 48, at 272.

334. *But see* Espionage Prosecution Case, Case No. 2 BGs 38/91, Bundesgerichtshof [BGH] [Federal Court of Justice] Jan. 30, 1991 (Ger.), *reprinted in* 94 INT'L L. REP. 69, 74–75 (1994) (where the Federal Supreme Court of Germany held that espionage is neither lawful nor unlawful).

335. *Canadian Security Intelligence Service Act (Re)*, *supra* note 182, ¶¶ 27, 53. *See also* Craig Forcese, *Triple Vision Accountability and Outsourcing of CSIS Intercepts*, NAT'L SEC. L. (Dec. 6, 2013), http://craigforcese.squarespace.com/national-security-law-blog/2013/12/6/triple-vision-accountability-and-the-outsourcing-of-csis-int.html [https://perma.cc/2RFD-RHFR]. *See generally* Oonagh E. Fitzgerald, *The Globalized Rule of Law and National Security: An Ongoing Question for Coherence,* 65 U. NEW BRUNSWICK L.J. 40 (2014).

336. *In re Canadian Security Intelligence Service Act*, *supra* note 182, at ¶ 53. This was confirmed later in another judgment of the Federal Court. *See* X (Re), 2009 F.C. 1058, [2010] 1 F.C.R. 460, ¶ 65 (Can.) (stating that "In *CSIS (Re)*, above, at paragraph 54, Justice Blanchard held that '[n]o other basis under international law' had been put before him to warrant displacing the principles of sovereign equality, non-intervention and territoriality. CSIS had argued that customary international practice as it relates to intelligence gathering operations in a foreign state constituted an exception to principles of territorial sovereignty.").

Conclusion

For many years, international legal scholars insisted that there was little interaction between international law and espionage. This argument is no longer taken seriously. Nowadays, scholars readily admit that international law applies to espionage, and accept that certain forms of espionage run afoul of various prohibitive international legal rules. But the battlelines have been redrawn. Scholars wishing to perverse espionage as a national security tool have instead advanced the argument that, even if certain forms of espionage violate international law, this conduct is nevertheless lawful due to the existence of permissive CIL exceptions.

This Article debunks this thesis. This Article demonstrates that neither of the two elements necessary for customary espionage exceptions to ripen are present—public State practice and *opinio juris*. Although States engage in espionage on a regular basis, they do so in secret, which precludes such conduct from qualifying as State practice under CIL. Even if we accept for the sake of argument that there is patchy and anecdotal evidence of public State practice, States have nevertheless failed to issue unambiguous expressions of *opinio juris* in support of this practice.

If States wish to construct customary rights of peacetime espionage in exception to primary rules of international law, they are perfectly entitled to do so. However, it behooves them to do so openly by claiming customary rights to spy,[337] instead of leveraging the tenderly nurtured POS surrounding past and new means and methods of espionage. Our conclusions are summarized in Table 1 below.[338]

To conclude, perhaps it is helpful to refer to a now classical metaphor. The emergence of a CIL norm has often been discussed in terms of the emergence of a footpath in a wild field.[339] This metaphor has its limitations, but the take-home point is edifying. In the words of Lowe:

> Regular following of the same track establishes an identifiable path, whether it be made by a few people or by many; and if there is an understanding that the path *should* be followed, it will be a clear path with little or no sign of people straying from it or trying to make new, competing paths.[340]

The essence of the problem is this. Customary espionage exceptions have yet to clear a path through the legal wilderness. If the path-takers zigzag so that there are no clear tracks; if they are careful to cover their

337. *See* Cheng, *supra* note 31, at 425–56. See also Wright, *supra* 56, who recognized the danger in maintaining this POS in cyberspace ("The very pervasiveness of cyber makes silence from states on the boundaries of acceptable behaviour in cyberspace unsustainable. If we stay silent, if we accept that the challenges posed by cyber technology are too great for the existing framework of international law to bear, that cyberspace will always be a grey area, a place of blurred boundaries, then we should expect cyberspace to continue to become a more dangerous place.").

338. This Article attempts only to investigate the *lex lata* of customary espionage exceptions, building on incidents available in open sources. While it proceeds holistically, Table 1 draws appropriate distinctions between different forms of spying.

339. *See, e.g.*, CHARLES DE VISSCHER, THEORY AND REALITY IN PUBLIC INTERNATIONAL LAW 149 (P.E. Corbett trans., 1960).

340. VAUGHAN LOWE, INTERNATIONAL LAW: A VERY SHORT INTRODUCTION 21 (2015).

footprints; and if they consistently deny following new tracks when they are caught in the act, then there can be no identifiable paths and no understanding that they *should* be followed.

Table 1: Customary Exceptions for Acts of Intelligence Collection

Constituent Acts	Breached Rule(s) or Principle(s)	Objective Element	Subjective Element	Customary Exception
Territorially intrusive acts by undercover agent (with no diplomatic or consular status) in the territory of the injured State	Principle of territorial integrity	Longstanding and widespread, but practice is not uniform nor public	Subjective element does not support legality	No exception
Territorially intrusive acts in the national airspace of the injured State	Principle of territorial integrity and Chicago Convention	Widespread, but practice is not uniform nor public	Subjective element does not support legality	No exception
Territorially intrusive acts in the territorial waters of the injured State	Principle of territorial integrity and article 19(2)(c) UNCLOS	Widespread, but practice is probably not uniform nor public	Subjective element does not support legality	No exception
'Diplomatic' espionage	VCDR, notably art. 3(d), 21, 24, and 41(1)	Longstanding and widespread, but practice is not uniform nor public	Subjective element does not support legality	No exception
'Consular' espionage	VCCR, notably art. 31, 33, 55(1) and 55(2)	Longstanding and widespread, but practice is not uniform nor public	Subjective element does not support legality	No exception
Remote access cyber espionage	Possibly in breach of the principle of territorial integrity	Nascent	Nascent	Insufficient data to conclude for now
Reconnaissance from outer space	Outer space freedom *allows* for such conduct	Longstanding, uniform, widespread and public	Subjective element supports legality	N/A
Reconnaissance from international waters	High sea freedom *allows* for such conduct	Longstanding, uniform, widespread and public	Subjective element supports legality	N/A
Reconnaissance from international airspace	Freedom of flight in international air space *allows* for such conduct	Longstanding, uniform, widespread and public	Subjective element supports legality	N/A
Blanket espionage exception	N/A	N/A	Subjective element confirms that 'peacetime espionage' is not a legal category	N/A