"THE RIDDLE OF THE SANDS"†–PEACETIME ESPIONAGE AND PUBLIC INTERNATIONAL LAW

PATRICK C. R. TERRY*

"Partout où nécessité fait loi"[1]

ABSTRACT

In contrast to the enduring popularity of spy films and novels, the relationship between public international law and espionage has proven to be a less popular topic of discussion amongst academics and lawyers. The state of the law reflects this: while the international community has developed some rules on wartime espionage, there are no treaties or firm rules of customary international law dealing explicitly with the much more common phenomenon of espionage during times of peace. This has led some academics to concur with the motto attributed to France's External Security Service (DGSE), quoted above, according to which necessity determines the law. Following the Snowden revelations and the allegations of major Chinese and Russian cyber espionage attacks, however, a growing interest in examining whether peacetime espionage activities can be reconciled with international law is becoming apparent.

This Article argues that discussing the lawfulness or unlawfulness of peacetime espionage in international law per se is not only unhelpful, but actually serves to obscure the actual issue: whether a state's individual espionage activity directed against a target state can be reconciled with international law. I demonstrate that peacetime espionage activities are usually clearly unlawful under public international law, irrespective of whether the spying state employs traditional or more modern methods, i.e., cyber espionage. In fact, far from the relationship between international law and espionage being equivalent to "the Riddle of the Sands," legal rules are in place that already comprehensively

† The title of a spy novel by Robert Erskine Childers. The title refers to the North German/Frisian sands, which are either covered by water or turn into mudflats ("Wattenmeer"), an area often shrouded in fog. In the story, Imperial Germany is covertly planning an attack on the United Kingdom in this area—a complicated "riddle" solved by the two British heroes of the story. ROBERT ERSKINE CHILDERS, THE RIDDLE OF THE SANDS (1903).

* Patrick C. R. Terry is a Professor of Law and the Dean of the Faculty of Law at the University of Public Administration in Kehl, Germany.

1. "Everywhere where necessity determines the law" is the reputed motto of the French External Security Service DGSE (*Direction Générale de la Sécurité Extérieure*). *See* DGSE – Direction Générale de la Sécurité Extérieure, FACEBOOK (Feb. 4, 2016), https://fr-fr.facebook.com/DGSEFR/photos/partout-où-nécessité-fait-loi/439211472936976/.

regulate the relationship between peacetime espionage and public international law and are easy to discern if one wishes to do so.

I. Introduction

For more than a century now, espionage has captured people's imagination: works of fiction depicting the clandestine, often dangerous activities undertaken by real or imagined spies have proved immensely popular. Some of the more famous authors of spy novels, such as John le Carré, whom many credit with depicting the often cynical and harsh realities of espionage, are so influential that even their political views are respected beyond their readership. Others enjoy the more action-fueled and glittering, but less realistic, world of espionage reflected in James Bond films, where the difference between "good" and "bad" is comfortingly easy to discern.

In contrast to the enduring popularity of this film and literature genre, the relationship between public international law and espionage has proven to be a less popular topic of discussion amongst academics and lawyers. The state of the law reflects this: while the international

community has developed some rules on wartime espionage,[2] there are no treaties or firm rules of customary international law dealing explicitly with the much more common phenomenon of espionage during times of peace. Given the worldwide preponderance of espionage activities, this lack of discourse seems counterintuitive. Recent developments, however, evidence a change in attitude: following the Snowden revelations and the allegations of major Chinese and Russian cyber espionage attacks, a growing interest in examining whether peacetime espionage activities can be reconciled with international law is becoming apparent. Before setting out my arguments, I should clarify that peacetime espionage as understood in this article is limited to the gathering, by or on behalf of a state, of information which is not publicly available and which another state wants to keep secret.[3]

In this article, I argue that discussing the lawfulness of peacetime espionage in international law *per se* is not only unhelpful, but actually serves to obscure the actual issue: whether a particular state's individual espionage activity to the disadvantage of a target state can be reconciled with international law. In the past, espionage advocates have utilized the paucity of discussion and law on peacetime espionage to hastily conclude that such activity is in broad terms either lawful or, at the very least, not *unlawful*—thus allowing these advocates to avoid addressing

2. Convention (IV) Respecting the Laws and Customs of War on Land, arts. 29–31, Oct. 18, 1907, 187 C.T.S. 227; Geneva Convention Relative to the Treatment of Prisoners of War, art. 31, Aug. 12, 1949, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, arts. 5, 66, Aug. 12, 1949, 75 U.N.T.S. 287; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), arts. 39(3), 45(3), 46, June 8, 1977, 1125 U.N.T.S. 3: *see also* Richard A. Falk, *Space Espionage and World Order: A Consideration of the Samos-Midas-Program*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 45, 80–81 (Roland J. Stanger ed., 1962); Stefan Talmon, *Sachverständigengutachten gemäß Beweisbeschluss SV-4 des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode* (2014), 1–39, at 16 (Ger.), https://www.bundestag.de/blob/282872/2b7b605da4c13cc2bc512c9c899953c1/mat_a_sv-4-2_talmon-pdf-data.pdf; Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1181–82 (2014); Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1073–74 (2006); Ian H. Mack, Towards Intelligent Self-Defence: Bringing Peacetime Espionage in From the Cold and Under the Rubric of the Right of Self-Defence 3 (June 7, 2013) (unpublished dissertation, Sydney Law School) (on file with the University of Sydney Library system); Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SECURITY L. & POL'Y 179, 181–84 (2011) (correctly pointing out that spying is not a "legal," but rather a "colloquial term").

3. Talmon, *supra* note 2, at 16; Raphael Bitton, *The Legitimacy of Spying Among Nations*, 29 AM. U. INT'L L. REV. 1009, 1011 (2014); Russell J. Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage*, *in* INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES 65, 65 (Anna-Maria Osula and Henry Roigas eds., 2016).

whether a specific, individual act of espionage conforms with international law.

The discussion needs to be turned on its head, however: first, it is necessary to assess whether the individual act of espionage allegedly attributable to a foreign state is compatible with international law. Only after individual incidents have been assessed may it become possible to draw some conclusions as to the general legality or illegality of peacetime espionage. Based on this chronology of legal analysis, I demonstrate that most—if not all—peacetime spying activities are clearly unlawful under public international law. It turns out that in fact, far from the relationship between international law and espionage being something like "the Riddle of the Sands," i.e., covered in thick fog, legal rules are in place that already comprehensively regulate the relationship between peacetime espionage and public international law and are easy to discern if one wishes to do so.

First, I set out the state of the debate surrounding the legality of peacetime espionage. Then, I assess the three main strands of argument and show that none of them provides a satisfactory explanation of the relationship between peacetime espionage and international law. Following that, I examine, on an individual basis, whether the most common activities associated with espionage are reconcilable with international law. Lastly, I conclude that peacetime espionage activities are generally unlawful. However, my analysis does not extend to whether some espionage activities also violate international human rights law.

II. Peacetime Espionage's Legality in International Law—the State of the Debate

When confronted with a question concerning the legality of peacetime espionage, the International Court of Justice (ICJ) was able to avoid deciding the issue,[4] so there is therefore no international judicial authority to refer to when debating the topic. Among scholars and lawyers, meanwhile, there generally are three broad strands of argument

4. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, ¶ 80–86 (May 24). The ICJ discussed Iran's claims of U.S. espionage conducted from within the U.S. Embassy as a possible justification for the subsequent hostage taking. Not surprisingly, the ICJ rejected this line of argument by, firstly, pointing out that Iran had not substantiated its claims, and, secondly, finding that even if proven, these allegations would not serve as a justification for Iran's conduct (also because diplomatic law provided a self-contained regime to deal with "such abuses of the diplomatic function"). *Id.*

relating to the legality of peacetime espionage:[5] that it is (A) lawful, (B) unlawful, or (C) neither lawful nor unlawful. The following analysis sets out the main arguments in favor of each of these three hypotheses.

A. *Peacetime Espionage is Lawful*

The *Lotus* principle provides the legal foundation of this strand of thought: according to the ICJ's predecessor, the Permanent Court of International Justice (PCIJ), a state's conduct is permissible, unless an established rule of international law prohibits it.[6] As states have not concluded any treaties outlawing espionage, and have not permitted the creation of a prohibitive rule in customary international law, the PCIJ's jurisprudence necessitates the conclusion that espionage is lawful.[7] State practice allegedly confirms this, as every state engages in espionage activities against other states.[8] The fact that some states have

5. Christoph D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT' L. REV. 1091, 1093–97 (2004); Chesterman, *supra* note 2, at 1074–75; Forcese, *supra* note 2, at 204; A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 602 (2007).

6. The P.C.I.J. phrased the so-called Lotus principle as follows: "International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. *Restrictions upon the independence of States cannot therefore be presumed.*" *See* S.S. Lotus (Fr. v Turk.), Judgment, 1927 P.C.I. J. (ser. A) No. 10, at 18 (Sept. 17) (emphasis added).

7. Julius Stone, *Legal Problems of Espionage in Conditions of Modern Conflict*, *in* ESSAYS ON ESPIONAGE & INTERNATIONAL LAW 29, 33–34 (Roland J. Stanger ed., 1962); Talmon, *supra* note 2, at 16–18; Stefan Talmon, *Das Abhören des Kanzlerhandys und das Völkerrecht (Tapping the German Chancellor's Cell Phone and Public International Law)*, BONN RES. PAPERS PUB. INT'L L., No. 3/2013, at 1, 6; MARKUS GEHRLEIN, DIE STRAFBARKEIT DER OST-SPIONE AUF DEM PRÜFSTAND DES VERFASSUNGS- UND VÖLKERRECHTS 87, 100–03 (1996); Bundesgerichtshof [BGH] [Federal Court of Justice] Jan, 30, 1991, 37 ENTSCHEIDUNGEN DES BUNDESGERICHTSHOFES IN STRAFSACHEN [BGHSt] 305, 308, 1992 (Ger.) (*Juris Online*; for details, see note 29). Ernesto J. Sanchez takes a different approach by mainly arguing that international law was so vague, it was not possible for opponents of espionage to argue convincingly that spying was unlawful. Ernesto J. Sanchez, *Intelligence Collection, Covert Operations, and International Law*, 23 INTELLIGENCER: J. U.S. INTELLIGENCE STUD. 73 (2017).

8. Stone, *supra* note 7, at 33–35; Gary Brown and Keira Poellet, *The Customary International Law of Cyberspace*, 6 STRATEGIC STUD. Q. 126, 133–34 (2012); GEHRLEIN, *supra* note 7, at 87, 100–03; Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F.L. REV. 217, 218 (1999); Jorge H. Romero, Cyberespionage 2010: Is the Current Status of Espionage under International Law Applicable in Cyberspace? 4–5, 16 (Apr. 30, 2001) (unpublished LL.M. thesis, Georgetown University Law Center) (on file with Defense Technical Information Center); Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 628–29 (2007); Jeffrey H. Smith, *A Matter of Integrity*, 49 L. QUADRANGLE NOTES 15, 15

allegedly concluded bilateral or multilateral treaties limiting espionage between them[9] is seen by some scholars as confirming espionage's basic legality.[10] Some proponents go even further, and argue that prolific state practice has led to the creation of a rule in customary international law explicitly permitting espionage.[11] They underpin this conclusion with the argument that espionage is and ought to be legal, because it allegedly reinforces international stability: spying allows states to gain information on another state's activities, enabling them to respond proactively to developing crises, thus possibly making the subsequent use of force unnecessary.[12] The latter argument leads others to conclude that espionage is merely a facet of self-defense.[13] Interestingly, however, some advocates of the lawfulness of espionage are in favor of creating new rules outlawing cyber espionage[14]—a threat to which the West seems to feel more vulnerable than traditional

(2007); Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 302–03 (2015).

9. Deeks, *supra* note 8, at 303. In this context, she refers to the Five-Eyes-Espionage Cooperation Agreements between the United States, the United Kingdom, Canada, Australia and New Zealand, which allegedly limit spying between these five states. W. Michael Reisman, *Covert Action*, 20 YALE J. INT'L L. 419, 421 (1995) (referring to no-spy-agreements between the Warsaw Pact states).

10. Deeks, *supra* note 8, at 303.

11. Smith, *supra* note 8, at 15; Romero, *supra* note 8, at 19, 44; Scott, *supra* note 8, at 217–26. Scott is more careful in his assessment. While repeatedly stressing that states' practice indicated that "international law tolerates the collection of intelligence in the territory of other nations," he does conclude that international law is "ambiguous" as far as espionage is concerned. *Id.*

12. *See* Stone, *supra* note 7, at 40–43; Skinner, *supra* note 2, at 1183; Baker, *supra* note 5, at 1095–96; Chesterman, *supra* note 2, at 1076, 1090–98, 1126, 1129; Romero, *supra* note 8, at 8–10; Sulmasy and Yoo, *supra* note 8, at 625–28, 633–36; Deeks, *supra* note 8, at 313–14; Asaf Lubin, *Cyber Law and Espionage Law as Communicating Vessels*, in 2018 10TH INT'L CONF. ON CYBER CONFLICT 203, 219–21 (T. Minarik et al. eds., 2018); Mack, *supra* note 2, at 4, 21–22 (appearing to view espionage as currently unlawful, but arguing that public international law ought to permit espionage). *See generally* Bitton, *supra* note 3.

13. *See* Sanchez, *supra* note 7, at 74; Baker, *supra* note 5, at 1091–92, 1096–97 (supporting the view that espionage is neither "endorsed" nor "prohibited" by international law); Mack, *supra* note 2, at 34–42; Romero, *supra* note 8, at 16; Sulmasy & Yoo, *supra* note 8, at 636–37; Lubin, *supra* note 12, at 219–21; Oscar Lopez, *Live and Let Spy: U.S. Intelligence in Brazil*, 1 CORNELL INT'L L. J. ONLINE 63, 63–66 (2013) (referring to "national security" instead of self-defense).

14. *See* Skinner, *supra* note 2, at 1183–97. While not looking at the legal issues raised by "traditional espionage" and claiming that espionage was beneficial, Skinner goes on to argue that economic cyber espionage should be treated differently by adopting broad interpretations of concepts such as sovereignty and intervention. Brown and Poellet, *supra* note 8, at 141 (arguing that treaties on cyber activities should be negotiated). *See* Romero, *supra* note 8, at 38–43 (presenting another view). *See generally* John F. Murphy, *Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?* 89 INT'L L. STUD. 309 (2013).

espionage.[15] Certainly, concerning economic cyber espionage, the United States, despite being accused of such conduct itself,[16] has been forthright in condemning such activities on the part of other states.[17]

B. *Peacetime Espionage is Unlawful*

Some international lawyers generally view espionage as unlawful.[18] In 1960, when asked about the relationship between espionage and international law before the Senate Committee on Foreign Relations, U.S. Secretary of State Herter responded, "[a]ll espionage is a violation of sovereignty, all forms of espionage."[19] Many would agree with this categorical statement: a state spying on foreign soil extends its governmental functions and activities beyond its own and onto another state's territory without respecting that state's jurisdiction. This consequently violates the target state's exclusive right of enforcement within its own

15. David E. Sanger, *Cyberthreat Posed by China and Iran Confounds White House*, N. Y. TIMES (Sept. 16, 2015), https://www.nytimes.com/2015/09/16/world/asia/cyberthreat-posed-by-china-and-iran-confounds-white-house.html; Murphy, *supra* note 14, at 322–27. Indicative of the U.S. approach in this area are comments by Waxman, who notes that "[e]xperts inside and outside the government widely agree that the United States is especially strong relative to other states with respect to its ability to penetrate and collect information from others' systems . . . U.S. planners may be reluctant to draw boundaries too tight, lest those boundaries impede their own ability to infiltrate and extract information from others' systems." Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article2 (4)*, 36 YALE J. INT'L L. 421, 435 (2011).

16. Klaus Remme, *Kein Partner der USA, sondern Konkurrent*, DEUTSCHLANDRADIO KULTUR (July 2, 2015), http://www.deutschlandradiokultur.de/nsa-spionage-kein-partner-der-usa-sondern-konkurrent.996.de.html?dram:article_id=324367.

17. *See U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, U.S. DEP'T OF JUSTICE (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; Siobhan Gorman, *China Singled Out for Cyberspying*, WALL STREET J. (Nov. 4, 2011), http://www.wsj.com/articles/SB10001424052970203716204577015540198801540.

18. *See* Falk, *supra* note 2, at 57; Douwe Korff, *Expert Opinion prepared for the Committee of Inquiry of the Bundestag into the "5EYES" global surveillance systems revealed by Edward Snowden* 1, 6 (June 5, 2014), https://www.bundestag.de/resource/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf (referring only to spying activities that amount to criminal offences according to the laws of the "target state"); Mack, *supra* note 2, at 15; 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); Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. INT'L L. 53, 67–68 (1984) (referring only to "the presence of agents sent clandestinely by a foreign power into the territory of another state").

19. *Events Incident to the Summit Conference 1960*: *Hearings before the Sen. Comm. on Foreign Relations*, 86th Cong., 2d Session 43 (1960) ("Espionage and International law"). Former U.K. Prime Minister Harold Macmillan also stated that espionage was "clearly contrary to international law." RICHARD J. ALDRICH AND RORY CORMAC, THE BLACK DOOR: SPIES, SECRET INTELLIGENCE AND BRITISH PRIME MINISTERS 205 (2016).

territory.[20] Spying, the argument continues, is also always an unlawful interference or intervention in another state's internal affairs.[21] The fact that virtually all domestic criminal law codes expressly forbid espionage arguably confirms espionage's unlawfulness;[22] this prohibition even extends to diplomats, a group of individuals often privileged, for example, by the fact that they and their families are usually immune from prosecution.[23] Following the Snowden revelations concerning widespread spying by the United States, some political leaders, mainly in South America, but also the Chinese government,[24] publicly stated their view that espionage is contrary to international law.[25]

C. *Peacetime Espionage is Neither Lawful nor Unlawful*

Finally, a third strand of argument claims espionage is neither lawful nor unlawful–there is a gap in public international law.[26] Advocates

---

20. Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, in ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, 12–13 (1962); Mack, *supra* note 2, at 16.

21. *See* Wright, *supra* note 20, at 5; Mack, *supra* note 2, at 15–16; Jared Beim, *Enforcing a Prohibition on International Espionage*, 18 CHICAGO J. INT'L L. 647, 652–54, 656–57 (2018).

22. Falk, *supra* note 2, at 57.

23. Wright, *supra* note 20, at 13; *see* Vienna Convention on Diplomatic Relations arts. XXIX-XXXI, Apr. 18, 1961, 500 U.N.T.S. 95 (discussing diplomatic immunity).

24. *China demands halt to 'unscrupulous' US cyber-spying*, THE GUARDIAN (May 27, 2014), https://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying.

25. *See* Julian Borger, *Brazilian president: US surveillance a 'breach of international law'*, THE GUARDIAN (Sept. 24, 2013) http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance; Carla Stea, *Latin America Condemns US Espionage at United Nations Security Council*, GLOBAL RESEARCH (Aug. 17, 2013), http://www.globalresearch.ca/latin-america-condemns-us-espionage-at-united-nations-security-council/5346120; David Fickling, '*Mossad spies' jailed over New Zealand passport fraud*, THE GUARDIAN (July 16, 2004), https://www.theguardian.com/world/2004/jul/16/israel. In response to reports that the Australian Secret Services had tapped the Indonesian President's phone, the Indonesian Foreign Secretary declared: "[i]t violates every single decent and legal instrument I can think of on a national level in both countries and on an international level." Helen Davidson and Matthew Weaver, *Indonesia Recalls Ambassador to Australia over spy claims- as it happened*, THE GUARDIAN (Nov. 18, 2013), https://www.theguardian.com/world/2013/nov/18/australia-indonesia-spying-revelations-live.

26. *See* Helmut P. Aust, *Stellungnahme zur Sachverständigenanhörung am 5.* JUNI 2014 1–30, at 14–15 (2014) (Ger.), https://www.bundestag.de/blob/282870/fc52462f2ffd254849bce19d25f72fa2/mat_a_sv-4-1_aust-pdf-data.pdf; Christoph Gusy, *Spionage im Völkerrecht*, 5 NZWEHRR 187, 190–91 (1984); Baker, *supra* note 5, at 1092; Jessica A. Feil, *Cyberwar and Unmanned Aerial Vehicles: Using New Technologies, from Espionage to Action*, 45 CASE W. RES. J. INT'L L. 513, 524–25 (2012); Forcese, *supra* note 2, at 204–05 ("position . . . closest to the truth"); Scott, *supra* note 8, at 223; Radsan, *supra* note 5, at 596; Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 321 (1996); Torsten Stein and Thilo Marauhn, *Völkerrechtliche Aspekte von Informationsoperationen*, 60 ZAÖRV 1, at 32–33 (2000) (referring repeatedly to espionage as being "not prohibited" in public international law).

offer a combination of arguments put forward by the two other strands of thought described above. On the one hand, they insist that because there is neither a treaty nor a rule of customary international law that expressly prohibits espionage, it is impossible to argue that peacetime spying is unlawful.[27] State practice allegedly also contradicts the assumption that espionage is unlawful: as every state is engaged in such activities, it would not be credible for one spying state to sustain the argument that another state's spying is unlawful. Consequently, for example, the Tallinn Manual 2.0 states: "The International Group of Experts agreed that customary international law does not prohibit espionage *per se*."[28] On the other hand, advocates of this "third way" acknowledge that every state is entitled to prosecute domestic and foreign spies, thereby undermining the argument that such conduct was expressly lawful under public international law.[29] Some therefore conclude their analyses by referring to this apparent contradiction as a "paradox."[30]

III. Peacetime Espionage's Lawfulness—An Assessment

In this section, I explain that all three stands of argument that dominate the debate on espionage's lawfulness are inherently contradictory and therefore not persuasive. This comes as no surprise: the discussion on peacetime espionage and international law is to some extent no

27. *See* Aust, *supra* note 26, at 14–15; Baker, *supra* note 5, at 1094; Radsan, *supra* note 5, at 597; Demarest, *supra* note 26, at 342–48.

28. Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 169, rule 32 (2017) (noting, however, that the experts only cited one source for this categorical statement).

29. That was the view taken by the German Constitutional Court (Bundesverfassungsgericht or BVerfG) when deciding whether East German spies engaged in espionage against West Germany could be prosecuted for treason/espionage following unification. The court declared that the special status of espionage in public international law was based on the fact that, on the one hand, public international law did "not prohibit" such activity, while it, on the other hand, allowed states to prosecute a spy even if he/she had only been active abroad. The court went on to describe espionage as "legally ambivalent." BVerfGE 92, 277 ¶¶ 190, 191. The German *Federal Court of Justice* (Criminal Law Division), however, seems to take a slightly different approach. After explaining that espionage was neither permitted nor outlawed or limited in any way by treaty or customary international law, it concludes that espionage was therefore "permitted" in public international law. BGHSt 37, 305, 308; *see also* Kirsten Schmalenbach, Casebook Internationales Recht, 25–26 (2d ed. 2014); Aust, *supra* note 26, at 14–15; Feil, *supra* note 26, at 524–25; Scott, *supra* note 8, 217–26; Demarest, *supra* note 27, at 342–48; Gusy, *supra* note 26, at 190–91 (pointing out the fact that public international law does not regulate espionage also means that a state cannot justify its spying based on public international law).

30. Demarest, *supra* note 26, at 331.

more than a smokescreen, distracting from the genuine issues at stake. On one hand, the term "espionage" is itself an ambiguous concept: there is no universally agreed-upon definition and the nature of espionage activities has changed radically over the last century. On the other hand, I show that international law already regulates most activities commonly associated with espionage, making a distinct body of rules on "espionage" almost superfluous.

A. *Peacetime Espionage is Lawful*

The proposition that espionage is lawful under public international law is the least convincing. There is no known treaty in force that declares espionage as lawful. Admittedly, there are a number of arms control treaties in place that grant other states or international organizations at times far-reaching rights of inspection within state parties' territories.[31] However, the fact that these treaties explicitly grant such rights strongly implies that such conduct would otherwise be unlawful. Relying on customary international law as permitting espionage is just as unjustified. As the ICJ has explained, a rule of customary international law comes into being when there is sufficient state practice and states have justified their practice by referring to international law (*opinio juris*).[32] Regarding espionage, the latter requirement is completely lacking.[33] Not once has a state, accused of espionage, claimed that its

31. *See, e.g.*, Statute of the International Atomic Energy Agency art. XII(A) ¶ 6, *opened for signature* Oct. 26, 1956, 276 U.N.T.S. 3 (entered into force July 29, 1957) [hereinafter IAEA Statute]; Treaty on the Non-Proliferation of Nuclear Weapons art. 3, Jan. 7, 1968, 729 U.N.T.S. 161 (referring to article XII of the IAEA Statute); Treaty between the United States of America and the Union of Soviet Socialist Republics on the Elimination of their Intermediate-Range and Shorter-Range Missiles, U.S.-Russ., art. XI, Dec. 8, 1987, 1657 U.N.T.S. 2 [hereinafter INF Treaty].

32. North Sea Continental Shelf Cases (Ger. v. Den. & Neth.), Judgment, 1969 I.C.J. 3, ¶73–74 (Feb. 20); Int'l Law Comm'n, Draft Conclusions on Identification of Customary International Law, U.N. Doc. A/73/10, at 124–26 (2018); *see also* Statute of the International Court of Justice art. 38(1)(b), Oct. 24, 1945, 33 U.N.T.S. 993.

33. In refusing the Canadian Security Service's application for a warrant to undertake investigative actions in other states, the Federal Court explicitly rejected the CSIS's argument that "the practice of 'intelligence-gathering operations' in foreign states is recognized as a 'customary practice' in international law." Canadian Security Intelligence Service Act, [2008] F.C. 301, ¶ 53 (Can.); Wright goes further and argues "the practice is accompanied not by a sense of right but by a sense of wrong." Wright, *supra* note 20, at 17; *see also* Forcese, *supra* note 2, at 203; Chesterman, *supra* note 2, at 1072; ELLA SHOSHAN, APPLICABILITY OF INTERNATIONAL LAW ON CYBER ESPIONAGE INTRUSIONS 27–28 (2014); Pal Wrange, *Intervention in National and Private Cyber Space and International Law*, FOURTH BIENNIAL CONF. ASIAN SOC'Y INT'L L. 13 (2013); Aaron Shull, *Cyberespionage and International Law*, *in* GIGANET 8TH ANNUAL SYMPOSIUM 7–8 (2013).

conduct was legal. Rather, states have remained silent in the face of such accusations or have flatly denied the charge.[34]

Furthermore, target states have frequently expressed their disapproval of such conduct on the part of other states, even if they have not couched their opposition in legal terms,[35] and have reacted by expelling diplomats of the accused state, even if the diplomats themselves were not involved in the alleged espionage activities.[36] Moreover, in recent times, some heads of government have explicitly stated that espionage violates international law.[37] The prevalence of state practice

34. Wright, *supra* note 20, at 17; Anne Peters, *Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part I*, EJIL: TALK! (Nov. 1, 2013), http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/; SHOSHAN, *supra* note 33, at 28; Demarest, *supra* note 26, at 340.

35. Buchan, *supra* note 3, at 83–84; Chesterman, *supra* note 2, at 1072, Chesterman claims state practice and *opinio juris* "appear to run in opposite directions"; *see also Hollande: alleged US spying 'unacceptable'*, DEUTSCHE WELLE (June 24, 2015), http://www.dw.com/en/hollande-alleged-us-espionage-unacceptable/a-18538105; Andrea Thomas, *US Spying on Germany unacceptable, says Merkel*, WALL STREET J. (July 12, 2014), http://www.wsj.com/articles/u-s-spying-on-germany-unacceptable-says-merkel-1405174452; *Christopher calls Russian espionage 'unacceptable'*, LUDINGTON DAILY NEWS (Feb. 23, 1994), https://news.google.com/newspapers?nid=110&dat=19940223&id=nTRQAAAAIBAJ&sjid=yFUDAAAAIBAJ&pg=2916,4110458&hl=de; *Netanyahu says US spying on Israel 'unacceptable', calls for 'clarifications'*, JERUSALEM POST (Dec. 23, 2013), http://www.jpost.com/Diplomacy-and-Politics/Netanyahu-says-US-spying-on-Israel-unacceptable-calls-for-clarifications-335901; SHOSHAN, *supra* note 33, at 28.

36. Following the arrest of the alleged Russian spy, FBI agent Hanssen, in February 2001, the United States expelled 50 Russian diplomats in March 2001, James Risen and Jane Perlez, *Russian diplomats ordered expelled in a countermove*, N.Y. TIMES (Mar. 22, 2001), http://www.nytimes.com/2001/03/22/world/russian-diplomats-ordered-expelled-in-a-countermove.html; in 2009, Romania expelled three Russian and two Ukrainian diplomats after news surfaced according to which a Romanian and a Bulgarian had sold confidential information to a Ukrainian official, *Romania expelled three Russian diplomats after Ukraine espionage scandal*, NINE O'CLOCK, (May 17, 2009), http://www.nineoclock.ro/romania-expelled-three-russian-diplomats-after-ukraine-espionage-scandal/; in 2012, Canada expelled four Russian diplomats after it was claimed that a Canadian military officer had been spying for Russia. *See* Steven Chase et al., *Ottawa expels Russian diplomats in wake of charges against Canadian*, GLOBE & MAIL (Jan. 19, 2012), http://www.theglobeandmail.com/news/politics/ottawa-expels-russian-diplomats-in-wake-of-charges-against-canadian/article1359125/. In November 2014, Poland expelled a number of Russian diplomats after it became known that a Polish lawyer and a Polish military officer had allegedly been spying for Russia. Vanessa Gera, *Why Poland and Russia are Expelling Each Other's Diplomats*, THE CHRISTIAN SCIENCE MONITOR (Nov. 17, 2014), https://www.csmonitor.com/World/Latest-News-Wires/2014/1117/Why-Poland-and-Russia-are-expelling-each-other-s-diplomats. Indonesia recalled its Ambassador to Australia after it emerged the Australian Secret Services had tapped the Indonesian President's phone. Helen Davidson and Matthew Weaver, *Indonesia Recalls Ambassador to Australia over spy-claims- as it happened*, GUARDIAN (Nov. 18, 2013), https://www.theguardian.com/world/2013/nov/18/australia-indonesia-spying-revelations-live.

37. *See, e.g.*, *China demands halt to 'unscrupulous' US cyber-spying*, *supra* note 24.

regarding espionage does not permit any other conclusion. By necessity, states conduct espionage clandestinely; therefore, such state practice cannot contribute to the creation of customary international law: "It is difficult to see how practice can contribute to the formation or identification of general customary international law unless and until it has been disclosed publicly."[38] The existence of bilateral or multilateral treaties that allegedly limit the scope or outlaw spying between the respective state parties does not permit the conclusion that espionage therefore is a generally lawful activity.[39] Such a conclusion, after all, would imply that the existence of friendship treaties, which usually include references to settling disputes peacefully and respecting each other's independence and sovereignty, similarly confirm the lawfulness of the opposite conduct.

The arguments that peacetime espionage serves international stability, prevents wars, or is simply a facet of self-defense, are even harder to reconcile with reality. Given that espionage is often described as the "world's second-oldest profession,"[40] the vast number of armed conflicts the world has experienced in the last 2000 years contradicts that assumption.[41] To the contrary, manipulated and incomplete intelligence has in fact provided grounds for highly contentious wars, such as the attack on Iraq in 2003.[42] Viewing espionage as just another facet of self-defense under Article 51 of the U.N. Charter is hardly compatible with the purpose of the Charter. Such an assumption renders the

38. Int'l Law Comm'n, Second Rep. Identification of Customary International Law, U.N. Doc. A7/CN.4/672, ¶ 47, fn.144 (2014); *see also* Draft Conclusions on Identification of Customary International Law, *supra* note 32, at 134–135 (referring to "available" state practice); Buchan, *supra* note 3, at 81-82; Alexandra H. Perina, *Black Holes and Open Secrets: The Impact of Covert Action on International Law*, 53 COLUM. J. TRANSNAT'L L. 507-83 (2015).

39. As far as the Five-Eyes- espionage cooperation is concerned, see *supra* note 9. It is contentious whether the relevant, secret treaties really amount to a "No-Spy-Agreement." *See* Statement of Eric King, former Director of "Don't Spy On Us", DEUTSCHER BUNDESTAG (Dec. 15, 2016) (Ger.), https://www.bundestag.de/resource/blob/485038/762e01693b6088894ad6f9729b51bdfa/mat_a_sv-17_king-pdf-data.pdf.

40. Chesterman refers to Sun Tzu's *The Art of War* ("Chapter XIII On the Use of Spies") http://web.mit.edu/~dcltdw/AOW/13.html, generally assumed to have been written in the 6th century BC. Chesterman, *supra* note 2, at 1072 n.2. Spying is also mentioned in the Old Testament. *See, e.g., Joshua* 2:2.

41. Falk, *supra* note 2, at 57–68 (referring to a specific U.S. satellite program); Roland J. Stanger, *Espionage and Arms Control*, in ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 89-90, 99 (Quincy Wright et al. eds., 1962) (pointing out how ineffective espionage has been in detecting weapons capabilities).

42. *MI6 ran 'dubious' Iraq campaign*, BBC NEWS (Nov. 21, 2003), http://news.bbc.co.uk/2/hi/uk_news/3227506.stm; Jeffrey Donovan, *U.S.: CIA takes blame for dubious intelligence on Iraq*, RADIO FREE EUR./RADIO LIBERTY (July 14, 2003), http://www.rferl.org/content/article/1103790.html.

"armed attack" requirement in Article 51 meaningless, because peacetime spying obviously occurs well in advance of an armed attack and therefore certainly would not meet any sensibly defined imminence criterion.[43] In addition, the argument obscures the well-known fact that most espionage in which states engage is unrelated to assessing other countries' military capabilities or possible plans of attack. Rather, espionage activities frequently are directed at gaining economic or strategic advantages by learning about other states' trade and (peaceful) foreign policy goals, which enable the spying state to undermine policies that are incompatible with its own aims.[44] Certainly, plain economic espionage, of which states, such as China and, more recently, the United States[45] stand accused, can only rarely be reconciled with self-defense arguments. Lastly, this view fails to explain the apparent contradiction between the purported legality of espionage in international law and the undisputed right of every state to prosecute and imprison convicted foreign spies. Certainly, besides claiming their citizens' innocence, no state has publicly condemned the arrest and/or incarceration of its citizens for espionage due to the legality, in international law, of such conduct.

B. *Peacetime Espionage is Neither Lawful nor Unlawful*

That espionage is neither lawful nor unlawful in international law is a more convincing proposition. Exponents of this view attempt to bridge the gap between the lack of official statements condemning espionage as a violation of international law and the right of states to prosecute foreign spies.[46] However, the strongest argument in support of espionage's legality is this argument's weakest link: adherents fail to reconcile their arguments with the *Lotus* principle, described above, on which the ICJ still seems to rely in its reasoning.[47] They also fail to

43. Wright, *supra* note 20, at 19; Darien Pun, *Rethinking Espionage in the Modern World*, 18 CHI. J. INT'L L. 353, 366 (2018).

44. National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (2018), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf; *see generally* Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets In Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011*, (Oct. 2011), https://www.hsdl.org/?view&did=720057; Wesley Bruer, *FBI sees Chinese involvement amid sharp rise in economic espionage*, CNN (July 24, 2015), http://edition.cnn.com/2015/07/24/politics/fbi-economic-espionage/.

45. Remme, *supra* note 16.

46. *See supra* note 27 and note 29 and accompanying text.

47. Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, 2010 I.C.J. 2010 403, ¶ 122 (July 22, 2010) (concluding that Kosovo's unilateral declaration of independence was in accordance with international law, the

explain why this apparent "paradox" should exist and what consequences such a hybrid status would or should have.

C. *Peacetime Espionage is Unlawful*

The most convincing proposition is the argument that peacetime espionage is unlawful.[48] It requires little effort to classify many activities associated with espionage as violations of another state's sovereignty, irrespective of the status of espionage in international law. Furthermore, treaties are in place that prohibit, or at least enable the target state to impede, activities commonly associated with espionage.[49] However, whilst states have indeed often penalized other states' espionage activities, there is an evident lack of official statements referring to a violation of international law. Rather, states have generally avoided expressing their disapproval in legal terms, despite having many opportunities to do so.[50] Only very recently have individual states resorted to condemning other states' espionage openly and unequivocally as a violation of international law. Adherents of this view have also failed to draw the logical conclusion that results from their reasoning: only by referring to the unlawfulness of individual espionage activities can they conclude that espionage itself is unlawful. This implies that it is necessary to examine the lawfulness of the individual action in order to be able to draw conclusions as to the general lawfulness of peacetime espionage.[51] Though this is the logical approach, it also risks rendering superfluous the discussion on whether "espionage" as a whole is lawful.

IV. Espionage and International Law—"The Riddle of the Sands"?

Why has public international law not produced a compelling answer to the question of whether espionage is lawful or unlawful?[52] There are two main reasons for this: firstly, there is no concise, universally agreed

ICJ deemed it sufficient to establish a lack of any legal prohibition); *see also* Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Declaration Simma, 2010 I.C.J. 403, 479 (July 22, 2010) (accusing the I.C.J. of "fail[ing] to seize a chance to move beyond this anachronistic, extremely consensualist vision of international law . . . by upholding the Lotus principle").

48. *See Ex parte* Quirin, 317 U.S. 1 (1942).

49. *See, e.g.*, United Nations Convention on the Law of the Sea, art. 19(2), Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS]; Convention on International Civil Aviation, art 9(a), (c), Dec. 7, 1944, 15 U.N.T.S. 295.

50. Alison Pert, *Australia's Jakarta Phone-Tapping: Was it Illegal?* Inside Story (Nov. 27, 2013), at 2, http://insidestory.org.au/australias-jakarta-phone-tapping-was-it-illegal; Skinner, *supra* note 2, at 1182–83.

51. *See* Tallinn Manual 2.0, *supra* note 28, at 170 rule 32; Pun, *supra* note 43, at 359.

52. Forcese, *supra* note 2, at 185, 201–05, he argues that the "international law of spying is best described as 'underdeveloped'."

upon definition of "espionage." Continuous technological progress is rapidly changing the means of espionage, making it fiendishly difficult to find a precise definition. Secondly, and more importantly, there is no need for a specific legal regime to deal with peacetime espionage. International law already regulates most activities commonly associated with the term "espionage."

A. *Definition of "Peacetime Espionage"*

There is no general agreement as to the definition of peacetime espionage[53]—some authors agree with the definition used in this Article, namely that espionage includes only the gathering by one state of another state's secret, not publicly available information.[54] Some want to include the gathering of information from open sources, but usually go on to exclude such activities from their legal discourse. Others believe espionage includes the analysis of the information obtained. Others, again, believe espionage includes covert actions undertaken against another state's government, although most authors attempt to exclude such actions from their analysis. Then there are various possible scenarios concerning the actors and victims of peacetime espionage: some only want to discuss espionage by a state directed against another state, others include economic espionage directed against non-state actors when conducted by a state, and others again include espionage by non-state actors against other non-state actors.[55] As Romero has summarized, "Espionage and intelligence collection will mean

53. In public international law, only the Hague Convention Respecting the Laws and Customs of War on Land of 1907 (Articles 29–31) and the Geneva Conventions of 1949 deal with spying and spies—however, these treaties only apply to espionage in times of war. *See* Falk, *supra* note 2, at 79 n.28; Talmon, *supra* note 2, at 16; Skinner, *supra* note 2, at 1181–82; Chesterman, *supra* note 2, at 1073-74; Mack, *supra* note 2, at 3; Forcese, *supra* note 2, at 181–84; Demarest, *supra* note 26, at 322–25; Lubin, *supra* note 12, at 206–07.

54. *See also* Buchan, *supra* note 3, at 65; Demarest, *supra* note 26, at 325–26; Pun, *supra* note 43, at 358.

55. For examples providing various, often conflicting definitions of espionage, *see* Sanchez, *supra* note 7, at 73 (distinguishing between five different kinds of intelligence gathering which, according to him, all have "potential implications for international law"); Gusy, *supra* note 26, at 195–96 (attempting to differentiate between "simple spying" and other activities); Stein & Marauhn, *supra* note 26, at 1–40 (attempting to distinguish between various kinds of "information operations" while only equating the "offensive information operations" with espionage); Baker, *supra* note 5, at 1093–94; Forcese, *supra* note 2, at 181–84 (providing a table explaining six different types of intelligence collections); Stefan Kirchner, *Beyond Privacy Rights: Crossborder Cyber-Espionage and International Law*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 369, 370–71 (2014); Mack, *supra* note 2, at 6 (providing a detailed interpretation of "espionage," including some, while excluding other, activities); Radsan, *supra* note 5, at 599–601; Romero, *supra* note 8, at 15,

something different to each nation."[56] Based on this hazy view of what "espionage" actually means, it is no surprise that there is no agreement as to the legality or illegality of such conduct.

Furthermore, the nature of espionage has undergone an enormous transformation in the last 100 years. Traditionally, espionage mainly involved "cloak-and-dagger spies," operating in foreign countries and attempting to steal or otherwise illicitly obtain secret information, for example, by bribing foreign officials.[57] Such conduct, of course, still takes place, as evidenced by the Russian sleepers in the United States.[58] Nowadays, however, states very often engage in remote espionage, i.e., by satellite or cyber espionage. These more modern modi operandi raise different legal issues than the traditional forms of spying, based on the simple fact that the spy almost never physically enters the target state's territory, but remains in his home state while spying.[59]

The wide range of activities encompassed by the term "peacetime espionage" underscores the necessity to judge the lawfulness of every such activity separately. Discussing the lawfulness of peacetime espionage by referring to this blanket term is unhelpful and does not address the genuine legal issues.

B. *Regulation of Espionage Activities in International Law*

Once the term "peacetime espionage" is broken down into each individual espionage activity, it will become evident that in most cases international law *does* provide answers. In the next section I show that most, if not all, such activities are unlawful under public international law according to widely accepted general rules in customary international law that do not refer to espionage specifically.[60] This also helps explain

17, 33–38; SHOSHAN, *supra* note 33, at 14–15; Sulmasy & Yoo, *supra* note 8, at 625; Deeks, *supra* note 8, 298–300.

56. Romero, *supra* note 8, at 9.

57. Falk, *supra* note 2, at 50.

58. Thom Patterson, *The Russian spies living next door*, CNN (July 19, 2017), https://edition.cnn.com/2017/07/19/us/russian-spies-united-states-declassified/index.html; Chris McGreal, *FBI breaks up alleged Russian spy ring in deep cover*, GUARDIAN (June 28, 2010), https://www.theguardian.com/world/2010/jun/29/fbi-breaks-up-alleged-russian-spy-ring-deep-cover.

59. Falk, *supra* note 2, at 50–51; Kirchner, *supra* note 55, at 369-78; Mack, *supra* note 2, at 25–26; Romero, *supra* note 8, at 33-38; SHOSHAN, *supra* note 33, at 7–8, 13–14.

60. TALLINN MANUAL 2.0, *supra* note 28, at 169–70 (noting that the experts involved nevertheless argue that "international law does not prohibit espionage *per se*"). *See also* Pert, *supra* note 50, at 2; Korff, *supra* note 18, at 6 (limiting discussion to spying activities that amount to the "deliberate" commission of "criminal offences" in the "targeted state" and that harm that state's "interests," yet effectively covering most acts of espionage); Chesterman, *supra* note 2, at 1127 (referring to a "normative context . . . within which intelligence collections takes place"); Forcese,

the lack of explicit condemnations of espionage as unlawful by states. Possibly, the initiation of repeated discussions on peacetime espionage's lawfulness serves another purpose: invariably concluding such discussions with the assertion that the relationship of peacetime espionage and international law is like "the riddle of the sands," i.e., undeterminable, enables the respective author to imply that such conduct may well be legal—a conclusion many states are bound to find highly satisfactory.

1. "Traditional" Espionage

Covert espionage activities conducted on the territory of the target state, perhaps best described as the "traditional" form of spying, have fueled public imagination for generations. Such activities include the sending of agents or citizens of the spying state to the target state so that they can obtain secret/confidential material there in various ways. Another alternative is for state agents to convince officials of the target state to provide the desired information, by way of bribery or blackmail.[61] Lastly, states utilize their military installations, embassies or consular offices in order to spy on the host country by, for example, installing espionage equipment on/in the buildings.[62] Of course, many states engage in a combination of such spying activities.

---

supra note 2, at 209 ("Public international law rules pertaining to spying are best described as a checkerboard of principles, constraining some practices in some places and in relation to some actors, but not in other cases in relation to other actors."). Kirchner claims that there is no "general rule" in international law as far as espionage is concerned, but that there are "specific rules concerning espionage under specific conditions or 'situation[s].'" Kirchner, *supra* note 55, at 372; SHOSHAN, *supra* note 33, at 14, 30–31; Wrange, *supra* note 33, at 12.

61. For example, it is alleged that the CIA paid a German employee of the German External Security Service, the BND, € 90000 for passing on secret documents between 2008 and 2014. The employee was arrested in 2014 and has since been sentenced to eight years in prison for high treason. *See Landesverrat: Ex-BND-Mitarbeiter legt Geständnis ab*, DIE ZEIT (Nov. 16, 2015), http://www.zeit.de/politik/2015-11/bnd-mitarbeiter-cia-spion-landesverrat-prozess; *see also* Philip Oltermann, *No one trusted me with anything, says German triple agent*, GUARDIAN (Mar. 17, 2016), http://www.theguardian.com/world/2016/mar/17/german-triple-agent-markus-reichel-started-spying-because-he-felt-under-appreciated.

62. For example, it has been claimed that the United States is monitoring German government communications from its consulate in Frankfurt and its embassy in Berlin. *See Die Spionage-Botschaft*, FRANKFURTER ALLGEMEINE ZEITUNG (Oct. 26, 2013), http://www.faz.net/aktuell/politik/ausland/ausspaeh-affaere-die-spionage-botschaft-12635377.html; Von Konrad Lischka und Matthias Kremp, *NSA-Spähaffäre: So funktionieren die Abhöranlagen in US-Botschaften*, DER SPIEGEL (Oct. 28, 2013), http://www.spiegel.de/netzwelt/netzpolitik/nsa-spaehskandal-so-funktionieren-die-abhoeranlagen-in-us-botschaften-a-930392.html; *Das Dachgeschoss gehört den Spionen*, FRANKFURTER ALLGEMEINE ZEITUNG (Oct. 27, 2013), http://www.faz.net/aktuell/politik/inland/amerikanische-botschaft-in-berlin-das-dachgeschoss-gehoert-den-spionen-12635981.html.

Common to these undertakings is the violation of the host state's territorial sovereignty. Although it is difficult to provide a precise definition of the term "sovereignty" as understood in public international law today,[63] there is no serious doubt that sovereignty includes a state's right to demand respect for its territorial integrity and political independence.[64]

As early as 1949, the ICJ stressed the importance of the concept of sovereignty: "between independent states, respect for territorial sovereignty is an essential foundation of international relations."[65] Territorial sovereignty includes a state's right to govern effectively to the exclusion of other states on its territory. Consequently, no state has the right to exercise governmental functions on another state's territory without that state's permission.[66] The PCIJ underlined this in 1927 when it declared that, "now 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."[67] The arbitrator in the *Las Palmas* case was even more explicit:

> 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. The development of the national organisation of States during the last few centuries and, as a corollary, the development of international law, have established this principle

63. The precise meaning and scope of the term "sovereignty" in international law need not be examined in this context. It is, however, worth noting that the concept as such is a much contested one. *See* MATTHEW C. R. CRAVEN, THE DECOLONIZATION OF INTERNATIONAL LAW: STATE SUCCESSION AND THE LAW OF TREATIES 7–92 (2007); KAREN KNOP, DIVERSITY AND SELF-DETERMINATION IN INTERNATIONAL LAW 109–211 (2002); ANTONY ANGHIE, IMPERIALISM, SOVEREIGNTY AND THE MAKING OF INTERNATIONAL LAW (2005).

64. U.N. Charter art. 2, ¶ 4; League of Nations Covenant art. 10; *see also* Wright, *supra* note 20, at 24; Stein & Marauhn, *supra* note 26, at 23–24; Chesterman, *supra* note 2, at 1081–82; Forcese, *supra* note 2, at 185, 198; JOHN KISH, INTERNATIONAL LAW AND ESPIONAGE 83-84 (1995); SHOSHAN, *supra* note 33, at 32–34.

65. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 35 (Apr. 9); *see also* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168 (Dec. 19).

66. Pert, *supra* note 50, at 2–3; Korff, *supra* note 18, at 4–5; Forcese, *supra* note 2, at 185, 198; KISH, *supra* note 64, at 83; SHOSHAN, *supra* note 33, at 32–34, 37; Wrange, *supra* note 33, at 5; Buchan, *supra* note 3, at 68; Wolff Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, 4TH INT'L CONF. ON CYBER CONFLICT 8 (2012), http://insct.syr.edu/wp-content/uploads/2015/06/Heinegg_Sovereignty_In_Cyberspace.pdf.

67. *S.S. Lotus*, 1927 P.C.I.J. (ser. A) No. 10, at 18.

> of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations.[68]

Turning to the various "traditional" espionage activities described above, it is evident that they all violate the target state's sovereignty. By either illicitly obtaining secret information themselves or by bribing/blackmailing public officials to do so for them, the state thus engages in espionage and is effectively exercising its own executive or governmental power on the target state's territory without the target state's permission.[69] Undoubtedly, the spying state incurs state responsibility with respect to such activities: the secret service officials are representatives and therefore agents of the spying state, and they act on its instructions when illicitly obtaining confidential material.[70] In this context, it is irrelevant whether the spies are acting on their own or inciting target state officials to act for them, because, in both situations, the spying state exerts effective control over the operation.[71]

Furthermore, state agents who illicitly obtain information in such a manner are violating the target state's domestic laws. When acting on

---

68. Islands of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (1928), http://legal.un.org/riaa/cases/vol_II/829-871.pdf.

69. Korff, *supra* note 18, at 5; KISH, *supra* note 64, at 83–88; Delupis, *supra* note 18, at 67–68; Donald K. Anton, *The Timor Sea Treaty Arbitration: Timor-Leste Challenges Australian Espionage and Seizure of Documents*, 18 ASIL INSIGHTS 3 (2014). Gusy, on the other hand, claims that a state's exclusive right to exercise governmental functions within its territory only prohibits a foreign state from engaging in activities which impede the target state's exercise of governmental authority. He goes on to argue that a foreign state's espionage activities regularly do not limit a state's ability to govern effectively and therefore do not violate territorial sovereignty. *See* Gusy, *supra* note 26, at 192–94. However, this argument is not convincing, as it contradicts the generally accepted definition of territorial sovereignty, which prohibits the exercise of power by a foreign state on another state's territory "in any form." An actual impediment is not required. Romero, *supra* note 8, at 17–18. Romero relies on the clean-hands-principle in order to negate a violation of territorial sovereignty, an argument which I will address in due course.

70. Martin Scheinin (Special Rapporteur on The Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism), *Compilation of Good Practices on Legal and Institutional Frameworks and Measures That Ensure Respect for Human Rights by Intelligence Agencies While Countering Terrorism, Including on Their Oversight*, 13–14, U.N. Doc. A/HRC/14/46 (May 17, 2010), https://digitallibrary.un.org/record/684869/files/A_HRC_14_46-EN.pdf.

71. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/10, art. VIII (2001); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27); Application of Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. 43, ¶¶ 392, 398, 407 (Feb. 26). *See also* Gusy, *supra* note 26, at 189–90; Wrange, *supra* note 33, at 6.

their own, the spies will regularly be engaged in theft and/or unlawful entry, not to mention violating data protection and privacy laws. When bribing or blackmailing a target state official on the target state's territory, the violation of domestic criminal law is even more obvious. Even when the blackmail or bribery occurs outside of the target state's territory, the spies will be participating and instigating the target state official to commit crimes, such as treason, on the target state's territory.[72]

A state that instructs its agents to commit a criminal offense in another state, however, violates public international law. Such conduct infringes on another aspect of territorial sovereignty—it amounts to a violation of the target state's "enforcement jurisdiction."[73] As Korff has convincingly explained, "if agents of one state (the spying state) deliberately commit criminal offenses in another state (the targeted state) that harm the interests of the targeted state and its citizens and officials, that constitutes an internationally unlawful act on the part of the spying state."[74] Although the prohibition on violating another state's domestic laws may not apply to such laws that themselves disregard basic human rights, there is no reason to assume that this exception should apply to the crimes of theft, treason, or espionage.[75] By committing crimes on the target state's territory, the spying state, represented by its agents, is acting unlawfully under public international law.[76]

A Canadian federal court has provided a succinct description of this legal situation. In response to an application by the Canadian Security Intelligence Service (CSIS) for a warrant to engage in investigative activities in another state, the Court, in rejecting the application, held:

> The intrusive activities that are contemplated in the warrant sought are activities that clearly impinge upon the above-mentioned 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. By authorizing

72. STRAFGESETZBUCH [STGB] [PENAL CODE], §§ 94, 99 (Ger.).

73. Craig Forcese, *The Ugly Canadian? International Law and Canada's New Covert National Security Vision*, (May 28, 2015), http://craigforcese.squarespace.com/national-security-law-blog/2015/5/28/the-ugly-canadian-international-law-and-canadas-new-covert-n.html.

74. Korff, *supra* note 18, at 6; *see also* Wright, *supra* note 20, at 13 ("It belongs to each state to define peacetime espionage, sedition, subversion, . . . as it sees fit, and it is the duty of other states to respect such exercise of domestic jurisdiction. Thus, any act by an agent of one state committed in another state's territory, contrary to the laws of the latter, constitutes intervention, provided those laws are not contrary to the state's international obligations.").

75. Wright, *supra* note 20, at 12–13.

76. Korff, *supra* note 18, at 6; Wright, *supra* note 20, at 12; Wrange, *supra* note 33, at 13.

> such activities, the warrant would therefore be authorizing activities that are inconsistent with and likely to breach the binding customary principles of territorial sovereign equality and non- intervention, by the comity of nations. These prohibitive rules of customary international law have evolved to protect the sovereignty of nation states against interference from other states. Extraterritorial jurisdiction, prescriptive, enforcement or adjudicative, exists under international law and is subject to the strict limits under international law based on sovereign equality, non-intervention and the territorial principle.[77]

Activities associated with "traditional" espionage thus disregard the target state's right to unlimited governmental authority and its exclusive enforcement jurisdiction within its own territory. Whether stealing documents, bugging premises or bribing/blackmailing target state officials, the spying state undertaking such actions is violating public international law.

When a state exploits the permitted presence of its representatives on the target state's territory in order to engage in espionage, the legal situation is usually even more transparent. Not only do the arguments just outlined apply to the spying state's conduct,[78] but the spying state usually will also be violating treaty law.

Conduct utilizing the spying state's embassy or consulate on the target state's territory for espionage activities is unlawful.[79] The Vienna Convention on Diplomatic Relations and the Vienna Convention on Consular Relations regulate the use of embassies and consular offices. Regarding embassies, Article 41(3) of the Vienna Convention on Diplomatic Relations stipulates:

---

77. Canadian Security Intelligence Service Act, [2008] F.C. 301, Summary (1) ¶¶ 49–55 (Can.).

78. *Id. See also* Pert, *supra* note 50, at 2–3; Korff, *supra* note 18, at 6. For a different view, see Brown & Poellet, *supra* note 8, at 133–34 (arguing that state practice does "not prohibit spying that might involve crossing international borders" and has led "to the establishment of an exception to traditional rules of sovereignty"). As already pointed out, this argument is unconvincing. An exception to the "traditional rules of sovereignty" as a rule of customary international law could only have come about if the state practice Brown and Poellet claim exists were accompanied by corresponding *opinio juris*. This, however, is not the case as I have already explained.

79. Philip Oltermann, Julian Borger & Nicholas Watt, *Germany Calls in UK Ambassador Over Spy Claims*, GUARDIAN (Nov. 5, 2013), http://www.theguardian.com/world/2013/nov/05/germany-summons-uk-ambassador-spy-claims-berlin; Korff, *supra* note 18, at 6; Delupis, *supra* note 18, at 69.

> [t]he premises of the mission must not be used in any manner incompatible with the functions of the mission as laid down in the present Convention or by other rules of general international law or by any special agreements in force between the sending and the receiving State.[80]

Article 3 enumerates such permissible functions of the mission. With respect to the gathering of information, Article 3(d) mandates that one such function is the "ascertaining *by all lawful means*[81] conditions and developments in the receiving State, and reporting thereon to the Government of the sending State." Furthermore, Article 41(1) obliges all diplomats "to respect the laws and regulations of the receiving State" and "not to interfere in the internal affairs of that State."[82] Engaging in the espionage activities described above from within an embassy therefore not only infringes on the target state's sovereignty, but is also incompatible with Articles 41(1), 41(3), and 41(3)(d) of the Vienna Convention on Diplomatic Relations.[83]

The same is true for espionage activities undertaken from within consular offices.[84] Such conduct violates Articles 55(1), 55(2), and 5(c) of the Vienna Convention on Consular Relations.[85] Article 55(1) obliges all diplomats to respect the receiving state's "laws and regulations" while Article 55(2) prohibits the use of the "consular premises . . . in any manner incompatible with the exercise of consular functions" as defined in Article 5.[86]

---

80. Vienna Convention on Diplomatic Relations art. 41(3), Apr. 18, 1961, 500 U.N.T.S. 95.

81. Author's emphasis.

82. Vienna Convention on Diplomatic Relations art. 41(1), Apr. 18, 1961, 23 U.ST. 3327, 500 U.N.T.S 95.

83. *U.S. v. Iran*, 1980 I.C.J. 3, ¶ 84-86; Pert, *supra* note 50, at 2-3; Talmon, *supra* note 2, at 21–22; Talmon, *supra* note 7, at 8; Aust, *supra* note 26, at 15; Chesterman, *supra* note 2, at 1087–90; Forcese, *supra* note 2, at 200; Kirchner, *supra* note 55, at 373–74; SANDERIJN DUQUET & JAN WOUTERS, LEGAL DUTIES OF DIPLOMATS TODAY: THE CONTINUING RELEVANCE OF THE VIENNA CONVENTION 19–20 (Leuven Ctr. for Global Governance Studies, Working Paper No. 146) (2015); *see generally* Helmut Kreicker, *Konsularische Immunität und Spionage*, 3 ZEITSCHRIFT FÜR INTERNATIONALE STRAFRECHTSDOGMATIK 129 (2014).

84. Pert, *supra* note 50, at 3; Talmon, *supra* note 2, at 21–22; Talmon *supra* note 7, at 8; Aust, *supra* note 26, at 15; Kreicker, *supra* note 83, at 129–33; Chesterman, *supra* note 2, at 1087–90; Forcese, *supra* note 2, at 200; Kirchner, *supra* note 55, at 373–74; DUQUET & WOUTERS, *supra* note 83, at 19–20 .

85. United States Diplomatic and Consular Staff in Tehran, *supra* note 4, ¶ 84–86.

86. Article 5(c) only permits the gathering of information in the receiving state "by all lawful means." *See Vienna Convention on Consular Relations* art. 5(c), Apr. 24, 1963, 596 U.N.T.S. 261.

Whether or not treaty law (also) prohibits the use of military installations on the target state's territory for espionage depends on the applicable bilateral or multilateral treaty regulating the specific deployment. It is, however, reasonable to assume that most such treaties contain prohibitions as far as espionage is concerned. Certainly, among NATO member states, spying from within military installations is unlawful.[87] Under Article 2 of the NATO Status of Forces Treaty, all members of NATO forces deployed to other member states as well as any "civilian component" are required to respect the laws of the "receiving State" which, of course, include criminal law prohibitions on espionage, theft, etc.[88] Article VII mandates that members of the military are prohibited from engaging in acts of "espionage" when deployed in the target state: paragraph 2(b) grants the receiving state "exclusive jurisdiction" as far as the prosecution of "offences relating to [the] security" of the receiving state are concerned, while paragraph 2(c) states that both "treason against the state" and "espionage" are to be viewed as such offenses.[89] Provisions sometimes included in supplementary agreements,[90] according to which the states concerned are obliged to cooperate on issues relating to the security of the sending state's military forces and those forces' right to install/erect means of telecommunication, do not provide any justification for spying in the receiving state.[91]

The same prohibition applies to ships entering another state's territorial sea.[92] The United Nations Convention on the Law of the Seas (UNCLOS)[93] provides an extension of a state's sovereignty to its territorial sea,[94] which is at the same time subject to other states' right of innocent passage.[95] However, it later excludes activities associated with espionage from that right:

87. Talmon, *supra* note 2, at 22; Talmon, *supra* note 7, at 8–10; KISH, *supra* note 64, at 84–85.

88. Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces art. 2, June 19, 1951, 4 U.S.T. 1792.

89. *Id.* art. 7.

90. *See, e.g.*, Agreement to Supplement the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces with respect to Foreign Forces stationed in the Federal Republic of Germany and Protocol of Signature, art. 3(2)(a), 60(1), Aug. 3, 1959, 14 U.S.T. 689. (Applicable to Germany); Agreement between the United States of America and Romania Regarding the Activities of United States Forces Located on the Territory of Romania, art. II(1), U.S.-Rom., Dec. 6, 2005, 80 Stat. 271.

91. Talmon, *supra* note 2, at 23–24; Talmon *supra* note 7, at 9.

92. KISH, *supra* note 64, at 88–97; Delupis, *supra* note 18, at 69.

93. UNCLOS, *supra* note 49.

94. *Id.* art. 2(1), art. 3 (defining territorial sea).

95. *Id.* art. 17.

> Passage of a foreign ship shall be considered to be prejudicial to the peace, good order or security of the coastal State if in the territorial sea it engages in any of the following activities: . . . (c) any act aimed at collecting information to the prejudice of the defence or security of the coastal State; . . . (j) the carrying out of research or survey activities; (k) any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State; . . .[96]

Article 25 further strengthens the coastal state's rights by permitting it to "prevent" non-innocent passage and "suspend temporarily" the right of innocent passage if this "is essential for the protection of its security."[97]

A state's sovereignty does not only extend to its territorial sea, but also to the airspace above its territory including its territorial sea.[98] Contrary to the legal situation regarding the territorial sea, there is no generally applicable treaty granting foreign aircraft the equivalent of the right to innocent passage as far as a state's airspace is concerned.[99] Rather, foreign aircraft generally require the consent of the state whose airspace is to be crossed.[100] Already in 1902, realizing the potential for espionage during overflights over foreign territory, the Institute of International Law, while still being more generous as far as a right of overflight is concerned, passed a resolution that stated in its Article 7: "L'air est libre . . . Ces droits sont relatifs à la repression de l'espionnage . . . ."[101] Subsequent treaties, which permitted state parties to ban foreign aircraft from flying over certain areas, reaffirmed this sentiment.[102] Articles 1 and 2 of the Convention on International Civil Aviation (the Chicago Convention)[103] confirm the state parties' sovereignty over the airspace above their respective territory and territorial sea. The

96. *Id.* art. 19(2).

97. *Id.* arts. 25(1), (3).

98. KISH, *supra* note 64, at 97–101.

99. KISH, *supra* note 64, at 97.

100. *Id.*

101. Institut de droit international, 19 ANNUAIRE DE L'INSTITUT DE DROIT INT'L 32 (1902) (noting that while the air space above a state's territory was open to all, the resolution did grant states the right to suppress espionage as "[t]he air is free . . . these [the rights necessary for a state to preserve itself] concern the suppression of espionage . . .").

102. Convention Relating to the Regulation of Aerial Navigation art. III, Oct. 13, 1919, 11 L.N.T.S. 173; Convention on Commercial Aviation (Inter-American) art. V, Feb. 20, 1928, 129 L.N.T.S. 225.

103. Convention on International Civil Aviation art. I–II, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 296.

Convention goes on to allow some aircraft to fly into or transit another state's national airspace without prior permission.[104] However, this right does not extend to state aircraft,[105] scheduled air services,[106] and pilotless flights.[107] Although the Convention contains no specific regulation outlawing espionage activities, it does allow state parties to "restrict or prohibit uniformly the aircraft of other States from flying over certain areas of its territory"[108] and to force aircraft nevertheless entering such areas to land at an airport within its territory.[109] While the Chicago Convention and its predecessors thus do not explicitly prohibit the gathering of information as UNCLOS does, they do permit states to ban the use of their airspace over areas they wish to conceal from other states. The ICJ, too, has confirmed the prohibition of overflights in order to spy on other states. When assessing what it described as "high-altitude reconnaissance flights"[110] by the United States over Nicaraguan territory, it concluded: "The principle of 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."[111] That is also the rationale behind the conclusion of the Treaty on Open Skies, which allows unarmed observation flights over the state parties' territories, and would otherwise be superfluous.[112]

In summary, peacetime espionage is always unlawful when it involves activities that unfold on the target state's territory, including its territorial sea and airspace. By engaging in such activities, the spying state is exercising governmental functions on the target state's territory, thus violating the latter's territorial sovereignty. Even when treaties explicitly permit states to maintain an official or other presence on another state's territory, these typically contain clauses outlawing activities commonly associated with espionage.

---

104. *Id.* art. V.

105. *Id.* art. III.

106. *Id.* art. VI.

107. *Id.* art. VIII.

108. *Id.* art. IX(a).

109. *Id.* art. IX(c).

110. *Nicar. v. U.S.*, 1986 I.C.J. 14, ¶ 91.

111. *Id.* ¶ 251*; see also Mutual Security Act of 1960: Hearing Before the S. Comm. on Foreign Relations*, 86th Cong. 2 (1960) (statement of U.S. Sec'y of State Christian Herter).

112. Treaty on Open Skies, Mar. 24, 1992, S. TREATY DOC. NO. 102-37 (1992) (the treaty was concluded by OSCE member states).

2. "Modern" Espionage

Since the second half of the 20th century, however, the way states spy has changed irrevocably: technological progress has created new opportunities for espionage, which are more difficult to detect and potentially pose serious challenges to international law. Beginning in the 1960s, states have been deploying reconnaissance satellites in outer space, which, frequently, are utilized to spy on other states' military installations. More recently and more ubiquitously, states have turned to an even more modern tool, namely cyber espionage.

a. Violation of Territorial Sovereignty

The difficulty in assessing whether the use of reconnaissance satellites or the conduct of cyber espionage are lawful in public international law originates from the seeming lack of a violation of territorial sovereignty that is inherent to other traditional espionage activities. Spying by government officials in another state, bribing foreign government officials in order to obtain secret information, and using embassies or military bases abroad in order to spy on foreign governments all involve the exercise of executive or governmental power by one state on the territory of another without permission. Such actions violate the target state's territorial sovereignty and political independence and are thus contrary to international law.

By contrast, satellite and cyber espionage usually do not require the physical presence of a "spy" in the target state's territory. Rather, states often conduct such espionage remotely, without sending an agent abroad. This makes it difficult to claim a violation of the target state's territorial sovereignty because satellites operate in outer space,[113] which is not subject to a claim of territorial sovereignty.[114] This precludes a claim of unlawfulness based on a violation of a state's territorial sovereignty,[115] even when the satellites are reconnoitering above another

113. There is no clear rule in international law on where national airspace ends and outer space begins. Kish explains that the "zone for the boundary between" national airspace and outer space is found at the "upper flight height of aircraft and the lower orbit of spacecraft." KISH, *supra* note 64, at 115.

114. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, art. II, Jan. 27, 1967, 610 U.N.T.S. 205. This leads Kish, for example, to conclude that espionage from outer space is permissible under international law, *see* KISH, *supra* note 64, at 115–20.

115. The same applies to espionage undertaken on the high seas. According to Article 89 of UNCLOS, the high seas (including the airspace above) are not subject to a claim of territorial sovereignty by any state. UNCLOS, *supra* note 49, art. 89. All ships, including warships, are

state's territory.[116] The same is true of cyber espionage, as the monitoring and intrusion of electronic databases often occurs from within the spying state's territory.[117]

The European Court of Human Rights (ECHR), in dealing with a related—though by no means identical—situation, rejected the claim that such activities necessarily violate another state's territorial sovereignty. Two applicants living in Uruguay claimed that the German External Security Service (BND) had unlawfully monitored their telecommunications from sites in Germany. The ECHR, however, concluded that there was no violation of territorial sovereignty:

> Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants have failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law.[118]

---

generally only subject to the flag state's jurisdiction. *Id.* art. 92, 95. The legal situation regarding espionage on the high seas is no different than in cases of cyber or satellite espionage. However, it is much more difficult to imagine situations unfolding on the high seas reaching the threshold of a prohibited intervention in another state's affairs (that is, without further measures, such as cyber espionage or boarding another ship), which is why this article does not analyze this variant in any detail. The mere surveillance of other ships on the high seas is not an activity associated with espionage because neither the surveillance itself nor the ship surveilled are "secret". Such activity is more akin to the gathering of "open" information, which does not qualify as espionage. Kish disagrees. *See* KISH, *supra* note 64, at 102–09. However, the examples of state practice he mentions were either contentious between the states concerned (Pueblo Incident of 1968) or the flag state had consented to the surveillance of the respective ships ("Santa Maria" (1961); "Achille Lauro" (1985)). Furthermore, the treaties he cites that permit surveillance seem to confirm the unlawfulness of such conduct absent just such a treaty. He also mostly refers to cases of surveillance, which, as previously explained, is not espionage.

116. Falk, *supra* note 2, at 50–51.

117. Pert, *supra* note 50, at 2–3; Talmon, *supra* note 2, at 19–20; Talmon, *supra* note 7, at 10; Korff, *supra* note 18, at 7; Stein and Marauhn, *supra* note 26, at 32–33. *But see* Peters, *supra* note 34, at 2. Peters seems to view the spying on communications in Germany even from within the United States as the exercise of U.S. jurisdiction in Germany which, according to her, might amount to a violation of Germany's sovereignty; *see also* SHOSHAN, *supra* note 33, at 18, 36–38 (making the interesting argument that communications that can clearly be identified as government communications (such as e-mail addresses with the internet address ".gov") are subject to that state's sovereignty); Shull, *supra* note 33, at 5; von Heinegg, *supra* note 66, at 9–13.

118. Weber and Saravia v. Germany, 2006-XI Eur. Ct. H.R. 1, 20 (2006); Canadian Security Intelligence Service Act, [2009] F.C. 1058 (Can).

The ECHR's decision reinforces the view that a monitoring state does not violate a target state's territorial sovereignty when the monitoring activity occurs remotely. Nevertheless, this analysis does not address the whole range of cyber espionage activities. The ECHR's decision concerned a case in which German authorities intercepted signals during transmission. Frequently, however, states attempt to obtain data stored on servers located in the target state. In these situations, the data's interception occurs at its source within the target state's territory, not during transmission.

As territorial sovereignty encompasses a state's "right to exercise therein, to the exclusion of any other State, the functions of a State,"[119] which means a state "may not exercise its power in any form in the territory of another state,"[120] such actions necessitate a separate, different evaluation. The intrusion of one state into another state's data violates the target state's territorial sovereignty when the data is stored on servers, which require physical infrastructure on the target state's territory.[121] State practice confirms this view.[122] By carrying out such an act, the spying state is unlawfully exercising governmental authority on the target state's territory.[123] The fact that the initial action occurs remotely is irrelevant, as the intrusion and interception takes place on the target state's territory. Cyber espionage, undertaken in order to obtain data stored on servers in the target state, is therefore unlawful.

b. Intervention in Another State's Affairs

The conclusion that cyber espionage can be a violation of territorial sovereignty, however, only applies when the espionage activities involve an intrusion on the target state's territory. This is very uncommon: in

119. *Neth. v. U.S.*, 2 R.I.A.A. at 838.

120. *S.S. Lotus*, 1927 P.C.I.J. (ser. A) No. 10, at 18.

121. Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123, 125–26 (2013); *see also* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 15, 18 (Michael N. Schmitt ed., 2013); TALLINN MANUAL 2.0, *supra* note 28, at 13.

122. *See generally* U. K. GOVERNMENT, NATIONAL CYBER SECURITY STRATEGY 2016-2021, 33–45 (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf; BUNDESMINISTERIUM DES INNERN, CYBER-SICHERHEITSSTRATEGIE FÜR DEUTSCHLAND 27–37 (2016), https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf; THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 12–15 (2011).

123. INTERNATIONAL TELECOMMUNICATION UNION (ITU), UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE 277-78 (2012), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf; SHOSHAN, *supra* note 33, at 36-39; Buchan, *supra* note 3, at 71. *Cf.* Peters, *supra* note 34, at 2.

many cases, it remains unclear where the obtained data was stored at the time of the cyber intrusion. Emails, for example, are often stored on servers located in a number of states and not necessarily in the state from which the emails originated.[124] Furthermore, target state officials may send emails while they travel abroad, which involves accessing servers located in various states. Even emails sent and received within one state are sometimes routed via servers in another state.[125] To complicate matters further, data is nowadays increasingly stored in one of many available clouds, which are frequently located outside the user's home state.[126] Lastly, some states have the capacity to monitor internet communications in real time.[127] These developments reinforce the limitations of the territorial sovereignty argument outlined above with respect to the legality of cyber espionage. Thus, the location of data obtained at the time of a cyber intrusion or cyber monitoring often cannot be determined with precision. The way in which internet services function very often will make it impossible for the target state to accuse another state that engages in cyber espionage of violating its territorial sovereignty. As such, the factual situation in such cases is entirely comparable to the one decided by the ECHR when it negated a violation of sovereignty.

Similarly, satellite espionage usually does not violate the target state's territorial sovereignty. Because national airspace is limited in height by an invisible border that denotes the beginning of outer space, which is not subject to territorial sovereignty, it follows that spying activities conducted beyond national airspace cannot violate territorial sovereignty.

Even if such espionage activities do not violate territorial sovereignty, they might still implicate other prohibitive rules of public international law. Since espionage's aim is to uncover another state's internal

124. For example, Microsoft stores e-mails generated in Germany on servers located in Ireland. *See* Christian Kirsch, *Microsoft verteidigt Daten in Europa vor US-Zugriff*, HEISE ONLINE (Sept. 10, 2015), http://www.heise.de/newsticker/meldung/Microsoft-verteidigt-Daten-in-Europa-gegen-US-Zugriff-2809638.html.

125. Patrick Beuth, *NSA kann drei von vier E-Mails mitlesen*, DIE ZEIT (Aug. 21, 2013), http://www.zeit.de/digital/datenschutz/2013-08/nsa-ueberwacht-75-prozent-internet; Charles Arthur, *NSA-Scandal: what data is being monitored and how does it work?* GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions.

126. *See generally* Hyunji Chung et al., *Digital Forensic Investigation of Cloud Storage Services*, 9(2) DIGITAL INVESTIGATION 81 (2012).

127. Glenn Greenwald, *XKeyscore: NSA tools collect 'nearly everything a user does on the internet'*, GUARDIAN (July 13, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; *NSA sucks realtime data from fifty companies*, DAILY MAIL (June 9, 2013), http://www.dailymail.co.uk/news/article-2338367/NSA-sucks-realtime-data-FIFTY-companies.html.

deliberations, its policy objectives, and its strategy and planning, a violation of the prohibition on interventions in the internal affairs is implied.[128]

It is widely agreed that the prohibition on intervening in the internal affairs of other states has become a rule of customary international law. The 1933 Montevideo Convention included the provision that "no state has the right to intervene in the internal or external affairs of another,"[129] and Article 2(7) of the 1945 U.N. Charter rules out U.N. intervention in a member state's internal affairs. By the 1960s, a broad international consensus on the prohibition on intervention in another state's internal affairs had developed. In 1965, the General Assembly passed the *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty* by a 109:0:1 vote.[130] The 1970 General Assembly *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, which passed without a vote, reaffirmed that "no State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State."[131] Although these resolutions were not legally binding, they passed by consensus—with the final one explicitly referring to international law—which makes it reasonable to conclude that states viewed the declarations as reflecting international legal rules. Therefore, the prohibition on intervention in the internal or external affairs of another state is very likely a rule of customary international law. In 2005, the ICJ confirmed that the *Friendly Relations Resolution* was "declaratory of international law."[132] The ICJ itself has also repeatedly stressed the legal quality of the prohibition of such interventions; as soon as 1949, the Court declared interventions in other states' affairs to be unlawful.[133]

---

128. Forcese, *supra* note 2, at 208. Forcese mentions that a state may claim that there has been an "interference in its internal affairs" in cases ofwhat he refers to as "transnational spying." It is, however, not clear whether he believes such a claim would be justified. Wrange, *supra* note 33, at 7–8; Buchan, *supra* note 3, at 73–74.

129. Montevideo Convention on the Rights and Duties of States, art. 8, Dec. 26, 1933, 165 L.N.T.S. 19; *see also* Charter of the Organization of American States, art. 19, Feb. 27, 1967, 119 U.N.T.S. 47; The Warsaw Security Pact, Treaty of Friendship, Cooperation and Mutual Assistance, art. 8, May 14, 1955, 219 U.N.T.S. 23.

130. G.A. Res. 2131 (XX) (Dec. 12, 1965).

131. G.A. Res. 2625 (XXV) (Nov. 25, 1970).

132. *Dem. Rep. Congo v. Uganda*, 2005 I.C.J. 168, ¶ 162.

133. *U.K. v. Alb.*, 1949 I.C.J. 4, at 34–35.

The ICJ's 1986 *Nicaragua* judgment provides the clearest rationale for the prohibition on interventions:

> The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law.[134] . . . A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.[135]

Some claim the reference to "methods of coercion" limits the scope of the prohibition. Because of this, when analyzing cyber or satellite espionage, many doubt that such activities meet the ICJ's requirement of a coercive element.[136] However, this ignores the fact that the ICJ stressed it was only looking at "those aspects of the principle which appear to be relevant" to the case before it.[137] As the court was addressing the United States' support of the Nicaraguan rebels, the Contras, who were attempting to overthrow their country's government by force, there was no need to explore the issue of "coercion" in any detail. The United States' involvement in the rebels' use of force was undoubtedly "coercive" regarding Nicaragua's "choice of a political . . . system."

---

134. *Nicar. v. U.S.*, 1986 I.C.J. 14, ¶ 202; *see also Dem. Rep. Congo v. Uganda*, 2005 I.C.J. 168, ¶ 161–65.

135. *Nicar. v. U.S.*, 1986 I.C.J. 14, ¶ 205.

136. SCHMALENBACH, *supra* note 29, at 29–30; Aust, *supra* note 26, at 16; Peters, *supra* note 34, at 2; SHOSHAN, *supra* note 33, at 43–45; Talmon also justifies his views by referring to the ICJ's reasoning in the *Nicaragua Case*. When dealing with unauthorized overflights over Nicaraguan territory by U.S. planes, the court concluded that such conduct violated Nicaragua's sovereignty, but the court did not examine whether these flights amounted to an unlawful intervention. *See* Talmon, *supra* note 2, at 20–21. However, there was no reason for the ICJ to examine whether the reconnaissance flights constituted an unlawful intervention, having already concluded that the flights had violated Nicaragua's sovereignty (as claimed by Nicaragua) and were therefore unlawful. The court's conclusion obviously obviated the need for further legal analysis. *See Nicar. v. U.S.*, 1986 I.C.J. 14, ¶ 87–91, 251; *see also* Stein & Marauhn, *supra* note 26, at 2225.

137. *Nicar. v. U.S.*, 1986 I.C.J. 14, ¶ 205.

Contrary to what some scholars argue,[138] however, the forceful nature of the United States' intervention in the case before the ICJ does not necessarily imply that lesser coercive means are permissible. Rather, it seems that the difference between coercive intervention and potentially permissible interference comes down to whether the target state retains its freedom to choose in matters related to its sovereignty. On the one hand, an intervention is unlawful when the target state risks losing its freedom to act on an issue related to its internal and/or external affairs. On the other hand, actions below that threshold, aimed at persuasion rather than compulsion, may well be permissible.

Applying these parameters to cyber and satellite espionage allows the conclusion, certainly at a basic level, that such conduct is coercive in relation to the target state. It is every state's prerogative and sovereign right, as part of its overall policy, to decide what information it shares with other states, whether these are allies or foes. A sovereign government has the right to develop its domestic and foreign affairs policies unobserved by foreign powers.[139] Cyber and satellite espionage, however, force the target state to disclose what it, as a sovereign state, had decided not to disclose in pursuit of its overall policies. By intercepting, monitoring or otherwise obtaining data (cyber espionage) or reconnoitering military bases (satellite espionage), the spying state deprives the target state of its right to a sovereign decision on whether to disclose such information.[140]

Depriving the target state of its sovereign right to decide whether to disclose secret information is, however, not the only aspect under which such espionage activities amount to an intervention in the target state's internal affairs. Rather, the spying state's motives when engaging in espionage activities play an important role in determining whether such actions are lawful.[141]

---

138. *Id.*

139. G. Zhukov, *Space Espionage Plans and International Law*, INT'L AFF. (1960), https://www.cia.gov/library/readingroom/docs/CIA-RDP63-00313A000600160051-3.pdf; *cf.* Buchan, *supra* note 3, at 76.

140. Schmalenbach mentions this argument, but it remains unclear whether or not she agrees with it. *See* SCHMALENBACH, *supra* note 29, at 30. For related arguments, *see* SHOSHAN, *supra* note 33, at 45–47; Shull, *supra* note 33, at 6–7; *see also* Buchan, *supra* note 3, at 78; Wrange, *supra* note 33, at 8–9 (basing this conclusion on the fact that the agent, operating remotely from his own country, nevertheless is violating the domestic laws of the target state and is therefore guilty of an illegal intervention).

141. Falk, *supra* note 2, at 58; Pert, *supra* note 50, at 2; Shull, *supra* note 33, at 5; Gehrlein, *supra* note 7, at 101; 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, 70–77 (2016).

Some may disagree and argue that while the reason for collecting information may well be incompatible with public international law, this is irrelevant to any assessment of espionage's lawfulness.[142] It is true that, there are cases when a state's motives are not decisive in determining the lawfulness of a state's conduct.[143] However, there is no general rule to this effect. Rather, there have always been cases when a state's motivation is of vital importance in judging its conduct: the lawfulness of a state's armed response to an armed attack will depend on whether that response was defensive in nature (lawful self-defense) or rather punitive (unlawful reprisal).[144] Similarly, a state that intervenes in another state, relying on the controversial doctrine of humanitarian intervention/the Responsibility to Protect, will have acted unlawfully if it becomes apparent that its motivation was not humanitarian in nature.[145]

When a state engages in espionage in order to undermine the target state's foreign policy, to gain an upper hand in negotiations or to preempt the target state's defensive measures, its motivation is of vital importance when assessing the lawfulness of such conduct.[146] A state collecting another state's secret government communications or reconnoitering its military installations will act upon the information it has received. Subsequently, it will attempt to undermine the target state's foreign policy initiatives when incompatible with its own national interest, it will try to gain an advantage in bilateral or multilateral negotiations and it will condition its military to react to the information gained. Of course, cyber espionage also enables states to target another state's officials by, for example, intercepting their private e-mail communications and subsequently bribing or blackmailing them.[147]

Thus, espionage in these cases evidences the necessary coercive element for it to be an unlawful intervention in another's state internal

142. SCHMALENBACH, *supra* note 29, at 30; SHOSHAN, *supra* note 33, at 45.

143. Aerial Incident of 3 July 1988 (Islamic Republic of Iran v. U.S.), Memorial of the Islamic Republic of Iran, 197–208 (July 24, 1990) (mentioning many incidents when the accused state's motives were viewed as irrelevant when assessing the legality of that state's actions), https://www.icj-cij.org/files/case-related/79/6629.pdf.

144. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 203 (2008); ANTONIO CASSESE, INTERNATIONAL LAW, 299–302 (2d ed. 2005); W. Michael Reisman, *The Raid on Bagdad: Some Reflections on its Lawfulness and Implications*, 5 EUR. J. INT'L L. 120, 125, 129 (1994).

145. *See, e.g.*, U.N. Secretary-General, *Implementing the Responsibility to Protect*, U.N. Doc. A/63/677 (Jan. 12, 2009).

146. Pert, *supra* note 50, at 2; Stein & Marauhn, *supra* note 26, at 24; Baker, *supra* note 5, at 1097; Falk, *supra* note 2, at 58; Kilovaty, *supra* note 140, at 70–77.

147. Gehrlein, *supra* note 7, at 101.

affairs. The spying state is employing the means of espionage to undermine the target state's foreign policy, its bargaining position in negotiations and/or its defense policy.[148] These, however, are matters in which, according to the ICJ, "each State is permitted, by the principle of State sovereignty, to decide freely."[149] Prima facie, this still seems to be the case, as the target state remains free in its decisions. In reality, however, this is no longer so. Based on the information gained by espionage, the spying state will preempt and undermine the target state's policies, thereby reducing or even eliminating the capacity to choose. Therefore, it is indispensable to assess espionage and its motivation together when assessing the former's lawfulness. Espionage is no more and no less than the indispensable, enabling initiation of an unlawful intervention in the target state's affairs.

Furthermore, espionage activities can violate the principle of sovereign equality enshrined in Article 2(1) of the U.N. Charter,[150] as the ICJ recently pointed out in a dispute between East Timor and Australia.[151] Australia's Security Service (ASIO) had raided the offices of East Timor's Australian lawyer and thereby obtained documents and data pertinent to ongoing negotiations, which the two states were conducting regarding oil and gas reserves in the Timor Sea.[152] In a preliminary ruling on the matter, the ICJ came to the following conclusion:

> The principal claim of Timor-Leste is that a violation has occurred of its right to communicate with its counsel and lawyers in a confidential manner with regard to issues forming the subject-matter of pending arbitral proceedings and future negotiations between the Parties. The Court notes that this

148. For example, a leaked memorandum revealed that the United States spied on UN diplomats representing states sitting on the Security Council during the Iraq crisis, *see* Martin Bright et al., *Revealed: US dirty tricks to win vote on Iraq war*, GUARDIAN (Mar. 2, 2003), http://www.theguardian.com/world/2003/mar/02/usa.iraq. Referring to U.S. spying on UN diplomats representing states sitting on the Security Council at that time, the article explains: "The memo is directed at senior NSA officials and advises them that the agency is 'mounting a surge' aimed at gleaning information not only on how delegations on the Security Council will vote on any second resolution on Iraq, but also 'policies', 'negotiating positions', 'alliances' and 'dependencies' - the 'whole gamut of information that could give U.S. policymakers an edge in obtaining results favourable to U.S. goals or to head off surprises.'"

149. *Nicar. v. U.S.*, 1986 I.C.J. 14, ¶ 205.

150. Wright, *supra* note 20, at 23; SCHMALENBACH, *supra* note 29, at 30–31; Peters, *supra* note 34, at 2.

151. Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Order, 2014 I.C.J. 147 (Mar. 3).

152. *Id.* ¶ 27.

> claimed right might be derived from the principle of the sovereign equality of States, which is one of the fundamental principles of the international legal order and is reflected in Article 2, paragraph 1, of the Charter of the United Nations. More specifically, equality of the parties must be preserved when they are involved, pursuant to Article 2, paragraph 3, of the Charter, in the process of settling an international dispute by peaceful means. If a State is engaged in the peaceful settlement of a dispute with another State through arbitration or negotiations, it would expect to undertake these arbitration proceedings or negotiations without interference by the other party in the preparation and conduct of its case. It would follow that in such a situation, a State has a plausible right to the protection of its communications with counsel relating to an arbitration or to negotiations, in particular, to the protection of the correspondence between them, as well as to the protection of confidentiality of any documents and data prepared by counsel to advise that State in such a context.[153]

Although the direct applicability of the ICJ's preliminary ruling is limited in scope, as it only applies to information related to ongoing negotiations between the spying and the target state obtained by any means of espionage,[154] its potential relevance is much greater.[155] Using another state's confidential information in order to undermine its foreign, defense or trade policies is surely similarly detrimental to the principle of sovereign equality as the seizure of documents in order to undermine the other state's bargaining power during ongoing negotiations. Besides, there will not be many states actually spying on each other that are not involved in some kind of bilateral or multilateral negotiations. In summary, the collection of another state's confidential information, also by means of cyber or satellite espionage, in order to potentially frustrate that state's policies, is a violation of the principle of sovereign equality.

---

153. *Id.*

154. Such conduct during ongoing treaty negotiations might also raise good faith issues that, *in extremis*, could threaten a concluded treaty's validity. The ICJ has repeatedly stressed the importance, in public international law, of the principle of good faith when states are negotiating treaties. In fact, the ICJ has referred to it as "[o]ne of the basic principles governing the creation and performance of legal obligations." Nuclear Tests (Austl. v. Fr.), Judgment 1974 I.C.J. 253, ¶ 46 (Dec. 20); *see also Ger. V. Den. & Neth.*, 1969 I.C.J. 3, ¶ 85; Anton, *supra* note 69, at 3.

155. *See also* Ronald J. Bettauer, *Questions Relating to the Seizure and Detention of Certain Documents and Data*, 108 AM. J. INT'L L. 763, 767–69 (2014).

"Modern" espionage, employing the means of cyber or satellite spying, is therefore usually unlawful. If cyber espionage involves obtaining data from servers located within the target state, the violation of the target state's territorial sovereignty is no less than in the more traditional forms of espionage. However, satellite and most cyber espionage activities do not involve an infringement of the target state's territorial sovereignty. Nevertheless, such activities generally are unlawful as well. In most cases, they are an indispensable part of an effort to undermine and thwart the target state's policies. As such, they amount to an unlawful intervention in the target state's internal affairs and a violation of the principle of sovereign equality.

C. *Clean-Hands-Principle*

Many will counter that, given espionage's ubiquitous nature, it would not be plausible for a state to invoke its unlawfulness. As all states engage in the kind of espionage activities analyzed here as a means of statecraft, no state can rightfully deplore their illegality.[156] This argument relies mainly on the so-called "clean-hands-principle."[157]

The status of the clean-hands-principle in international law is highly contentious.[158] Whether it has evolved into a rule of customary international law is very doubtful.[159] Even if this were assumed, there is even less support for the notion that the principle could "[preclude] the wrongfulness of the conduct which caused injury" to the target state.[160] Rather, the more common argument is that the principle may cause a state's claim against another state to be inadmissible.[161] Even then, it is generally agreed that the clean-hands-principle can only be invoked by the offending state if the reciprocal conduct is of a comparable "nature

156. SCHMALENBACH, *supra* note 29, at 30–34; Romero, *supra* note 8, at 19.

157. Judge Hudson of the PCIJ provided a definition in his *Individual Opinion* in the *River Meuse* Case: "It would seem . . . that where two parties have assumed an identical or a reciprocal obligation, one party which is engaged in a continuing non-performance of that obligation should not be permitted to take advantage of a similar non-performance of that obligation by the other party"; Diversion of Water from the River Meuse (Neth. v. Belg.), Judgement, 1937 P.C.I.J. (ser. A/B) No. 70, at 77 (June 28) (separate opinion by Hudson, J.); *see also* Diversion of Water from the River Meuse (Neth. v. Belg.), Judgement, 1937 P.C.I.J. (ser. A/B) No. 70, at 24–25 (June 28).

158. Int'l Law Comm'n, Second Rep. on State Responsibility, ¶¶ 332–36, U.N. Doc. A/CN.4/498 (1999); JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 701 (8th ed. 2012).

159. Int'l Law Comm'n, *supra* note 158, ¶ 336.

160. *Id.* ¶ 335.

161. *Id.* ¶¶ 333–35.

and gravity."[162] These further limitations would make it very difficult for a spying state to invoke the principle successfully against a claim of unlawfulness by a target state.

However, it is unlikely the principle is reflective of customary international law at all. Crawford summarizes his findings for the International Law Commission by relying on a quote from Rousseau, according to whom "[I]t is not possible to consider the 'clean hands' theory as an institution of general customary law."[163] Thus, given the principle's uncertain status in public international law, the clean-hands-principle does not affect the conclusion that espionage activities are unlawful in public international law.

V. Conclusion

This article began by posing the question of whether the relationship between peacetime espionage and public international law is as complicated as is often implied in discussions on the topic, which often conclude with references to an apparent "paradox." In the preceding paragraphs, I set out why I believe this not to be the case.

The confusion surrounding the lawfulness of peacetime espionage is a result of the futile investigation into what international law has to say about "espionage" which invariably leads to the finding of "little" or "very little." Whilst this is correct, it is the wrong question. Rather, the issue at stake is whether an alleged individual espionage activity is reconcilable with public international law or not. Once the legal analysis focuses on individual state activities commonly associated with espionage, public international law very often does provide a clear answer.

Obtaining documents or data by theft and/or bribery/blackmail of target state officials violates the target state's territorial sovereignty. Exploiting a permitted presence within the target state to spy often even violates treaty law. Admittedly, this is not the case in relation to more modern means of espionage: most forms of cyber espionage and satellite espionage do not infringe on the target state's territorial sovereignty. Nevertheless, public international law provides an answer even to these more modern phenomena: a state engages in espionage in order to gain an advantage. The state seeks to gain the upper hand in negotiations or to undermine or thwart policy initiatives by other states incompatible with its own goals. Espionage forces states to reveal secret information to the spying state, which subsequently helps the latter to frustrate the target state's foreign, trade, and defense policies. Thus, in

162. Wright, *supra* note 20, at 21; Schmalenbach, *supra* note 29, at 30–34.

163. Int'l Law Comm'n, *supra* note 158, ¶ 336.

effect, the target state loses its ability to "decide freely" in matters the ICJ has seen as vital to state sovereignty.[164] In conclusion, espionage activities are an unlawful intervention in the target state's affairs and, as the ICJ has recently indicated, may well violate the principle of sovereign equality.[165]

Far from being "the riddle in the sands," public international law in most cases does provide an unequivocal answer to the question of whether espionage activities are lawful or not. This also helps explain the lack of rules dealing specifically with peacetime espionage: besides it being an ill-defined and therefore contentious concept, current law is sufficiently clear to regulate peacetime espionage in most cases.

164. *Nicar. v. U.S.*, 1986 I.C.J. 14, ¶ 205

165. *Timor-Leste v. Australia*, 2014 I.C.J. 147, ¶ 27.