2020

The Liberty to Spy

Asaf Lubin
Maurer School of Law - Indiana University, lubina@iu.edu

VOLUME 61, NUMBER 1, WINTER 2020

The Liberty to Spy

Asaf Lubin*

Many, if not most, international legal scholars share the ominous contention that espionage, as a legal field, is devoid of meaning. For them, any attempt to extrapolate the lex lata corpus of the International Law of Intelligence (ILI), let alone its lex scripta, would inevitably prove to be a failed attempt, as there is simply nothing to extrapolate. The notion that international law is moot as to the question of if, when, and how intelligence is to be collected, analyzed, and promulgated, has been repeated so many times that it has become the prevailing orthodoxy.

This paper offers a new and innovative legal framework for articulating the law and practice of interstate peacetime espionage operations, relying on a body of moral philosophy and intelligence ethics thus far ignored by legal thinkers. This framework diagnoses the legality of covert intelligence at three distinct temporal stages: before, during, and after. In doing so it follows the traditional paradigms of international law and the use of force, which themselves are grounded in the history of Just War Theory. Adopting the Jus Ad, Jus In, Jus Post model is appropriate, given the symbiosis between espionage and fundamental U.N. Charter principles.

This paper focuses on the first of these three paradigms, the Jus Ad Explorationem ("JAE"), a sovereign's prerogative to engage in peacetime espionage and the right's core limitations. Examining a plethora of international legal sources, the paper exemplifies the myriad ways by which peacetime intelligence gathering has been already recognized as a necessary pre-requisite for the functioning of our global legal order. The paper then discusses the nature of the JAE. It argues that the right to spy is best understood as a privilege in Hohfeldian terms. It shows how understanding interstate intelligence operations as a weaker "liberty right" that imposes no obligations on third parties to tolerate such behavior helps capture the essence of the customary norms that form part of the practice.

Recognizing the liberty right to spy opens the door for the doctrine of "abuse of rights" to play a role in constraining the practice. By identifying the only two legitimate justifications for peacetime espionage—advancing the national security interests of States and promoting an increase in international stability and cooperation—we are able to delimit what may constitute abusive spying, defined as exploiting one's right to spy not for the purposes for which the right was intended. The paper concludes by introducing four categories of unlawful espionage: (1) spying as a means to advance personal interests; (2) spying as a means to commit internationally wrongful acts; (3) spying as a means to advance corporate interests; and (4) spying as a means to exploit post-colonial relations.

INTRODUCTION

Thomas Middleton's satirical play, *A Game at Chess*,[1] was first performed in August 1624 in the Shakespearean Globe Theater and had "an unprece-

* Affiliate, Berkman Klein Center for Internet and Society Harvard University, Visiting Fellow at the Information Society Project of Yale Law School, and a Visiting Scholar at the Hebrew University of Jerusalem Federmann Cyber Security Center. I wish to thank Michael Reisman, Matthew Waxman, Fabien Lafouasse, Curtis Bradley, Laurence Helfer, and Quinn White for comments on previous drafts of this piece. I also wish to thank those who attended previous workshops of this paper at events at Harvard Law School, Yale Law School, the Naval War College, and the American Society of International Law. Finally, I wish to thank the editorial board and staff of the Harvard International Law Journal for excellent comments and edits throughout the editorial process. This work was partially supported by the William and Flora Hewlett Foundation under grant 2018-7277.

1. THOMAS MIDDLETON, A GAME AT CHESS 10, n.1 (J.W. Harper ed. 1966).

dented run, the longest on the Jacobean stage."[2] Filtered through the allegory of a chess match, it offered a political commentary to the prevailing tensions between the royal houses of Spain and Great Britain. It was a period of civic life considered by some to be the "golden age of espionage, when Europe appeared to be fairly crawling with spies."[3] The European Wars of Religion were what triggered this lavish expansion in spycraft.[4] The Protestant Reformation movement and the Counter-Reformation Catholic crusade turned Europe into a "maelstrom of entities warring over religion" which brought with it a "constant danger that put a premium on intelligence."[5] The Westphalian legal order that emerged at the end of the Thirty Years' War—and which was established on the principles of sovereign equality and non-intervention—was thus an order extremely cognizant of and susceptible to the moral debauchery of interstate intelligence gathering. The intricate webs of spies that was weaved over Europe at that time period simultaneously helped shape Westphalia and were shaped by it.

The intelligence profession, the shadowy work of spooks and saboteurs operating in disguise, played a critical role in maintaining the 17th century's balance of power and has continued to do so over the centuries.[6] From the days of Sir Francis Walsingham, the father of modern intelligence agencies and the first spymaster to manage an omnipresent mass surveillance program across the European continent, all the way to the Trump-Russia dossier produced by former MI6 agent Christopher Steele, intelligence seems to guide world politics. Espionage plays such a cardinal role in both our domestic affairs and foreign policies that one would have presumed there to be well-established rules of international law undergirded by a vibrant academic exchange and jurisprudential debate surrounding the ways by which intelligence is to be ordered, collected, analyzed, and disseminated. Instead, as noted by Chesterman, intelligence exits in a "legal penumbra, lying at

2. Thomas Cogswell, *Thomas Middleton and the Court 1624: A Game at Chess in Context*, 47 HUNTINGTON LIBR. Q. 273, 273 (1984).

3. ERNEST VOLKMAN, THE HISTORY OF ESPIONAGE: THE CLANDESTINE WORLD OF SURVEILLANCE, SPYING AND INTELLIGENCE FROM ANCIENT TIMES TO THE POST-9/11 WORLD 58 (2007).

4. *Id.* Chesterman cites Garrett Mattingly to suggest that espionage is grounded in modern diplomacy as it evolved from the Renaissance through the post-Westphalian legal order. He explains that "a chief function of the resident ambassador soon became to ensure that 'a continuous stream of foreign political news flow[ed] to his home government'." *See* Simon Chesterman, *The Spy Who Came in From the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1087 (2006) (citing GARRETT MATTINGLY, RENAISSANCE DIPLOMACY 67 (1955)).

5. *See* VOLKMAN, *supra* note 3, at 58.

6. Hungarian adventurer and former spy Ignatius Trebitsch-Lincoln describes the role intelligence played in maintaining the European balance of power: "[w]hen Kaiser William II meets the Tzar of all the Russias, it is France, England, and Turkey who must penetrate the veil of the secret conclaves. When Edward VII meets Clemenceau, the French Prime Minister at Marienbard, the secret intelligence departments of Germany and Austria must watch for shadows on the political map of Europe. When England and France sign an *entente cordiale*, the starting point for new negotiations between these powers and Russia, the men from Wilhelmstrasse have already forecasted this eventuality. Such things hidden from the eyes of the plodding citizen in his complacent world are the momentous problems of the diplomatic spy." IGNATIUS TIMOTHY TREBITSCH-LINCOLN, REVELATIONS OF AN INTERNATIONAL SPY 40 (1916).

the margins of diverse legal regimes and at the edge of international legitimacy."[7]

This should come as no surprise to those who have mastered the arts of "the second oldest profession."[8] The literature surrounding the international law of espionage has been historically stagnant, coalescing around three contradictory accounts, with three different conclusions as to the legality of spying: "legal," "illegal," or "neither legal nor illegal."[9] Take, for example, *Essays on Espionage and International Law*, a compilation of reaction papers produced for the 1961 regional meeting of the American Society of International Law ("ASIL"). The articles cover the commentaries of a number of prominent legal scholars to both the U2 spy plane incident of 1960 and the American program of early warning reconnaissance satellites (the Missile Defense Alarm System, "MIDAS"). Whereas Julius Stone took a permissivist point of view (suggesting that we live in a "system of reciprocally tolerated espionage"), Quincy Wright adopted a prohibitionist theory (considering espionage as a form of "illegal intervention"), and Richard Falk seemed closest to the extralegalist camp (concluding that "it is probably not useful to debate the legality" of espionage in traditional international law).[10]

It is only quite recently that we have witnessed a gradual shift from these old-school absolutist theories to new-school thinkers who have centered their research on a relativist model of espionage law, suggesting rather that

7. Chesterman, *supra* note 4, at 1130; *see also* David Silver, *Intelligence and Counterintelligence*, *in* National Security Law 935, 965 (John Norton Moore & Robert Turner eds., 2d ed. 2005) ("There is something almost oxymoronic about addressing the legality of espionage under international law.").

8. Michael J. Barrett, *Honorable Espionage*, J. Def. & Dipl., Feb. 1984, at 13, 14 ("Espionage is the world's second oldest profession and just as honorable as the first.").

9. For literature that splits the law on espionage into these three camps, or a similar version of them, *see* John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 Mich. J. Int'l L. 595, 602 (2007); Peyton Cooke, *Bringing the Spies from the Cold: Legal Cosmopolitanism and Intelligence Under the Laws of War*, 44 U.S.F. L. Rev. 601, 609-10 (2010); Ashley Deeks, *An International Legal Framework for Surveillance*, 55 Va. J. Int'l L. 291, 300–13 (2015); Captain M. E. Bowman, *Intelligence and International Law*, 8 Int'l J. Intelligence & Counterintelligence 321, 328 (1995); *cf.* Craig Forcese, *Pragmatism and Principle: Intelligence Agencies and International Law*, 102 Va. L. Rev. 67, 68 (2016) (after citing Radsan's partitioning of "academic commentaries on the topic into three categories," Forcese notes that a fourth category exists, one which "subdivides the world of intelligence collection into constituent state acts . . . examin[ing] law governing specific conduct." Forcese places himself and Inñaki Navarrete in this camp).

10. Quincy Wright et al., Essays on Espionage and International Law (Roland J. Stranger ed., 1962). Stone did distinguish between spying that serves a "destructive . . . green-light function" which should be limited, and a "salutary red-light function" which should be embraced. Nonetheless, he left open the question of how to regulate against the green-light function. *See* Julius Stone, *Legal Problems of Espionage in Conditions of Modern Conflict*, *supra,* at 29, 42-43 (Roland J. Stranger ed., 1962). Quincy Wright saw espionage as a form of "illegal intervention" to be condemned and argued further that where it occurs it should be dealt with through means of collective action. Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *supra,* at 3, 23-26 (Roland J. Stranger ed., 1962). Falk argued that espionage possesses "the peculiar quality of being tolerated but illegal." Falk simultaneously argued, however, that from a policy perspective the destabilizing nature of espionage challenges the rationality of any of the justifications raised in favor of it. Richard A. Falk, *Space Espionage and World Order: A Consideration of the Samos-Midas Program*, *supra,* at 45, 57, 68, 74-75 (Roland J. Stranger ed., 1962).

the practice is sometimes legal and sometimes illegal.[11] These emerging voices take the strong view that while peacetime espionage "does not *per se* violate international law, the method by which it is carried out might do so."[12] In their literature, these scholars have thus attempted to draw legal distinctions between different types of intelligence gathering activities and techniques, focusing mainly on questions of territoriality. For example, as the International Group of Experts ("IGE") who drafted Tallinn Manual 2.0 recently put forward, an agent of State A who covertly enters State B and while physically present on its territory uses a USB flash drive to introduce certain spyware into that country's infrastructure, will be in violation of the U.N. Charter principle of territorial sovereignty and therefore violates international law.[13] That would not be true, argues the IGE, if the espionage was instead carried out through remote sensing from a satellite in outer space, or through the interception of those communications that, due to the nature of the Internet, just happen to cross into the surveilling state's territory.

The legal discourse has thus far overwhelmingly ignored a body of moral philosophy and intelligence ethics literature that has long suggested that rules on spying may be identified by considering a different set of lenses altogether. In explaining the practice of intelligence and the moral foundations that reinforce it, these philosophers have adopted an approach that maneuvers through espionage's great "wilderness of mirrors"[14] by following a normative diagnosis of intelligence operations at three distinct temporal stages: before, during, and after. In so doing, these writers adopt the traditional paradigms of international law and the use of force, which are themselves grounded in the history of Just War Theory ("JWT"). Using the *Jus Ad*, *Jus In*, *Jus Post* models for intelligence regulation is appropriate given the symbiosis between espionage, fundamental Charter principles, and control over international violence. As Darrell Cole notes, the just war criteria offer intelligence agencies readily available principles to be internalized as "checks in extreme circumstances," and thus "ought to be foundational for the moral formation for any spy."[15]

This article attempts to lay the foundation for the translation of these moral accounts into a revolutionary *lex specialis* subfield of international law,

11. *See, e.g.*, Jared Beim, *Enforcing a Prohibition on International Espionage*, 18 CHI. J. INT'L L. 647, 656 (2018) (suggesting that "all espionage is not created equal" and that certain forms of espionage are "not worth punishing" compared to others).

12. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 168 (Michael Schmitt ed., 2d ed. 2017) [hereinafter TM 2.0] (the International Group of Experts ("IGE") placed "peacetime cyber espionage" under Section 5, which covers those cyber operations that the IGE deemed to be "not per se regulated by international law"). For a critique of TM 2.0, particularly the "loose relationship between the Tallinn Rules and post-Tallinn state practice," see Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583 (2018).

13. TM 2.0, *supra* note 12, at 19.

14. *See* DAVID C. MARTIN, WILDERNESS OF MIRRORS 10 (1980).

15. DARRELL COLE, JUST WAR AND THE ETHICS OF ESPIONAGE 151 (2014).

what I call the International Law of Intelligence ("ILI"). While opposing both old-school and new-school scholarship, this articulation of the ILI maintains a clear-eyed view of the important functions that intelligence plays in our legal world order, framing these functions within a larger global constitutive process. This paper seeks to learn from mistakes made in previous academic endeavors, which either erred by over-emphasizing the myth system or over-simplifying the operational code of spycraft.[16] Ultimately, the paper reaches the conclusion that states enjoy a peacetime right to spy under international law, that the existence of the right is essential for the functioning of our public world order, and that only by acknowledging the right may we be able to articulate when the right is abused.

As such, this article focuses only on the first of the three paradigms that comprise the ILI: the *Jus Ad Explorationem* ("*JAE*"), a sovereign's prerogative to collect intelligence in peacetime and the right's core limitations. After mapping the existing discourse and its discontents in Section II, the paper moves to assert the controversial claim that there exists in international law a "right to spy." To prove this point, Part II analyzes a plethora of international legal sources including states' rights to survival, self-defense, and self-determination; collective security obligations under U.N. and treaty law; international human rights law; and international humanitarian law. Ultimately, this Part reaffirms what Professors McDougal, Lasswell, and Reisman had argued some forty-five years ago, that "[t]he key to the contemporary global security system is a reliable and unremitting flow of intelligence to the pinnacle elites."[17] In the absence of centralized suprana-

16. As Professor W. Michael Reisman noted "in law things are not always what they seem," and one needs to be particularly mindful of the existence of "two 'relevant' normative systems: one which is supposed to apply and which continues to enjoy lip service among elites [which he calls the myth system] and one which is actually applied [which he calls the operational code]." Reisman describes the tension between the myth and the code as a "dynamic process" and a "symbiotic relationship." *See* W. Michael Reisman, *On the Causes of Uncertainty and Volatility in International Law*, *in* The Shifting Allocation of Authority in International Law: Considering Sovereignty, Supremacy and Subsidiarity 33, 44-45 (Tomer Broude & Yuval Shany eds., 2008) ("[T]he myth system is *not* widely appreciated as consciously false. It does not express values that are obsolete. On the contrary: it affirms values that continue to be important socially and personally. Although not applied in the 'jurisdiction' of the operational code, the myth system may yet influence decision-making. Precisely because discrepancies between myth system and operational code can erode the credibility of the myth system, maintenance of belief in the myth system is a dynamic process requiring ongoing contributions from many. By contrast, those who practise the operational code try to obscure it from the general public. But there is an almost symbiotic relationship between myth system and operational code, with the latter providing a degree of suppleness and practicality that the myth system could not achieve without changing much of its content and procedure of application.").

17. Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, *The Intelligence Function and World Public Order*, 46 Temp. L.Q. 365, 434 (1973). The article, which was republished in International Law Essays in 1981, is one of the oldest and most comprehensive studies of the subject of intelligence collection and processing under the post-UN world order. The authors provide an original New Haven School account of the international law that governs intelligence activities. They predominantly focus on what they envision as the way forward for the evolution of the practice, or in their words: "If the policies affecting the constitutive structure and functions of the world community are to move toward the realization of at least minimum public order, the intelligence component of the decision process must harmonize as far as possible with criteria designed to provide the pertinent flow of communicated messages to

tional enforcement mechanisms, of hierarchal global structures or well-defined international prescriptive processes, states depend on such intelligence collection and analysis to monitor and divert potential threats and imperilments as well as to maximize their own relative power.[18] Lacking a world "Interspy" ("a service that draws upon the sources available to all organizations willing and able to work together to expose threats to world public order"),[19] international institutions rely almost entirely on intelligence produced by their member states to fulfill their mandate.[20] In other words, the gathering of intelligence is a necessary pre-requisite for the functioning of our broader legal order. This reality suggests that states enjoy a derivative right, and indeed under certain circumstances even an obligation, to continuously engage in peacetime espionage to achieve certain communal goals.

Part III shifts the discussion to the nature of the *JAE*. I contend that the right to spy is best understood not as a hard claim-right, but rather as a weaker privilege, borrowing from Hohfeld's Theory of Rights and Duties. I explain how conceptualizing interstate intelligence gathering as a liberty that imposes no obligations on third parties to tolerate such behavior when done unto them helps capture the essence of the customary norms that form part of the practice.[21]

---

all who participate in authoritative control." *Id.* at 370-71. By focusing on the important functions that intelligence play, they seem to adopt a pragmatic view, thereby rejecting interpretations of the prevailing legal regimes in vacuum.

18. Former director-general of MI5, Sir Stephen Lander, argued that "intelligence services and intelligence collection are at heart manifestations of individual state power and of national self-interest." Sir Stephen Lander, *International Intelligence Cooperation: An Inside Perspective*, 17 CAMBRIDGE REV. INT'L AFF. 481, 481 (2004). *See also* Jennifer E. Sims, *Foreign Intelligence Liaison: Devils, Deals, and Details*, 19 INT'L J. INTELLIGENCE & COUNTERINTELLIGENCE 195, 196 (2006); Don Munton, *Intelligence Cooperation Meets International Studies Theory: Explaining Canadian Operations in Castro's Cuba*, 24 INTELLIGENCE & NAT'L SEC. 119, 126-28 (2009).

19. McDougal, Lasswell & Reisman, *supra* note 17, at 447; *see also* James L. Tyron, *International Organization and Police*, 25 YALE L.J. 34, 34 (1916) (making the case for an "international army and navy" suggesting that such an idea "is one of the oldest and most persistent ideas associated with the movement for world peace").

20. *See, e.g.*, Bassey Ekpe, *The Intelligence Assets of the United Nations: Sources, Methods, and Implications*, 20 INT'L J. INTELLIGENCE & COUNTERINTELLIGENCE 377, 378-79 (2007) ("The assumption is that members of both the Security Council and the General Assembly, in their daily proceedings, come equipped with a wealth of knowledge on specific or emerging issues, provided to them by their national intelligence services or other forms of specialized information and analysis departments."); Guido Venturoni, *The Washington Summit Initiatives: Giving NATO the "Tools" to do its Job in the Next Century*, 47 NATO Rev. 8, 11 (1999) ("In the area of intelligence gathering, NATO—which has few intelligence assets of its own and is already dependent on its member nations for intelligence contributions—must solicit its members for considerably more input than previously."); OFFICE OF TECH. ASSESSMENT ("OTA"), *Nuclear Safeguards and the International Atomic Energy Agency*, UNITED STATES CONGRESS, 5 (1995), https://perma.cc/GH3R-K4F3 [hereinafter OTA Report] (discussing the IAEA's limited investigative ability to discover undeclared activities that states wish to keep hidden and its dependency on its members' intelligence capacities).

21. In doing so, this Section further challenges our existing perceptions of the *Lotus* doctrine. S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 19 (Sept. 7). The Lotus Principle, commonly cited as a foundational principle of international law, assumes that lawfulness on the international plain is derived from the absence of a prohibition. It runs in opposition to democratic and adminis-

Part IV ends by drawing the limits of the *JAE*. Acknowledging the existence of a liberty right to spy is important, as it allows us to begin sketching the justifications for spying and thereby articulating the limits of the practice—those cases in which the right may be abused by a country spying for illegitimate purposes. Relying on the abuse of rights doctrine as a general principle of international law, this Section identifies four such categories of abusive spying: (1) spying as a means to advance personal interests; (2) spying as a means to commit an internationally wrongful act; (3) spying as a means to advance corporate interests; and (4) spying as a means to exploit post-colonial relations.

I. The Faultlines of the Existing Discourse

A. Defining Espionage

As a preliminary matter, my choice of terminology should be clarified. I use the nouns "espionage," "intelligence," "surveillance," and "reconnaissance" (and their associated verbs, "to spy," "to surveil," "to monitor") interchangeably throughout this paper. While it is true that some of these words may have been traditionally used to refer to specific methods of intelligence collection,[22] they are all elements of spycraft and should thus be understood as forming part of a collective whole.

It is further worth noting that under customary international law there is no "internationally recognized and workable definition of 'intelligence collection.'"[23] There seems to be almost as many definitions of intelligence as there are experts asked to define it.[24] For the purposes of this paper I settle on the following self-crafted definition:[25]

---

trative rule of law systems that require, through a principle of legality, that state agencies possess statutory authorization prior to taking an action.

22. For example, Merriam Webster Dictionary defines "espionage" as "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company." The focus on "spies" might be perceived as associated with HUMINT collection activities. On the other hand, the term "reconnaissance" is defined as "a preliminary survey to gain information, especially an exploratory military survey of enemy territory." The focus on "military surveys" might denote different forms of VISINT exercises and SIGINT collection (in particular different types of electronic intelligence gathering, or ELINT). For the definitions of HUMINT, SIGINT, and VISINT, see *infra* note 29; see also Mark M. Lowenthal, Intelligence: From Secrets to Policy 88 (6th ed. 2015) (distinguishing between "surveillance," which he defines as the "systematic observation of a targeted area or group, usually for an extended period of time; "reconnaissance," defined as "a mission to acquire information about a target, sometimes meaning a one-time endeavor;" and "intelligence," defined as "a general term for collection").

23. *See* Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 Mich. J. Int'l L. 625, 637 (2006).

24. *See* Michael Warner, *Wanted: A Definition of "Intelligence"*, 46 Stud. Intelligence 15, 15 (2002) (suggesting that the term intelligence is "defined anew by each author who addresses it" and that so far "no one has succeeded in crafting a theory of intelligence").

25. The definition mirrors in some respects, and departs in others, from the definition put forward in Geoffrey Demarest, *Espionage in International Law*, 24 Denver J. Int'l L. & Pol'y 321, 325-26 (1996) ("[E]spionage can be defined as the consciously deceitful collection of information ordered by a govern-

Intelligence operations ("IOs") are those operations that encompass all five of the following components

> *(1) The operation occurs in peacetime*
>
> *(2) The operation involves the passive gathering, analysis, verification, and dissemination of information of relevance to a State or States' "decision-making process" and in service of some State interests.*
>
> *(3) The operation is launched by agents of a State or States, or those with a sufficient nexus to the State or States in question (the Surveilling State(s)).*
>
> *(4) The operation targets a foreign State or States, their subjects, associations, corporations, or agents, without that State or States' knowledge or consent (the Target State(s)).*
>
> *(5) The operation involves some degree of secrecy and confidentiality, as to both the needs behind the operation and the specific methods of collection and analysis employed, so to ensure its effectiveness. These cape et d'épée (cloak and dagger) operations, would often be coupled with some degree of deceitful intent on the part of the Surveilling State(s), though such is not always mandated.*[26]

A few observations emerge from examining this definition. Most importantly, the definition excludes many areas of government work that some might conceive of as falling under the broad umbrella of "espionage" as it is understood in popular media. Namely, I do not seek, or intend to address, the legality of covert action, influence operations, offensive cyber intrusions, election interferences, information warfare or assassinations, if to name but a few examples.[27] The right to spy as proposed in the following pages is an extremely narrow right and should thus not be confused with some monstrous *Jus Extra Bellum* –a kind of state right to engage in all national security activities that are below the threshold of armed conflict.[28]

---

ment or organization hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the collecting."), and another put forward in Raphael Bitton, *The Legitimacy of Spying Among Nations*, 29 Am. U. Int'l L. Rev. 1009, 1011 (2014) ("[E]spionage between states is . . . an undercover state-sponsored intrusion into the restricted space of another state or organization for the sake of collecting information.").

26. Each of the underlined terms in this definition requires unpacking that is impossible to do within the limits of this article. At the heart of my attempts to capture a definitional structure for intelligence operations, stands a desire to offer a narrow definition. This is because, as some commentators have noted: "most definitions of espionage and intelligence are so broad as to allow us to define even a local town library as intelligence." Jeffrey Burds, The Second Oldest Profession: A World History of Espionage - Part One 8 (2011).

27. For legal analysis of covert action and related activities, see W. Michael Reisman & James E. Baker, Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion in International and American Law (1992); Loch K. Johnson, *On Drawing a Bright Line for Covert Operations*, 86 Am. J. Int'l. L. 284, 305 (1992); Kenneth B. Nunn, *The Legality of Covert Action under Contemporary International Law*, 1 La Raza L. J. 139, 166-167 (1984).

28. For further reading, see Michael Jefferson Adams, *Jus Extra Bellum: Reconstructing the Ordinary, Realistic Conditions of Peace*, 5 Harv. Nat'l. Sec. J. 377 (2014).

Moreover, this definition seeks to encompass all primary fields of intelligence gathering (or INTs as they are known in traditional spy parlance), including, human intelligence ("HUMINT"), signals intelligence ("SIGINT"), and Visual Intelligence ("VISINT").[29] In fact even certain forms of Open Source Intelligence (or "OSINT") might be included, to the extent that the collection involves secrecy surrounding both the goals of the operation and the specific methods of collection. In this regard a diplomat sitting in his embassy reading a local newspaper or engaging in the course of regular diplomatic affairs should not be considered as engaging in an intelligence operation, even if they are doing so in support of some confidential objective. However, if that same diplomat relies on complex data mining algorithms to secretly scrape the governmental websites of the host state, this OSINT operation would fall under the definition, for both the algorithms employed and the nature and goals of the operation itself would have to be kept opaque.[30]

Finally, this definition focuses only on interstate and peacetime activities. I exclude both domestic forms of surveillance (subject to ever-increasing constitutional and administrative frameworks as well as international human

29. *Human Intelligence Collection ("HUMINT")* refers to the process of gathering information from human sources. HUMINT sources could be anyone. It may be "a foreign official who, by virtue of a position of trust in his government has access to important information and who is willing, for some reason, to pass it to officers of one's intelligence service." Abram N. Shulsky & Gary J. Schmitt, Silent Warfare: Understanding the World of Intelligence 11 (2002). At the same time, it may simply be a citizen of the surveilling state who has traveled abroad for study or who works in a certain industry that puts her in direct contact with foreign persons of interests. Specialized Handlers develop a profound mastery in human psychology, for "understanding people, with all of their complexities, is crucial to the business of running assets to collect HUMINT." *INTelligence: Human Intelligence*, Central Intelligence Agency (Oct. 21, 2010), https://perma.cc/CU85-FJH7. Collection methods may include in-person meetings and debriefs, secret exchanges, and remote communications using sophisticated technological means. For further reading see Lowenthal, *supra* note *22*, at 127-37. *Signal Intelligence Collection ("SIGINT")* refers to the process of deriving intelligence from intercepted electromagnetic waves. It may be sub-divided further based on the systems emanating the waves intercepted: Communication Intelligence ("COMINT") covers that information that is derived from the interception of communications signals (*e.g.* radio messages, telephonic communications, internet communications, satellite communications); Electronic Communications ("ELINT") covers that information derived from non-communication electromagnetic radiations, such as from radars and other weapon systems (for example, a sub category of ELINT is Foreign Instrumentation Signals Intelligence ("FISINT"), which concern electromagnetic emissions associated with the testing and operational deployment of foreign aerospace, surface, and subsurface systems). Focusing particularly on COMINT, the means of collection vary, and may include tapping an underwater fiber optic cable, hacking into a Domain Name System ("DNS") Server, strategically placing antennas to collect free-roaming radio signals, or hiding a recorder in the office of a particular high-profile target. For further reading, see *id.* at 118-27. Finally, *Visual Intelligence ("VISINT")* also referred to as Geo-Spatial Intelligence ("GEOINT"), Photographic Intelligence ("PHOTOINT"), and Imagery Intelligence ("IMINT") concerns the process of acquiring visual access to places or objects that are otherwise inaccessible to intelligence agents. Today's measures may include sending a surveillance drone into the territory of a neighboring country, directing a reconnaissance satellite to take images of the border region between two conflicting nations, and clandestinely placing a camera in the office of a foreign military commander. For further reading, see *id.* at 107-118.

30. For more on whether OSINT gathering should be considered a form of espionage, see Arthur S. Hulnick, *The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence*, *in* The Oxford Handbook of National Security Intelligence 229 (Loch K. Johnson ed., 2010).

rights law constraints) and wartime espionage (where there is greater degree of legal clarity as derived from the treatises of international humanitarian law ("IHL")).[31]

B. Old-School Absolutist Scholarship

The modern debates surrounding the permissibility of espionage in international law have their origins in the political philosophies of Kant and Hobbes. In *Perpetual Peace*, Kant described the "employment of spies" as one of those "diabolical arts" that are "intrinsically despicable."[32] Two years later in *The Metaphysics of Morals*, Kant expanded on his thinking, arguing that a state may not engage "underhanded" means of defense that could destroy the trust necessary for a lasting peace in the future, such as the utilizing of citizen-spies, assassins, poisoners, or propagandists.[33]

This Kantian approach inspired later lawyers to mobilize against what they perceived as a morally repugnant behavior. Fifty years prior to the materialization of the campaign to outlaw war with the Kellogg-Briand pact, a failed campaign to outlaw espionage was attempted in the Netherlands. In 1880, as part of the drafting of a manual on the laws of war at the Institute of International Law, a proposal was made and eventually rejected for a treaty to be adopted that suppressed of all forms of espionage.[34] Nonetheless, at that time period moral resentment to espionage was a view shared by a number of thinkers. E.I. Bekker from Heidelberg, for example, raised this flag again in 1912, describing the practice of spying as a "repulsive phenomenon" that could get in the way of "reasonable rapprochement among nations."[35] Modern prohibitionists include Professor Manuel Garcia-Mora,[36] Quincy Wright,[37] and the Dutch Court in *Re Flesche*.[38]

---

31. This is not to say that some of the regulations I propose might not also be applicable, *mutatis mutandis*, to both the domestic and wartime scenarios as well. In international law we are all too familiar with spillage between foreign and domestic legal frameworks as well as wartime and peacetime legal frameworks. The same is true for espionage.

32. Immanuel Kant, *Perpetual Peace: A Philosophical Sketch*, *in* KANT: POLITICAL WRITINGS 93, 97 (Hans Reiss ed., H.B. Nisbet trans., 1st ed., 1970) (1797).

33. IMMANUEL KANT, THE METAPHYSICS OF MORALS 127 (Lara Denis ed., Mary Gregor trans., revised ed. 2017) (1797).

34. Former Dutch Minister of War, Jacobus Catharjnus Cornelis den Beer Poortugael, was the one who pushed for the rejection of the proposal. For further reading, see ÉDOUARD CLUNET, QUESTIONS DE DROIT RELATIVES A L'INCIDENT FRANCO-ALLEMAND DE PAGNY (AFFAIRE SCHNÆBELÉ) 27 (1887); VICTOR COLONIEU, L'ESPIONAGE AU POINT DE VUE DU DROIT INTERNATIONAL ET DU DROIT PÉNAL FRANÇAIS 30 (Arthur Rousseau ed., 1888).

35. E. I. Bekker, *Staatsverträge wider die Spionage (State Treaties Against Espionage)*, 17 DEUTSCHE JURISTEN-ZEITUNG [DJZ] 297, 297 (1912) (translated from the original German).

36. 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) ("[P]eacetime espionage is regarded as an international delinquency and a violation of international law.").

37. *See* Wright, *supra* note 10.

38. *In re* Flesche, Holland Special Court of Cassation (27 June 1949), *reprinted in* 16 ANNUAL DIGEST AND REPORTS OF PUBLIC INTERNATIONAL LAW CASES: YEAR 1949, 266, 272 (Lauterpacht ed., 1955)

On the other end of the spectrum, Hobbes believed that the supreme law and duty of all sovereigns is to maintain the safety of their people.[39] To achieve that, states must collect intelligence, and Hobbes considered such spying a "natural right."[40] He likened intelligence agents to both "rays of light to the human soul" as well as to spiders' webs, "whose incredibly fine threads spread out in all directions and convey outside movements to the spiders sitting in their little cavities inside."[41] Much like Sun Tzu,[42] Nizam Al-Mulk,[43] and Hugo Grotius[44] before him, Hobbes shared the thinking that a leader who fails to spy is a lofty leader who abrogates a core responsibility.[45] Hobbes followed the Machiavellian notion that a ruler "must never stop thinking about war and preparing for war and he must work at it even more in peacetime than in war itself."[46] Modern permissivists have included Lassa Oppenheim,[47] Gary Sharp, Sr.,[48] Christopher Baker,[49] Julius Stone,[50] and the German Federal Court in the Espionage Prosecution Case.[51]

("[Peacetime espionage] when taking place by order of a State, constitutes an international delinquency by that State against another State for which it is answerable under international law.").

39. *See* Thomas Hobbes, On the Citizen 143 (Richard Tuck and Michael Silverthorne ed. and trans., 1998).

40. *Id.* at 145.

41. *Id.*

42. Sun Tzu, The Art of War 124 (Lionel Giles trans., 2015).

43. The 11th Century Persian scholar Abu Ali Hasan ibn Ali Tusi, or Nizam Al-Mulk, contended that "[i]t is indispensable for a sovereign to obtain information on his subjects and his soldiers, on all which happens near him or in distant regions, and to know about everything which is occurring, be it of small or great importance. If he does not do so, this will prove a disgrace, a proof of his negligence and neglect of justice." Charles E. Lathrop, The Literary Spy: The Ultimate Source for Quotations on Espionage & Intelligence 226 (2004).

44. Hugo Grotius, De Jure Belli Ac Pacis Libri Tres 655 (Francis W. Kelsey trans., 1925) (1625).

45. *See* Hobbes, *supra* note 39, at 143-45; *see also* Arthur S. Hulnick & Daniel W. Mattausch, *Ethics and Morality in U.S. Secret Intelligence*, *in* Ethics of Spying: A Reader for the Intelligence Professional 40, 40-41 (Jan Goldman ed., 2006) ("[B]ecause a state has the responsibility to its citizens to protect their lives, welfare, and property, it must take steps to understand the foreign threats, if there are any, to those citizens as well as to the nation as a whole. . . . Historically, the notion that 'Gentlemen do not read each other's mail' has proven dangerous when applied to a state's collection of information affecting national security.").

46. Niccolò Machiavelli, The Prince 58 (Tim Parks trans., 2009).

47. 1 Lassa Oppenheim, International Law: A Treatise § 455, at 491 (1905) (noting that "all States constantly or occasionally send spies abroad" and "it is neither morally nor politically and legally considered wrong" to do so).

48. Walter Gary Sharp, Sr., Cyberspace and the Use of Force 123 (1999) (claiming that in light of vast state practice international law has "specifically recognized a right to engage in [espionage] as an inherent part of foreign relations"). Sharp was the first, to my knowledge, to recognize that a right to spy under contemporary international law existed.

49. Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 Am. U. Int'l. L. Rev. 1091, 1112-13 (2004) (arguing that espionage was necessary as it facilitated both cooperative negotiations and cooperative compliance).

50. *See* Stone, *supra* note 10.

51. Espionage Prosecution Case (Case No 2 BGs 38/91), Bundesgerichtshof [BGH][Federal Court of Justice] Jan. 30, 1991, 94 International Law Reports [ILR] 68, 70, 1994 (Ger.) ("From the standpoint of international law, espionage in peacetime could not be considered as unlawful. No international agreement had ever been concluded on the subject. Neither was there any usage sufficient to establish a customary rule permitting, prohibiting or otherwise regulating such activity.").

A third absolutist movement considers espionage as existing outside the bounds of law, being "neither legal nor illegal." Today, many international legal scholars share the ominous contention that espionage, as a legal field, is devoid of meaning. For them, any attempt to extrapolate the *lex lata* corpus of the ILI, let alone its *lex scripta*, would inevitably flounder, as there is nothing to extrapolate—espionage is simply an extralegal construct.[52]

In fact, the notion that international law is moot as to the question of if, when, and how intelligence is to be collected, analyzed, or dispensed, has been repeated so many times that it has become the prevailing view.[53] This fiction forms the basis for a *Lotus* world of action,[54] one in which "states may spy on each other – and on each other's nationals – without restriction,"[55] justifying their behavior through the *argumentum ad hominem* of "*tu quoque.*"[56] Perhaps the most forceful proponent of this extralegal agenda in recent years has been former Assistant General Counsel to the CIA, Professor Afsheen Radsan.

As a participant in a 2007 symposium organized by the *Michigan Journal of International Law*, Radsan produced an article where he compared the at-

52. *See, e.g.*, Jeffrey H. Smith, *Keynote Address: State Intelligence Gathering and International Law*, 28 MICH. J. INT'L L. 543, 544 (2007) ("[M]ost lawyers would likely scoff at the notion that espionage activities are constrained in any meaningful way by international law. Indeed, most probably believe that international law's only influence on espionage is that in wartime, spies caught behind the lines out of uniform can be shot. Hardly a sophisticated or, to intelligence services, comforting notion."); Baker, *supra* note 49, at 1091 ("Espionage is curiously ill-defined under international law."); Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SEC. L. & POL'Y 115, 116 (2014) ("[T]here is a long-standing (and cynically named) 'gentleman's agreement' between nations to ignore espionage in international law.").

53. Sulmasy & Yoo, *supra* note 23, at 637-38 ("International law has never prohibited intelligence collection, in peacetime or wartime . . . . The history of state practice reveals that the regulation of intelligence gathering has always been left to domestic enforcement . . . . Calls to pursue the establishment of international entities or international law to regulate the intelligence collection activities of nations-states are counterproductive."); Deeks, *supra* note 9, at 293 ("[W]hy has international law had so little to say about how, when, and where governments may spy on other states and foreign citizens, including by electronic means? . . . states sensibly concluded that the benefits to unregulated spying were high and the corresponding costs were few.").

54. Falk clarifies the role that the *Lotus* decision plays within the conventional account in explaining the practice of peacetime espionage: "[A] voluntaristic theory of international obligations, as formulated by the *Lotus* majority decision, gives a supporting analysis. The basic idea is that the objecting state has the burden of showing that the defendant state acted in violation of an existing rule of international law. Put affirmatively, this means that a state may do whatever it is not expressly forbidden to do by international law. Thus, in areas where there is no consensus as to even the existence of a legal order, much less its quality, a state may do whatever it pleases, subject only to another state's right to act in self-defense. Specifically, the United States may launch its observational satellites and the Russians may shoot them down if they purport to do so in self-defense." Falk, *supra* note 10, at 68.

55. Deeks, *supra* note 9, at 301 ("Several government officials and scholars believe that the *Lotus* approach provides the best way to think about spying in international law. For them, the idea is simply that nothing in international law forbids states from spying on each other . . . Spying is therefore unregulated in international law.").

56. OFFICE OF GENERAL COUNSEL, DEPARTMENT OF DEFENSE, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 40 (1999) ("The lack of strong international legal sanctions for peacetime espionage may also constitute an implicit application of the international law doctrine of 'tu quoque' (roughly, a nation has no standing to complain about a practice in which it itself engages).").

tempts at regulating espionage with wizardry and alchemy. For Radsan, espionage and international law could not be reconciled "in a complete synthesis," for the two start from different premises—one is rooted in the peaceful resolution of conflicts, due regards to the rights of others, and good faith and honest dealing; the other is centered around "treachery and deceit."[57] He therefore concluded that "[i]nternational law does not change the reality of espionage,"[58] sending a clear message to future scholars interested in engaging in research and writing on the topic: "move to other projects—with grace."[59]

C. *New-School Relativist Scholarship*

Gracefully rejecting Radsan's invitation, scholars in recent years have moved towards the development of a fourth theoretical camp. This camp may be described as the "sometimes legal, sometimes illegal" camp, or the relativist piecemeal approach to the ILI. In this group we find writing that "abandons the debate of whether 'intelligence gathering' or 'espionage' is per se legal or illegal and instead subdivides the world of intelligence collection into constituent state acts . . . examin[ing] law governing specific conduct."[60] We could place the works of the likes of Craig Forcese,[61] Iñaki Navarrete,[62] Russell Buchan,[63] and Fabien Lafouasse,[64] in this camp,[65] as well as Tallinn Manual 2.0.[66]

57. *See* Radsan, *supra* note 9, at 596.

58. *Id.* at 623.

59. *Id.* at 597.

60. Forcese, *supra* note 9, at 68.

61. *Id.*; *see also* Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SEC. L. & POL'Y 179 (2011).

62. *See* Iñaki Navarrete, *L'espionnage en temps de paix en droit international public*, 53 CAN. Y.B. INT'L L. 1 (2015); *see also* Iñaki Navarrete & Russel Buchan, *Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions*, 51 CORNELL INT'L L. J. 897 (2019).

63. *See* RUSSELL BUCHAN, CYBER ESPIONAGE AND INTERNATIONAL LAW 192-93 (2019) (referring to a "patchwork of norms" constraining acts of cyber espionage, which may be derived from examining diplomatic and consular law, international human rights law, international trade law, and the law on sovereignty); *see also* Navarrete & Buchan, *supra* note 62.

64. *See* FABIEN LAFOUASSE, L'ESPIONAGE DANS LE DROIT INTERNATIONAL (2012). The final conclusion of the book, in line with the piecemeal account, is that while an act of spying *ipso facto* is not unlawful but only an unfriendly and tolerated act, specific types of spying operations conducted within the territory of a state would violate its sovereignty and therefore constitute a violation of international law that may trigger state responsibility. *See id.* at 461.

65. These scholars might have found their theoretical underpinnings in more historical works that made similar claims. *See, e.g.*, Gérard Cohen-Jonathan & Robert Kovar, *L'espionnage en temps de paix*, 6 ANNUAIRE FRANÇAIS DE DROIT INT'L 239, 246 (1960) (noting that "undoubtedly espionage is unlawful when it uses means that are prohibited by international law"); Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. INT'L L. 53, 67-69 (1984) (suggesting that "espionage appears to be illegal under international law in time of peace if it involves the presence of agents sent clandestinely by a foreign power into the territory of another state" and giving the example of diplomats committing acts contrary to international law in the gathering of secret information); NOYES E. LEECH, COVEY T. OLIVER, & JOSEPH M. SWEENEY, CASES AND MATERIALS ON THE INTERNATIONAL LEGAL SYSTEM 264 (1973) (suggesting that espionage is illegal only if it involves trespass to the territory of other states).

66. *See* TM 2.0, *supra* note 12, and accompanying text.

Two features are common to piecemeal scholars. First, these scholars equally discredit the "*lex specialists*" as they do the "*extralegalists*."[67] For them there is no special customary body of international law that can be said to control the intelligence function.[68] We should only look within the broader *lex generalis* (namely the Charter principles of territorial sovereignty and non-intervention, human rights law, and diplomatic and consular law) to identify norms that control all of state behavior, then apply those most relevant amongst them. As a result of their methodology, the framework adopted by these scholars is one that puts significant emphasis on questions of territoriality.[69] An undercover spy in a fedora hat and trench coat taking pictures of a foreign parliament house,[70] or a diplomat conducting intelligence operations against her host country from within her embassy,[71] will always violate international law, as they violate both general treaty provisions (for example those enshrined in the Vienna Convention on Diplomatic Relations ("VCDR")) and general customary principles (for example the principle of territorial sovereignty). These scholars thus limit acts of lawful

67. *See, e.g.*, Forcese, *supra* note 9, at 81 ("The take-home point is this: to the extent that commentators are inclined to treat intelligence activities as a unique area immunized from international law or subject to some special, more relaxed *lex specialis*, they exaggerate considerably."); *see also* Navarrete & Buchan, *supra* note 62, at 952 (suggesting that extralegalist arguments are "no longer taken seriously," arguing further that the defenders of espionage have begun claiming the existence of customary exceptions, an argument which Navarrete and Buchan believe should be equally debunked).

68. *See, e.g.*, TM 2.0, *supra* note 12, at 169-70 ("[T]he IGE agreed that customary international law does not prohibit espionage *per se*."). Note that the Experts relied on a single source, the Office of General Counsel, Department of Defense Law of War Manual, to make this claim. However, paragraph 16.3.2, to which they cite, makes no reference to a lack of customary regulation of espionage under international law. Quite the opposite: it speaks clearly of "long-standing and well-established considerations" and "long-standing international norms" which govern this practice. Department of Defense, Law of War Manual 990 (2016). The IGE further concluded that while there are no customary rules in international law prohibiting spying *per se*, espionage may nonetheless be conducted "in a manner that violates international law due to the fact that certain of the methods employed to conduct cyber espionage are unlawful." TM 2.0, *supra* note 12, at 169–70. The experts claimed that the principle of territorial sovereignty, the prohibition on coercive intervention, and the human right to privacy could all be cited as bases for a violation of international law by particular methods of spying. *Id.*; *see also* Navarrete & Buchan, *supra* note 62, at 902 (referring to "a 'checkboard' of principles of international law . . . that indirectly regulate peacetime espionage on the basis of the underlying conduct of States.") Note further that a minority of the members of the IGE were willing to entertain the idea that there exists a *lex specialis* of espionage law, but their position was ultimately rejected. *Id.* at 19.

69. For example, see the concluding tables provided in Forcese, *supra* note 61, at 209 and Navarrete, *supra* note 62, at 63-64, as well as the figure in Lafouasse, *supra* note 64, at 311. They all establish distinctions of law based on the activity's territorial or extraterritorial nature.

70. *See, e.g.*, TM 2.0, *supra* note 12, at 19 (the majority took the view that, "if organs of one State are present in another State's territory and conduct cyber espionage against it without its consent or other legal justification, the latter's sovereignty has been violated." The majority acknowledged that there is widespread state practice of such acts of spying, but nonetheless argued that, "States have not defended such actions on the basis of international law.").

71. *Id.* at 211-12, 229 (the IGE argues that if a sending state launches spyware from within its diplomatic mission against the cyber infrastructures of another state that would constitute "an abuse of the diplomatic function and therefore an internationally wrongful act"). The same is true for the opposite, spying on a diplomatic mission. Forcese has claimed that spying on diplomats, even if widespread, cannot be squared with the actual rules found in the VCDR and therefore "while spying on diplomats may be commonplace, it is no less a violation of the Convention." *See* Forcese, *supra* note 61, at 197.

espionage only to those activities that take place remotely[72] (for example remote sensing from a satellite, aerial or naval vehicles, or remote interception of communications that just happen to cross through the surveilling state's electromagnetic spectrum or internet infrastructure),[73] or with the knowledge and authorization of the target state or the Security Council.

This framing of the ILI is unsatisfactory for four reasons. Most significant is the fact that this approach ignores widespread state practice of interstate territorial and diplomatic spying as well as the crucial functions that such intelligence operations play in our contemporary legal order. Relying heavily on the myth system, by merely citing generic treaty provisions and *lex generalis* principles, these scholars seem to give no weight to the operational code. They try to defend this point by citing to the silence of states. If secrecy surrounds peacetime espionage, that is to say if countries are unlikely to provide public statements in support of their operations, there is no *opinio juris* and therefore there can be no basis to make claims for customary rights or exceptions that could justify such spying.[74] Navarrete and Buchan adopt an ever more poetic tone. As they write:

> The essence of the problem is this. Customary espionage exceptions have yet to clear a path through the legal wilderness. If the path-takers zigzag so that there are no clear tracks; if they are careful to cover their footprints; and if they consistently deny following new tracks when they are caught in the act, then there can be no identifiable paths and no understanding that they *should* be followed.[75]

This argument is problematic as it treats secrecy as if existing in a binary. Either something is secret and therefore it should have no impact on the evolution of custom or it isn't. In reality, however, every act of state secrecy is located on a continuum between two poles: shallow secrets and deep secrets.[76] Shallow secrets, those secrets the general existence of which is known (even where detailed specifics about them remain hidden), do in fact

72. Note that Forcese and Navarrete distinguish further between two types of "remoteness" — acts that are purely extraterritorial (where both the governmental agents and their targets are located on the territory of another state) and acts that are transnational (where the target of the surveillance, for example the documents or the communications, are located/taking place on the territory of another state, but the governmental agents are at home).

73. Consider in this regard the European Court of Human Rights decision in Weber & Saravia v. Germany, 2006-XI Eur. Ct. H.R. 309 ¶ 88.

74. *See* Buchan, *supra* note 63, at 161 ("[S]ilence is the antithesis of *opinio juris* and under these conditions state practice cannot mature into binding rules of customary law . . . ."). Baked into Buchan's argument is the additional notion that practice must be of a public character to contribute towards the development of customary international law. This is because only public displays of state practice can be the subject of an "iterative process of claim and response" between sovereign states from which custom can emerge. *See* Navarrete & Buchan, *supra* note 62, at 920.

75. Navarrete & Buchan, *supra* note 62, at 952-53.

76. For further reading, including a summary of the literature around shallow and deep secrets, see David E. Pozen, *Deep Secrecy*, 62 Stan. L. Rev. 257 (2010).

play a role in our understanding of the evolution of custom.[77] In that regard, peacetime espionage is becoming more and more a shallow secret. The silent war is no longer so silent.[78] These open secrets can and do shape law-making processes and their substantive outcomes in more nuanced ways, such as in the relationship between the secret-knowers, the intelligence agencies and governments. As noted by the former legal advisor to the Foreign and Commonwealth Office of the U.K. Government, Sir Daniel Bethlehem, "one cannot make assumptions about what the law is, or reach considered conclusions on whether conduct is lawful or unlawful, until one has considered the invisible conduct, as well as the visible."[79]

Ultimately, because they ignore state practice and deny the prospect of *opinio juris*, these scholars fail to truly capture the reality and thereby lose their target audience: members of intelligence communities who are unlikely to accept such stringent normative framing. For this exact reason, McDougal, Lasswell, and Reisman took a completely different position in 1973, suggesting that "[t]he gathering of intelligence within the territorial confines of another state is not, in and of itself, contrary to international law unless it contravenes policies of the world constitutive process affording support to protected features of internal public order."[80] Obsessing over territoriality, in the way that piecemeal scholars tend to do, misses a real opportunity for us to begin articulating what those "policies" and "protected features" might be in our contemporary world.

Take for example the issue of diplomatic and consular law. As Chesterman notes, "[d]iplomacy and intelligence gathering have always gone hand in hand."[81] Citing to the emergence of modern diplomacy in Renaissance Italy, Chesterman highlights that "a chief function of the resident ambassador soon became to ensure that a continuous stream of foreign polit-

77. Daniel Bethlehem, *The Secret Life of International Law*, 1 CAMBRIDGE J. INT'L & COMP. L. 23, 36 (2012); *see also* Alexandra H. Perina, *Black Holes and Open Secrets: The Impact of Covert Action on International Law*, 53 COLUM. J. TRANSNAT'L. L. 507, 568 (2015) (suggesting that the non-acknowledgement by the acting state of a certain act would preclude it "from relying on that conduct as evidence that defines or shapes the law," but doesn't preclude everyone else from relying on it). This makes sense. Instead of suggesting that everyone is barred from relying on open secrets in the development of new customary international rules, we limit this sanction only to the ones who continue to deny the action ever took place. This could incentivize those "neither-confirm-nor-deny" states to favor policies that support greater transparency, statutory interpretation, and public regulation as a gateway into getting a seat around the rule-making table.

78. Jack Goldsmith, *A Partial Defense of the Front-Page Rule*, HOOVER INSTITUTION (Jan. 29, 2014), https://perma.cc/5MKX-AWNM ("[S]ecret intelligence actions . . . are increasingly difficult to keep secret.").

79. Bethlehem, *supra* note 77, at 36.

80. McDougal, Lasswell & Reisman, *supra* note 17, at 395.

81. Chesterman, *supra* note 4, at 1087; *see also* W. Michael Reisman, *Accord on Embassy Espionage Would Ease U.S.-Soviet Tensions*, NEW HAVEN REG., Sept. 11, 1988, at B3 ("Diplomacy and espionage are related and sometimes even symbiotic. Getting [intelligence on a foreign enemy] requires placing people you can trust in your enemy's capital. That's why diplomacy was invented . . . Embassies that can't collect information and relay it back in secrecy to their governments are ineffective.").

ical news flow[ed] to his home government."[82] This is why ambassadors were described as early as the 17th century as "honorable spies."[83] These acts of diplomatic spying continue even more forcefully in the age of electronic communications. During the enactment of the U.S. Foreign Intelligence Surveillance Act in 1978, for example, Congress discussed the issue of electronic surveillance of diplomatic premises and its compatibility with the rules of the VCDR at length. As Forcese highlights: "[t]he Administration overcame this concern by supplying a list of states that surveilled U.S diplomatic premises abroad, suggesting that such a widely accepted practice, while not authorized by the Convention, did not violate it."[84] There is significant evidence to back the administration's argument, as the practice of spying from and on diplomatic missions is indeed as historical as it is commonplace.[85]

Consider the following three alleged reports from the past two decades: (1) In the lead up to the U.N. Security Council vote authorizing to use force against Iraq in 2003, the United States and the United Kingdom spied on delegations to the Security Council;[86] (2) During the G20 talks in Toronto in 2010, the United States and Canada spied on large numbers of heads of states and other diplomats in attendance,[87] and in 2013 it was Russia's turn to provide its guests with bugged gift bags in the form of malware-filled USB sticks as part of the G20 summit in Saint Petersburg;[88] (3) Between 2012 and 2017, Chinese agencies used backdoors into computer networks at the African Union Headquarters (networks which China paid for and installed as a gift) in order to spy on the various delegations.[89]

If one wanted to apply the new school piecemeal model to these operations, one would have to conclude that all of them violated international law, because "while spying on diplomats may be commonplace, it is no less a violation of the Convention."[90] Adopting this position seems skewed. It stays true to a zealous defense of textual provisions while failing to give weight to the robust practice of states, which not only conduct such surveillance operations, but indeed tolerate them as a component of international

82. Chesterman, *supra* note 4, at 1087.

83. Ithiel de Sola Pool, *International Intelligence and Domestic Politics*, *in* Surveillance and Espionage in a Free Society 272, 274 (Richard H. Blum ed., 1972).

84. *See* Forcese, *supra* note 61, at 197.

85. *See* Deeks, *supra* note 9, at 313 (citing Antonin Scalia, who at the Department of Justice OLC drafted a memorandum that concluded that "the practice of spying on foreign missions was so widespread that the 'inviolability' provision of the VCDR should not be read to prohibit such activities").

86. *See, e.g.*, Martin Bright & Peter Beaumont, *Britain Spied on UN Allies over War Vote*, The Guardian (Feb. 7, 2004), https://perma.cc/TY8U-UCD2.

87. *See, e.g.*, Paul Owen, *Canada 'Allowed NSA to Spy on G8 and G20 Summits'*, The Guardian (Nov. 28, 2013), https://perma.cc/EX65-2S2A.

88. *See, e.g.*, Stuart Heritage, *Putin's USB Spy Sticks and Other Dodgy Espionage Tricks*, The Guardian (Oct. 30, 2013), https://perma.cc/MH7C-LD6G.

89. *See, e.g.*, Reuters, *China Rejects Claim it Bugged Headquarters it Built for African Union*, The Guardian (Jan. 29, 2018), https://perma.cc/XPN3-QZ9J.

90. *See* Forcese, *supra* note 61, at 197.

political life.[91] Piecemeal scholars seem to abet their own deception, "avoiding the truth like someone pulling blankets over his head to avoid the cold reality of dawn."[92] However, as Kelsen had taught us "the validity of the law presupposes a minimum efficacy of the law."[93] If the myth system becomes so disassociated with the operational code, it losses all sense of gravitas; piecemeal scholars seem to show no degree of concern to this fact, far from it—they shine light on this disconnect, thereby intensifying it.

To be clear, I am very sympathetic to piecemeal scholars' attempts to push the envelope of the ILI by sketching normative lines. I further support the general idea that the legality of espionage operations is relative—sometimes legal and sometimes illegal depending on a case-by-case analysis of the circumstances. Nonetheless, the basis for such determinations of law cannot rest solely on the technical question of the territory from which the operation is taking place, or the existence of certain international protections, immunities, or privileges around the specific target of the surveillance in question. These factors are but some of many criterions that need to be examined before a conclusion on legality can be reached.[94]

A second reason to reject the existing relativist account is its ineffectiveness in regulating the entire phenomenon of espionage. Piecemeal scholars address only the law governing specific methods of spying in isolation from

---

91. *See* W. Michael Reisman & Eric E. Freedman, *The Plaintiff's Dilemma: Illegally Obtained Evidence and Admissibility in International Adjudication*, 76 Am. J. Int'l L. 737, 751-52 (1982).

92. *See* W. Michael Reisman, *Myth System and Operational Code*, 3 Yale Stud. World Pub. Ord. 229, 237 (1977). Dinstein, who wrote about certain law of armed conflict scholarship which has gone so left of field that it has disconnected itself from battleground realities, such "legal chatter of armchair quarterbacks is no different from static in a telecommunications system. It must be separated from the genuine sound of law." Yoram Dinstein, *Keynote Address: The Recent Evolution of the International Law of Armed Conflict: Confusions, Constraints, and Challenges*, 51 Vand. J. Transnat'l L. 701, 709 (2018). Speaking more broadly, Glennon has written that "[t]reaty rules as well as customary rules fall into desuetude when they change from working rules to paper rules. Clarity of analysis is not advanced by confusing the two; paper rules may still in some circumstances generate compliance, but not often enough to qualify as law, for the key element of obligation is missing." Michael J. Glennon, The Fog of Law: Pragmatism, Security, and International Law 228 (2010).

93. *See* Hans Kelsen, Law and Peace in International Relations: The Oliver Wendell Holmes Lectures, 1940-1941 16 (1942).

94. In the analysis of the *Jus In Exploratione*, that is the law that governs the choice of means and choice of targets during an espionage operation, one consideration would have to be whether the operation is proportionate, which would be derived in part by its level of intrusiveness. This echoes moral philosophy theories that center around a metaphorical "escalation ladder." *See, e.g.*, Ross W. Bellaby, The Ethics of Intelligence: A New Framework 170 (2014); R. V. Jones, Reflections on Intelligence 50 (1989); Loch K. Johnson, *On Drawing a Bright Line for Covert Operations*, 86 Am. J. Int'l L. 284, 305 (1992); *see also* Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 Va. L. Rev. 599, 671-75 (2016) (suggesting that we adopt a pragmatist sliding scale taking into consideration different variables to determine the degree of flexibility intelligence agencies should be given in interpreting relevant international law. Those variables are: (1) the risk of error and quantum of harm; (2) the identity and nature of the target; (3) the nature of the international rules potentially violated; and (4) the existence of more overt and less intrusive means for achieving a similar aim). I completely endorse these factors, but I would go even further to suggest that Deeks's flexible analysis might have actual legal (and not mere policy) underpinnings if one considers certain general principles of international law (such as rule of law, good faith, proportionality, effectiveness, fairness, and comity) as rule clarifiers.

intelligence programs as a whole. In other words, they offer regulation of the *Jus In Exploratione* (the law governing the choice of means and targets in the conduct of spying) while leaving a lacuna as far as the *Jus Ad Explorationem* is concerned (what limits exist on the decision to launch espionage operations in the first place). In so doing they exacerbate a known problem in the literature on intelligence ethics: the vast majority of the literature seems to only be interested in "the ethical dilemmas raised during the collection of intelligence"[95] while ignoring the ethical dilemmas raised during all other stages of "the intelligence cycle."[96] By rejecting the idea that there exists a *lex specialis* of espionage law, piecemeal scholars have barred themselves from having any say over which are and are not legitimate reasons for spying. If legality is only rooted in an analysis of the means selected by the agencies, not in their programmatic motivations, then there is no room for international law to regulate much of the decision-making around which operations should be deemed necessary, and in fact on what necessity ultimately means for spycraft. Analogizing to the use of force, contemporary piecemeal thinkers seem eager to explain whether the use of chemical weapons or white phosphorus violates international law before they address the analytically distinct and far larger question of if and when is it lawful to go to war in the first place. Before we engage in a tactical review of the legality of particular means of spying (say bribery, torture, non-official covers, mass surveillance, CCTV cameras, or automated facial recognition), we should ask ourselves if and when is it lawful to spy. This is the focus of this paper.

A third concern with relativist piecemeal scholarship relates to the role it plays in entrenching regional and global social structures and enforcing a specific constellation of power and knowledge dynamics. This concern brings to bear Third World Approaches to International Law ("TWAIL") literature. Authorizing remote spying while prohibiting territorial spying serves the goals of those states who are sufficiently powerful and technologically advanced to have the capacity to engage in such expensive forms of espionage. Chimni had written that "where international law does not penetrate national spaces, powerful states put into effect laws that have an extraterritorial effect; third world states have little control over processes initiated without [their] consent in distant spaces."[97] Western foreign surveillance laws that authorize these programs of bulk remote interception of communications offer an example. Third world countries are impacted twice

95. Hans Born & Aidan Wills, *Beyond the Oxymoron: Exploring Ethics Through the Intelligence Cycle*, *in* 2 Ethics of Spying: A Reader for the Intelligence Professional 34, 45 (Jan Goldman ed., 2010).

96. What has come to be known as the "intelligence process/cycle" refers to a cyclical chain of routine steps taken "from policy makers perceiving a need for information to the community's delivery of an analytical intelligence product to them." *See* Lowenthal, *supra* note 22, at 70. Most articulations of this cycle follow the same general structure: (a) planning and direction; (b) collection; (c) processing; (d) analysis; (e) dissemination and consumption; then back to (a) and the wheel goes round and round.

97. *See* B.S. Chimni, *Third World Approaches to International Law: A Manifesto*, *in* The Third World and International Order: Law, Politics, and Globalization 47, 57 (Antony Anghie et al. eds., 2003).

by the piecemeal conceptualization of espionage law: once because they become the subject of these mass remote surveillance programs over which they have no control, and again because their own more primitive and less costly forms of territorial and diplomatic spying have now been deemed unlawful.

What is more, a legal regime that is based on legitimizing remote forms of espionage while prohibiting territorial spying further incentivizes states to rely on corporate actors as "surveillance intermediaries"—remote collectors and analyzers of raw digital communications and communications data.[98] We have witnessed this development in recent years, states turning to social media corporations and internet service providers to do the hard work of storing our ever-growing volumes of online human experiences further profiling our behaviors, from our iPhones tracking our geolocation and email metadata, to our Amazon Ring Doorbells security cameras surveilling our streets, to our FitBits marking changes in our physical activities.[99] This trend triggers "a global law without the state," a "*lex mercatoria*" where "the transnational corporate actor is the principal moving force in decentralized law-making."[100] Piecemeal scholars have overlooked potential TWAIL-critiques of their articulation of the ILI, a dynamic that has helped "create a global system of governance suited to the needs of transnational capital but to the disadvantage of third world peoples."[101]

Finally, as information becomes more "un-territorial,"[102] and as espionage goes more and more digital,[103] relying on territorial line drawing as the sole basis for the regulation of intelligence operations becomes less defensible. It should, therefore, not be surprising to find piecemeal scholars struggling to stipulate what rules should govern cyber-espionage. For how should we treat a scenario where agents from Country A, while sitting in their headquarters, gain complete access to and steal documents from governmental computers located in Country B, while spoofing servers located in Countries C, D, and

98. *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 112 (2018) ("In today's world, government surveillance—whether targeted or programmatic, for law enforcement or foreign intelligence—relies on the cooperation of a small number of technology companies that are large, multinational, and opposed to it.").

99. *See*, *e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 387 (2019) (describing how both intelligence agencies and law enforcement have turned to what Zuboff coins "instrumentarian power" to conduct their investigations. She specifically provides the examples of Fitbits, Amazon Echo, and smart pacemakers, as well as broader collaborations with Google and Facebook in the fight against international terrorism).

100. *See* Chimni, *supra* note 97, at 58.

101. *Id.* at 60; *see also* RATNA KAPUR, EROTIC JUSTICE: LAW AND THE NEW POLITICS OF POSTCOLONIALISM 22 (2005).

102. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326, 365–78 (2015).

103. *See* Forcese, *supra* note 9, at 77-78 ("Until recently, there was an obvious territorial element to covert actions—and indeed, almost all intelligence activity—that eased the assessment of legality . . . . The communications revolution, however, has changed the physical locus of at least some state action and has therefore created awkward questions for geocentric international law."); *see also* TM 2.0, *supra* note 12, at 170-71 ("The Experts were incapable of achieving consensus as to whether remote cyber espionage reaching a particular threshold of severity violates international law.").

E?[104] The Canadian courts seem to have adopted the position that such operations would result in extraterritorial enforcement actions in violation of international law.[105] But to suggest that these operations are either akin to or distinguishable from physical human spying is a matter of choosing one's preferred analogy, and whatever analogy is eventually endorsed seems to me to likely be difficult to justify, hard to explain, and complicated to apply.[106] Ultimately, we should agree that such cyber/kinetic comparisons are susceptible to manipulation in the name of advancing particular policy agendas, as is the case for all analogizing in the field of law and technology.[107]

The problem of using territorial lines as the legal standard for addressing new forms of remote surveillance has also manifested itself in the debates surrounding maritime and aerial reconnaissance operations conducted from inside and above a coastal state's Exclusive Economic Zone ("EEZ"). Much like cyberspace, the EEZ's legal regime's interaction with the principle of sovereignty is a tenuous one. Galdorisi and Kaufman described the EEZ as a "zone of tension between coastal state control and maritime state use of the sea," for it is where territorial waters clash against waves from the high seas.[108] This tension, coupled with the advancement of new maritime surveillance technologies for reconnaissance, has triggered multiple well-publi-

104. *See, e.g.,* Aaron Shull, *Cyber Espionage and International Law*, GigaNet: Global Internet Governance Academic Network, Annual Symposium 1 (2013) (noting that cyber intrusions do not seem to offend the principle of territorial integrity in the same way as the sending an actual state agent to gather human intelligence.) Ultimately, Shull concludes that "[t]he international governance regime surrounding cyber espionage is still in its infancy" and that "the norms that govern conduct in cyber space are in a period of flux and evolution." *Id*. at 15. As such "it is not entirely clear how the legal rules or norms of conduct will develop within this policy space." *Id*. at 19; *see also* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1 (2017) (discussing the legal grey zones associated with below-the-threshold remote cyber operations, including cyber-espionage, and the difficulty in applying traditional international law principles such as sovereignty and non-intervention to them).

105. In the Matter of an Application by [redacted] for Warrants Pursuant to Sections 16 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, c C-23, 2018 F.C. 738, ¶¶119–47 (Can.).

106. Buchan had made the claim that "states exercise territorial sovereignty over the cyber infrastructure that is physically located within their territory." He further argued that "an act of cyber espionage . . . . that penetrates computer networks and systems supported by cyber infrastructure situated within the territory of another state constitutes a violation of that state's territorial sovereignty, irrespective of whether that operation causes damages or harm." *See* BUCHAN, *supra* note 63, at 54. Buchan further argues that his contention is rooted in state practice. *Id*. This argument stands in stark contradiction with the recent collapse of the negotiations of the UN Group of Governmental Experts on Information Security after they failed to reach agreement as to the way the U.N. Charter principles, including the principle of sovereignty, should apply to cyberspace, *see, e.g.,* Elaine Korzak, *UN GGE on Cybersecurity: The End of an Era?*, THE DIPLOMAT (July 31, 2017), https://perma.cc/8SEF-VKS7, as well as the recent statement of the U.K. Attorney General who refused to apply the principles of sovereignty to cyberspace*, see, e.g.,* Jeremy Wright QC MP, *Cyber and International Law in the 21st Century*, ATTORNEY GENERAL'S OFFICE (May 23, 2018), https://perma.cc/PAS6-RK44.

107. Ryan Calo, *Robots as Legal Metaphors*, 30 HARV. J. L. & TECH. 209, 214 (2016) ("[T]he law and technology literature—particularly around information privacy—is plainly aware of the role metaphor can play in channeling legal outcomes in the context of emerging technology.").

108. George V. Galdorisi & Alan Kaufman, *Military Activities in the Exclusive Economic Zone: Preventing Uncertainty and Defusing Conflict*, 32 CAL. W. INT'L L. J. 253, 257 (2002).

cized confrontations around EEZ surveillance.[109] Adopting a piecemeal geographical zoning of espionage law fails to offer us a framework for mitigating these tensions, as we are unable to conclude determinatively whether spying within or above the zone—like in cyberspace—is akin to territorial surveillance and therefore illegal or to surveillance from the global commons and therefore legal. The development of high-altitude durable surveillance balloons and drones poses a similar challenge as we find it difficult to identify the legal lines between spying from the territorial airspace and outer space.

Piecemeal normative accounts fail to persuade as they ignore the open secret that all states engage in peacetime territorial and diplomatic spying; they avoid an analysis of the functions of espionage and thereby the justifications for launching espionage operations; they neglect to address TWAIL-critiques further incentivizing a market for private surveillance by affluent states; and they rest on territorial line drawing in a surveillance age that is proving more and more unterritorial. A new normative account is thus sorely needed.

D. Introducing the Lex Specialis of the ILI

The European Court of Human Rights ("ECtHR"), in its groundbreaking *Zakharov v. Russia* decision, laid the foundation for the regulation of clandestine intelligence gathering. The court clarified that secret surveillance measures may be reviewed "[A]t three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated."[110] A normative diagnosis of intelligence done at three distinct temporal phases (before, during, and after) should not seem unfamiliar to students of international law. After all, our traditional paradigms for controlling violence, enshrined in the post-Charter prohibition on the use of force, already recognize the distinction between *Jus Ad Bellum ("JAB")*, *Jus In Bello ("JIB")*, and *Jus Post Bellum ("JPB")*.

If peacetime espionage serves the dual role of being both the great political stabilizer (increasing the potential for peaceful settlement of disputes and cooperation by reducing the chances for strategic surprises)[111] and the great political destabilizer (working in the service of the "continuation of war by the clandestine interference of one power into the affairs of another

109. *See* Asaf Lubin, *The Dragon-Kings Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum*, 57 Washburn L. J. 17 (2018).

110. *Roman Zakharov v. Russia*, 2015-VIII Eur. Ct. H.R. 58–59.

111. *See* James E. Baker, *Prelude to Decision: Michael Reisman, the Intelligence Function, and a Scholar's Study of Intelligence in Law, Process, and Values*, *in* Looking to the Future: Essays on International Law in Honor of W. Michael Reisman 73, 76 (Mahnoush H. Arsanjani et al. eds., 2011); Michael Herman, *Ethics and Intelligence after September 2001*, *in* 2 Ethics of Spying: A Reader for the Intelligence Professional 106 (Jan Goldman ed., 2010) ("[G]overnments drawing on a professional standard of intelligence knowledge tended to behave as more responsible members of international society than those that had to manage without it, or chose to do so . . . .").

power,"[112] triggering an intelligence-driven security dilemma spiral[113]) it makes sense to tie its regulation to the same international structures that bind states' use of their other stability-impacting apparatuses: their military, diplomatic, and ideological instruments.

Philosophical literature surrounding the ethics of intelligence work has proposed that Just War Theory ("JWT") might serve as a useful tool in the regulation of espionage. In 1986 at a Conference on Military Ethics and Education in Washington D.C., Chomeau and Rudolph introduced one of the earliest detailed articulations of the application of JWT to the practice of espionage, arguing that "implied in 'just war' theory [is] a basis for the right of one government to interfere in the affairs of another, so long as the principles of just cause, just means, proportionality, etc., prevail."[114] Similarly, in 1989 William E. Colby argued that standards for the selection of just covert activities "can be developed by analogy with the long-standing effort to differentiate just from unjust wars."[115] As is explicit in the name, Just War Theory is a doctrine of ethics establishing criteria for the utilization of organized armed force, not espionage. Nonetheless, there are compelling reasons to compare and analogize clandestine intelligence collection and the use of force as the two are "sources of national power and instruments of foreign policy" that are routinely used by states to "defend their own national interests and manage world peace and stability" and which "give[ ] rise to ethical concerns" for their violation of core communal principles, like the principles of non-intervention, territorial integrity, and sovereign equality.[116] What is more, intelligence operations are not only similar in nature to uses of force; they are also extensions of them, derivative prerequisites necessary to operationalize those very uses.[117]

For these reasons, there is an analytical justification to subject both the right of states to use force and the right of states to spy to the same founda-

112. James Der Derian, Antidiplomacy: Spies, Terror, Speed, and War 21 (1992).

113. *See* Michael Herman, Intelligence Power in Peace and War, 371 (1996) (Herman explains that intelligence gathering "may produce its own spiral of increased threat perceptions among its targets, leading to more secrecy and more intrusive collection.").

114. John B. Chomeau & Anne C. Rudolph, *Ethical "Need to Knows" for Intelligence Officers,* 2 (1986), https://perma.cc/F86F-QTND.

115. William E. Colby, *Public Policy, Secret Action,* 3 Ethics & Int'l Aff. 61, 63 (1989); *see also* James A. Barry, *Managing Covert Political Action: Guideposts from Just War Theory*, 36 Stud. Intelligence 19 (1992).

116. Angela Gendron, *Just War, Just Intelligence: An Ethical Framework for Foreign Espionage*, 18 Int'l J. Intelligence & Counterintelligence 398, 408-10 (2005).

117. Bitton, *supra* note 25, at 1017 ("The argument has two distinct forms. In its first form, it asserts that intelligence is analogous to the use of force and is therefore justified under the same conditions. The other form casts intelligence as an inherent element of the use of force, as its natural extension. Whether directly or by analogy, the Just Intelligence approach argues that JWT should regulate espionage and serve as its source of legitimacy.").

tional framework, or in other words, to have JWT "regulate espionage and serve as its source of legitimacy."[118]

Two primary challenges have been raised in the literature against relying on JWT as the justification for espionage. The first is concerned with the normative value of open-ended standards in international law. Mark Phytian has noted his skepticism as to the value of rooting ILI in JWT, suggesting that the tests it adopts "involve subjective judgments taken in specific national contexts."[119] This is the classic realist argument against JWT and arguably against any international legal or moral constraint on national political power. As Paskins summarizes:

> Realists often think that the just war tradition is so vague and ambiguous, so indeterminate in practice, that its fine words lend themselves to so many conflicting interpretations as to afford no definite guide to policy. If we are in a mood to debate 'moral realities,' so the skeptical argument goes, then realists will choose interpretations that suit them, interpretations shaped by realism, not by the just war tradition. Whether to employ the just war idiom may be a matter partly of taste, partly of political context, but the deep realist thought is that this language is too vague to be doing any real work.[120]

Although this version of realism—which reasons that morality has no place in international politics—undoubtedly has its adherents,[121] it fails on descriptive grounds. Walzer has correctly shown that "for as long as men and women have talked about war, they have talked about it in terms of right and wrong."[122] Reaching moral judgments on war, as on intelligence—no matter how difficult or problematic such a process might prove to be—is not, and has never been, futile. Even if the rules are likely to be distorted or misinterpreted, even if their application will be shrouded with hypocrisy, even if for "men at war, the rules often don't seem relevant to the extremity of their situation,"[123] engaging in law and ethics talk is as prevalent as it once was, and one can assume this is because this exercise holds

118. *Id.*; *see also* Chomeau & Rudolph, *supra* note 114, at 9 ("Since the major function of intelligence is to provide early and adequate warning of an attack by forces inimical to the nation, one can derive an extension of the 'just war' principles to intelligence.").

119. David Omand & Mark Phythian, *Ethics and Intelligence: A Debate*, 26 INT'L J. INTELLIGENCE & COUNTERINTELLIGENCE 38, 57 (2013).

120. Barrie Paskins, *Realism and the Just War*, 6 J. MIL. ETHICS 117, 119 (2007).

121. HANS J. MORGENTHAU, POLITICS AMONG THE NATIONS: THE STRUGGLE FOR POWER AND PEACE 13 (6th ed. 1985) ("To know that nations are subject to the moral law is one thing, while to pretend to know with certainty what is good and evil in the relations among nations is quite another . . . . [I]t is exactly the concept of interest defined in terms of power that saves us from both that moral excess and that political folly.").

122. MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 3 (4th ed. 2006).

123. *Id.* at 15.

some value. Moralists must never surrender their ultimate sense that war and intelligence, are "a human action, purposive and premeditated, for whose effects someone is responsible."[124]

A second more specific criticism raised against the utilization of JWT in the study of intelligence ethics concerns the differences between war and espionage. The primary claim here is that "war is an exceptional case and intelligence is an enduring state. The Just War conditions govern the transition from peace to war. But the intelligence machine is always active in some form."[125] Bitton argues that JWT serves as a tool for deterrence and punishment because aggressors can be identified. "JWT facilitates identifying the aggressor by imposing a baseline norm of non-violence."[126] Against this backdrop of peace and quiet, argues Bitton, illegitimate attacks are identified immediately "like the first drop of ink falling on a sheet of white paper."[127] Aggression in espionage, however, is unobservable, "like reading white letters on that same sheet of white paper." That is because peacetime intelligence, claims Bitton, "is an ongoing operation."[128]

The counterargument, however, is twofold. First, we should reject the notion that the act of launching an aggressive war is always "identifiable," as Bitton suggests. In the 21st century we have witnessed a move towards the "forever war," the perpetual fight against global terrorism, in which states constantly expand their goals and objectives in conflicts, introducing more complex threats to be addressed and new targets to be neutralized.[129] Surely Bitton does not mean to suggest that JWT has fallen silent in the wake of these new types of conflicts, simply because of their continuous, ever-evolving nature.[130]

Similarly, to argue that espionage is a unitary continuous motion, and therefore "unobservable," is divorced from practice. The fact that intelligence agencies give codenames to espionage operations (e.g. Operation Ivy

124. *Id*.

125. Omand & Phythian, *supra* note 119, at 52.

126. Bitton, *supra* note 25, at 1018-19.

127. *Id*. at 1018.

128. *Id*.

129. *See, e.g.,* Mark Danner, Spiral: Trapped in the Forever War 10 (2016) ("the permanent politics of fear makes the country uniquely vulnerable to the very terrorism it means to combat. A vast counterterror apparatus has arisen that serves to magnify the importance of each terrorist attempt, and politicians and the press do their part to multiply the fear. . . . We have fallen into a self-defeating spiral of reaction and counterterror. Our policies, meant to extirpate our enemies, have strengthened and perpetuated them.").

130. For an example of JWT analysis of the global war on terrorism, see, e.g., Neta C. Crawford, *Just War Theory and the U.S. Counterterror War*, 1 Persp. on Pol. 5, 20-21 (2003) (suggesting that despite the recent "transformation of war" and the challenges that the fight against terrorism has introduced, "just war theory is remarkably resilient, which may be in part due to the codification of some of its core normative precepts into international law, and in part to its hard-headed recognition that violent conflict is a recurrent feature of international life."); But *cf.* Naomi Sussmann, *Can Just War Theory Delegitimate Terrorism?*, 12 Eur. J. Pol. Theory 425, 439 (2013) (suggesting that just war theory was formulated "*in* a different world, *for* a different world. Its categories and distinctions now break down or are no longer relevant.").

Bells, Project ColdFeet, Operation Lunik, Operation Socialist, Operation Optic Nerve) alone would suggest that they are distinguishable from one another. Indeed, we speak of the "intelligence cycle" for a reason. It has a beginning, a middle, and, yes, an end. It is derived directly from the different stages and organization of the intelligence process, from policymaker's demands to agencies' specific directives and guidelines to collectors', analysts', and translators' supply. Each operation requires a mission statement, and each agent and agency turns back to that statement to locate the internal and external rationales behind each of their actions. These statements, directives, guidelines—and ultimately reasoning—could all be the subject of a review which addresses both the justifications for the operation (the *jus ad*) and the operative methods employed in the conduct of the operation (the *jus in*).

In other words, the identification of unjust wars and unjust intelligence is neither to be compared to "a drop of ink falling on a sheet of white paper" nor to "reading white letters on that same white sheet;" it is rather closer to finding Martin Handford's famous Waldo in a sea of other colorful characters. Only the most determined of assessors might actually end up spotting what they were after. Identifying acts of aggressive wars and abusive spying thus requires patience and stamina, not any different than finding Waldo's red and white striped outfit.

My proposed framework thus adopts the structures of JWT. We can reconceive of the regulation of peacetime interstate espionage, the ILI, as a framework of three paradigms: the *Jus Ad Explorationem (JAE)* (the law governing the right to launch espionage operations), the *Jus In Exploratione (JIE)* (the law governing the choice of means and targets in conducting espionage operations), and the *Jus Post Explorationem (JPE)* (the law triggered after the espionage operations have ceased, concerning both ILI's prescription processes and accountability regimes).

Nonetheless, it is important to clarify that "to the student and practitioner of international law in the twenty-first century, the just war ethic is clearly part of moral theology" that only carries a "lingering flavor" over our legal paradigms.[131] JWT must not be confused for the law itself. The post-Charter order relied on the moral, ethical, and theoretical insights of JWT but then adapted and fitted them to meet the institutional structures put forward by the Charter's drafters. The modern-day prohibition on the use of force is more a reflection of treaty norms, customary practices, and general principles than of some theological dogma. As the ICJ noted in the South West Africa case, a court of law "can take account of moral principles only insofar as these are given sufficient expression in legal form."[132] To my

131. Joseph C. Sweeney, *The Just War Ethic in International Law,* 27 FORDHAM INT'L L. J. 1865, 1865 (2004).

132. South West Africa (Eth. v. S. Afr.) (Liber. v. S. Afr.), Judgment, 1966 I.C.J. 6, para. 49 (July 18).

knowledge, there has yet to come an international lawyer who has attempted to pick up the gauntlet by giving such "expression in legal form" to the philosophical accounts of "just intelligence." This paper seeks to offer such a translation so that "just intelligence" too could have actual bearing on the evolution of international law and an impact on the practice of espionage.

To engage in this act of "legal translation," I put particular emphasis throughout my framing on general principles of international law. It is important to clarify that I do not consider these principles as "gap fillers," transforming the adjudicative process into a legislative one by offering supplemental rules where treaty law and customary law are *non linquet*.[133] Rather I see them as 'standard clarifiers,' serving the purpose of defining "the depth and contours of broad or amorphous legal provisions" where international conventions and customs offer little organizational help.[134] Indeed one of the most fundamental functions of general principles is to promote the "organic growth" of international law,[135] especially when it is lagging behind new pressing problems or technological developments.[136]

Within the limits of this paper I focus only on my articulation of the *JAE*, discussing the existence of the right to spy as derived from a large set of international legal sources (Part III), the scope of the right to spy as an Hohfeldian liberty right (Part IV), and the limits of the right to spy resulting from the application of the doctrine of "abuse of rights" (Part V).

II. The Sources of the JUS AD Explorationem

A. *The Right of States to Survival and Collective Self-Determination*

There are different points of view as to the existence and nature of the right of states to survival. On the one end of the spectrum stand thinkers like Secretary of State Dean Acheson who argued during the 1963 ASIL Annual Meeting that "law simply does not deal with such questions of ultimate power—power that comes close to the sources of sovereignty. . . . No law can destroy the state creating the law. The survival of states is not a matter of law."[137] In other words, Acheson believes the survival of state

133. For a criticism of this aggressive usage of general principles as adjudicative "gap fillers," see Johan G. Lammers, *General Principles of Law Recognized by Civilized Nations*, *in* Essays on the Development of the International Legal Order: In Memory of Haro F. van Panhuys 53, 64–69 (Frits Kalshoven, Pieter Jan Kuyper & Johan G. Lammers eds., 1980).

134. Charles T. Kotuby Jr. & Luke A. Sobota, General Principles of law and International Due Process: Principles and Norms Applicable in Transnational Disputes 31–32 (2017).

135. *See* Maarten Bos, *The Recognized Manifestation of International Law*, 20 German Y.B. Int'l L. 9, 42 (1977) (noting that general principles "should be able to provide international law with a most welcome possibility for growth").

136. *See, e.g.*, C. Wilfred Jenks, The Proper Law of International Organizations 259–60 (1962); M. Cherif Bassiouni, *A Functional Approach to "General Principles of International Law,"* 11 Mich. J. Int'l L. 768, 777–78 (1990).

137. *Remarks by the Honorable Dean Acheson*, 57 Am. Soc'y Int'l L. Proc., 13, 14 (1963).

cannot and should not be subjected to mortal rules and regulations, it is rather a sort of fundamental, absolute, and overriding right.[138]

Some, such as Austrian international law professor and diplomat Alfred Verdross, consider the right of states to survive to be a softer liberty right that does not impose obligations on third parties, as opposed to a fundamental right:

> Any State, it is true, is legally free to ensure its preservation, as doing so does not violate the rules of the Law of Nations. This freedom, however, does not correspond to a duty placed on other States. They are under no obligation to tolerate anything that is necessary for the preservation of other States.[139]

Finally, on the far end of the spectrum are those that argue that the right of states for survival, to the extent that it still exists as a matter custom, has been overtaken by the Charter right of self-defense and its parallel doctrine of necessity. Lauterpacht noted as early as 1955 that it is becoming "more and more recognized" that "violations of other States in the interest of self-preservation are excused in cases of *necessity* only."[140] He then proceeded to give an example of a state that becomes "informed" that a group of armed men are organizing in a neighboring territory. To the extent that "the danger can be removed through an appeal to the authorities of the neighboring country," no right of self-preservation will stand. But if "such an appeal is fruitless or not possible, or if there is danger in delay, a case of necessity arises," and a right to take self-defensive measures in the name of preservation is authorized.[141]

Scholars who adopt Lauterpacht's approach cite as proof of their position the fact that few modern international instruments still recognize an absolute right for self-preservation. For example, the ILC in drafting the Decla-

---

138. There have been quite a number of scholars who have recognized the right of self-preservation as being incorporated into the broader doctrine of "fundamental rights of States." Kohen does a terrific job of listing these scholars, beginning with Hobbes and proceeding to 19th and 20th century natural law thinkers. *See* Marcelo G. Kohen, *The Notion of 'State Survival' in International Law*, *in* INTERNATIONAL LAW, THE INTERNATIONAL COURT OF JUSTICE AND NUCLEAR WEAPONS 293, 299–303 (Laurence Boisson de Chazournes & Phillipe Sands eds., 1999); *see also* LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE 207 (Hersch Lauterpacht ed., 8th ed. 1955). Nonetheless, the idea that the right of self-preservation is a "fundamental right" is highly contested. Those who oppose it argue that if we consider self-preservation "an absolute and overriding right" it would result in international law becoming "optional, and its observance would depend on a self-denying ordinance, revocable at will by each State, not to invoke this formidable superright." *See* Georg Schwarzenberger, *The Fundamental Principles of International Law*, 87 RECUEIL DES COURS DE L'ACADEMIE DE DROIT INTERNATIONAL 191, 195 (1955); *see also* JAMES LESLIE BRIERLY, THE LAW OF NATIONS 404 (6th ed. 1963) ("Such a doctrine would destroy the imperative character of any system of law in which it applied, for it makes all obligation to obey the law merely conditional.").

139. Alfred Verdross, *Règles générales du droit international de la paix*, 30 RECUEIL DES COURS DE L'ACADEMIE DE DROIT INTERNATIONAL 271, 415 (1929) (translated from the original French). I address the notion of liberty rights later in this paper.

140. OPPENHEIM, *supra* note 138, at 298.

141. *Id.*

ration on the Rights and Duties of States specifically excluded preliminary language proposed by Panama that introduced as Article 1 the idea that "every State has the right to exist and to preserve its existence."[142]

This brings us to the wording of the ICJ Nuclear Weapons Advisory Opinion, where the Court observed that it "cannot lose sight of the fundamental right of every State to survival, and thus its right to resort to self-defence, in accordance with Article 51 of the Charter when its survival is at stake."[143] The ICJ left matters sufficiently ambiguous. Whereas "fundamentalists" will find solace in the top half of the Court's reasoning, Charter defenders will find their comfort in the bottom half of that same sentence.

To this already robust body of scholarly interpretations I simply want to add another possible way of conceiving of the right of self-preservation—that is as an extension of the right of collective self-determination. Modern international law recognizes the right of a people to decide their own destiny in the international order by freely determining their political status.[144] Dinstein provides the example of the right to fend off existential threats to the polity as an extension of collective self-determination rights. He notes that "if the local people is truly at liberty to determine its political status, a post-*debellatio* annexation by the victorious State must clearly be precluded."[145] Surely, however, Dinstein's logic can be expanded beyond a simple limit on post-occupation annexation. Indeed, a broader right can be asserted, in the name of collective self-determination, for peoples to fight against any attempts at the obliteration of their political manifestation. Philip Marshall Brown alluded to this when he argued that of the rights endowed with states, "the solid rock of international law," is the right of states to exist, which he defined as a "mutual guarantee between nations, great and small, of their legal right to a separate existence in order to realize their own aspirations and destinies."[146]

Examining this entire body of literature, one key observation emerges. Regardless of where one identifies in terms of the spectrum of positions as to the existence, nature, and scope of the right to survival, all of them necessitate that states enjoy a corollary and derivative right to engage in peacetime intelligence gathering. You may be an Acheson and seek to exude your unconstrained power over the threat of Soviet ballistic missiles in Cuba, or a Lauterpacht who is only attempting to remain "informed" as to the imme-

142. *See* Kohen, *supra* note 138, at 295–96. For a complete review of the relevant international instruments which predominantly exclude language relevant to self-preservation, *see id.* at 295–98.

143. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 263 (July 8).

144. *See, e.g.*, G.A. Res. 2625 (XXV) (Oct. 24, 1970) (establishing the principle of equal rights and self-determination of peoples); Case Concerning East Timor (Port. v. Austl.), Judgment, 1995 I.C.J. 90, 102 (June 30) (concluding that the assertion that the right of peoples to self-determination has an *erga omnes* character "is irreproachable").

145. Yoram Dinstein, War, Aggression and Self-Defence 182 (5th ed. 2011).

146. Philip Marshall Brown, *The Rights of States under International Law*, 26 Yale L. J. 85, 87 (1916).

diate threat posed by an armed group in a neighboring territory, or a Dinstein who in the name of collective self-determination hopes to protect the polity against a pending and unlawful occupation and annexation, or the ICJ authorizing the threat or use of nuclear weapons in the extreme circumstance where "the very survival of a State would be at stake." Regardless of who you are and what position you take, you must recognize that foundational to your conceptualization of the "right to survive" is the associated right to develop at-all-times as complete and as accurate a picture of the impending threats to your nation and its people. For it is this derivative right to spy that operationalizes the right to survive.

B. The Inherent Right of Individual or Collective Self Defense

Dating back to the Caroline incident of 1837, the right of states to engage in pre-emptive self-defense in order to avert an attack that is "instant, overwhelming, leaving no choice of means, and moment of deliberation"[147] has been extensively documented and analyzed.[148] Even textualists who still maintain, based on the wording of the Charter, that a right of self-defense applies only "if an armed attack occurs," cannot ignore the diverse and robust subsequent practice by states.[149] The 2004 High-level Panel on Threats, Challenges, and Change established by the U.N. Secretary-General thus recognized that "a threatened State, according to long established international law, can take military action as long as the threatened attack is imminent, no other means would deflect it, and the action is proportionate."[150]

Regardless of what interpretation of "imminence" one adopts, from a classically restrictive "Pearl Harbor"-type position to a highly permissive "Bush doctrine"-styled approach,[151] the right of self-defense will embrace a state's derivative right to engage in peacetime intelligence gathering. If a state is entitled to retaliate against imminent threats, by definition it must be allowed to engage in peacetime espionage to gather the information nec-

147. *See British-American Diplomacy: The Caroline Case*, THE AVALON PROJECT AT YALE LAW SCHOOL (2008), https://perma.cc/ST6Z-ASBQ.

148. For a summary of the literature, see Christopher Greenwood, *Self-Defence*, MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. (Apr. 2011). For a more recent review of the literature, see Monica Hakimi, *North Korea and the Law on Anticipatory Self-Defense*, EJIL: TALK! (Mar. 28, 2017), https://perma.cc/J695-SXED.

149. W. Michael Reisman & Andrea Armstrong, *The Past and Future of the Claim of Preemptive Self-Defense*, 100 AM. J. INT'L L. 525, 526 (2006) (noting that anticipatory self-defense was not, in their view, "in the contemplation of drafters of the Charter, though claimed by many to have been grafted thereon by subsequent practice," followed by a showing of such practice through case studies).

150. U.N. Secretary-General, *High-Level Panel Report on Threats, Challenges, and Change, A More Secure World: Our Shared Responsibility*, ¶ 188, U.N. Doc. A/59/565 (Dec. 2, 2004), https://perma.cc/9HP3-DSRC.

151. For more moderate interpretations, see Daniel Bethlehem, *Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM. J. INT'L L. 769 (2012); Jeremy Wright, *The Modern Law of Self-Defence*, EJIL: TALK! (Jan. 11, 2017), https://perma.cc/ML53-JPZG.

essary to assess whether any threats are imminent (regardless of whatever level of imminence is deemed sufficient to justify military action).[152]

This derivative right also holds even were we to adopt the formalistic and, in my view, anachronistic approach that only Article 51 governs the use of force (and therefore that a state may only react to an imminent threat by seeking Security Council authorization to use force). Because the United Nations does not have its own intelligence capacities, the Security Council must rely on member states' intelligence in order to fulfill its mandate of maintaining peace and security. A delegation must engage in peacetime espionage to be able to prove to the Security Council that a threat is mounting, so as to convince its members to vote in favor of a Chapter VII resolution.

The case study of Israel's espionage operations against Iran's nuclear program offers a good example of the interrelations between the right of self-defense and the derivative right to spy. Recall the image of the Prime Minister of Israel, Benjamin Netanyahu, in his speech at the United Nations General Assembly in September 2012, drawing a red line at 90% enrichment over a cartoon of an Iranian uranium nuclear bomb.[153] At the time different positions were suggested as to whether Israel had the legal right to strike Iran. Alan Dershowitz claimed that given that Iran directed the 1992 attack on Israel's embassy in Argentina, and was supplying weapons to its proxies in Syria, Lebanon, and Palestine, who had used those weapons to attack Israel in the past, an armed attack had already occurred. The "law of war does not require an immediate military response to an armed attack," he claimed, adding that, "[t]he nation attacked can postpone its counterattack without waiving its right."[154]

On the other side, Kevin Jon Heller claimed that it is unlikely that Iranian links to Hezbollah and Hamas are sufficiently close to satisfy the legal standard of "overall and effective control." Therefore, he claimed, it would be impossible to make their actions imputable to Iran and thereby justify an action in self-defense. He added further that, "even if they did, just because there may be an armed attack on Israel by Hamas doesn't mean you can take out a country's nuclear programme. There has to be some kind of necessity and proportionality between the armed attack and the response."[155]

---

152. *See* Baker, *supra* note 49, at 1095–96 ("[I]n order to ensure that the right to self-defense retains substantive meaning, international law must permit states to predict armed attack. Therefore, for states to enjoy the positively-codified right to self-defense, they should retain the right to acquire information that would indicate whether they face imminent armed attack.").

153. *See, e.g.*, Harriet Sherwood, *Netanyahu's Bomb Diagram Succeeds –But Not in the Way the PM Wanted*, The Guardian (Sept. 27, 2012), https://perma.cc/PV9L-YXKL.

154. Alan Dershowitz, *Israel Has the Right to Attack Iran's Nuclear Reactors Now*, Huffington Post (Mar. 16, 2011, 6:07 PM), https://perma.cc/REA9-XABS.

155. Chris McGreal, *Iran's Nuclear Programme: Legal Debate Stirs over Basis for US or Israeli Attack*, The Guardian (Apr. 12, 2012), https://perma.cc/EW4W-L7C4.

Former legal advisor to the Israeli Ministry of Foreign Affairs, Professor Robbie Sabel, agreed with Heller, citing to existing ICJ jurisprudence and concluding that "supplying arms and training to an enemy of a State does not, by itself, constitute an armed attack against that State."[156] Nonetheless, focusing on anticipatory self-defence, Sabel noted that it would be necessary for Israel to prove that Iran's development of nuclear weapons was "a dire threat" and that "there was no other way to prevent such development."[157]

Notice how fundamental a reliable and discernible stream of intelligence is in the context of the prohibition on the use of force. To prove Dershowitz's point that Iran was behind the 1992 embassy attack, or Keller's point that Iran's support of Hezbollah in Lebanon does not rise to the level of either overall or effective control, or to meet Sabel's test of a "dire threat" leaving no alternative or moment for delay—one needs evidence. One also needs evidence to prepare for the attack and make sure it meets the necessity and proportionality requirements set under *JAB*. What's more, to build an effective international campaign behind such strikes, verifiable evidence that is capable of being shared across agencies is vital prior to the launch of the attack.

Fast forward to 2018. Netanyahu ran yet another performance of red-meat rhetoric and pop comedy, this time in the form of a staged unmasking of 55,000 printed pages and 183 compact discs stolen from Iran's secret nuclear archives.[158] While the Iranians scoffed at Netanyahu's theatrics, calling it a "prearranged show",[159] not even they challenged the legality of Israel's Mossad agents operating deep in Iran as part of the operation. More interestingly, the P5+1 and the International Atomic Energy Agency welcomed the opportunity to review the trove of documents provided by the Israeli intelligence.[160] These actors were not worried about being found complicit in a violation of international law simply by accepting the stolen documents; quite the opposite, they accepted them knowing very well that they were

156. Robbie Sabel, *The Legality of an Attack Against Iranian Nuclear Facilities*, INSS INSIGHT (June 15, 2012), https://perma.cc/2S4D-P7P5.

157. *Id*.

158. David M. Halbfinger, David E. Sanger & Ronen Bergman, *Israel Says Secret Files Detail Iran's Nuclear Subterfuge*, N.Y. TIMES (Apr. 30, 2018), https://perma.cc/ND7C-UWCF.

159. *Id*. (citing Iran's deputy foreign minister, Abbas Araghchi. Araghchi went on to suggest that Netanyahu's remarks were "a very childish and even a ridiculous play" coordinated with the Trump administration to destroy the Joint Comprehensive Plan of Action between the P5+1 and Iran around its nuclear program); *see also* Oren Liebermann, *What did Netanyahu Reveal About Iran's Nuclear Program? Nothing New, Experts Say*, CNN (May 3, 2018, 5:21 AM), https://perma.cc/2BWN-N238 (citing to other skeptics who challenged whether the stolen materials revealed any actual new intelligence that was not previously known).

160. *See* Ron Ben-Yishai, *European Delegations to Review Iranian Nuclear Archive*, YNET NEWS (May 1, 2018, 3:45 PM), https://perma.cc/359R-9HAJ.

produced as part of a territorial spying operation to advance non-proliferation goals.[161]

Our international legal order places the burden of proof,[162] and therefore the burden of intelligence collection, analysis, and verification, on the party alleging the fact (*e.g.* the threat), so States seeking to use their force in accordance with the Charter and customary law are encouraged to establish effective peacetime foreign intelligence apparatuses. In the context of the above case study and in line with this legal scheme, Israel was almost invited, if not required, to spy on Iran. Iran, in turn, is equally motivated to spy back on Israel.[163] The broader international community benefits from such reciprocal spying which increases the transparency around the strategic plans of both the rivalling nations. While we can debate the minutiae of the legal regime of Articles 2(4) and 51—who has the right to use force, against whom, and under what circumstances—there can be no debate that the right of sovereigns to spy, in the name of protecting their national security, is what activates those Charter provisions. Without it those Articles will become a dead letter.

C. *Collective Monitoring Obligations Under UN and Treaty Law*

While large international organizations, like the United Nations, have various means for directly collecting information (*e.g.* field studies, interviews, forensic analysis, open source analysis of images and videos, soliciting assistance from civil society, etc.),[164] certain determinations—perhaps the ones of most significance, such as those made in the context of establishing state responsibility for internationally wrongful acts or individual criminal liability for international crimes—could only be ascertained by consulting raw national security intelligence. In this regard it is important to recall the

161. *See* Joby Warrick, *Papers Stolen in a Daring Israeli Raid on Tehran Archive Reveal the Extent of Iran's Past Weapons Research,* WASH. POST (July 15, 2018), https://perma.cc/688E-FTDA (noting that the half a ton of documents was shared with U.S. and European intelligence agencies as well as with the IAEA).

162. With respect to matters of fact, the ICJ has adopted the principle of *onus probandi incumbit actiori* ("the burden of proof is on the claimant"). As the court has held on multiple occasions, the party alleging the fact bears the burden of proving it. *See, e.g.*, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croat. v. Serb.), Judgment, 2015 I.C.J. Rep. 3, ¶ 172 (Feb. 3); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1984 I.C.J. Rep. 392, ¶ 101 (Nov. 26). As for the standard of proof the ICJ has recognized that "claims against a State involving charges of exceptional gravity [e.g. use of force] must be proved by evidence that is fully conclusive." Croat. v. Serb., 2015 I.C.J. Rep at ¶ 178 (citing Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 17 (Apr. 9)). In *Corfu* the court noted that if evidence is in the "exclusive territorial control" of the respondent, the claimant "should be allowed a more liberal recourse to inferences of fact and circumstantial evidence." U.K. v. Alb., 1949 I.C.J. Rep. at 18.

163. *See, e.g.*, Dov Lieber, *Former Israeli Minister Admits to Spying for Iran*, WALL ST. J. (Jan. 9, 2019), https://perma.cc/8REW-BASS (reporting on a case of Iranian spying on Israel).

164. For a complete analysis of the sources of information available at the United Nations, see Ekpe, *supra* note 20 and accompanying text.

words of former Secretary General Butros Butros-Ghali who clarified in 1993 that the United Nations simply had no intelligence to call its own.[165]

The World Health Organization's capacity to investigate large-scale epidemics is dependent on cooperation and assistance from national health services,[166] and as we have already witnessed, the same is true for the needs of the IAEA in monitoring compliance with the Non-Proliferation Treaty.[167] International institutions, in the fulfillment of their varied mandates, continue to rely significantly on intelligence produced by their member states. From disarmament obligations[168] to counter-terrorism efforts,[169] and from running effective sanctions regimes[170] to providing assistance in disaster relief and humanitarian crises,[171] there isn't an area of work within the broader umbrella of "collective security" that doesn't require such information.

The international community, aware of this political reality, has established various treaty regimes that demand the collection and dissemination of information. A few early examples originated during the Cold War. Consider SALT I,[172] and the Anti-Balistic Missiles (ABM) Systems Treaty,[173] both signed in 1972 between the United States and the Soviet Union. Those treaties laid down a framework for reciprocal spying ("national technical means of verification" if to embrace the euphemism) between two super powers. "In a manner consistent with generally recognized principles of in-

165. Simon Chesterman, *Shared Secrets: Intelligence and Collective Security*, *in* 10 Lowy Institute Papers 7 (2006) (citing Georgie Anne Geyer, *Limited Tools for Complex Tasks*, Dallas Morning News (Sept. 28, 1993)).

166. *See generally*, World Health Org., WHO Report on Global Surveillance of Epidemic-prone Infectious Diseases, U.N. Doc. WHO/CDS/CSR/ISR/2000.1 (2000).

167. *See* OTA Report, *supra* note 20 and accompanying text; *supra* notes 158–160 and accompanying text.

168. *See, e.g.*, Allison Carnegie & Austin Carson, *The Disclosure Dilemma: Nuclear Intelligence and International Organizations*, 63 Am. J. Pol. Sci. 269, 269 (2019) ("[T]o punish states effectively, the international community must first learn about [breaches of disarmament obligations], yet this is difficult since states hide their violations and international organizations often lack the authority and resources to intrusively monitor compliance. While many states possess extensive intelligence capabilities that allow them to detect violations of treaties and norms, they often refuse to fill these informational gaps.").

169. *See, e.g.*, U.N. Sec. Council Counter-Terrorism Committee Executive Directorate (CTED), Terrorism Financing, (2018) https://perma.cc/M8VD-TSKK (suggesting that in order to tackle terrorism financing effectively it is essential to rely on member states exchanging of operational information and intelligence).

170. *See, e.g.*, Counter-terrorist sanctions regimes Legal framework and challenges at UN and EU levels, Briefing, European Parliament, 2 (Oct., 2016), https://perma.cc/JX4Q-BCT8 (suggesting that listings and designations for sanctions are dependent on classified intelligence and confidential information provided by member states).

171. *See, e.g.*, Mirielle M. Petitjean, *Intelligence Support to Disaster Relief and Humanitarian Assistance*, 19 Intelligencer: J. U.S. Intelligence Stud. 57 (2013) (canvassing examples for uses of IMINT, SIGINT, and OSINT in disaster relief operations).

172. Interim Agreement Between the United States of America and the Union of Soviet Socialist Republics on Certain Measures with Respect to the Limitation of Strategic Offensive Arms, U.S.-U.S.S.R., art. V, May 26, 1972, 23 U.S.T. 3462 ["SALT I"].

173. Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, U.S.-U.S.S.R., art. XII, May 26, 1972, 23 U.S.T. 3435 ["ABM Treaty"].

ternational law," each power was allowed to use such technical means of verification and the other power was prohibited from interfering with those measures.[174]

The Treaty on Open Skies,[175] with its 34 ratifiers, offers a contemporary example despite some recent enforcement issues.[176] This treaty does exactly what SALT I and the ABM Treaty did, just on a global scale; it establishes an affirmative right to spy in the territorial airspace of members while setting strong limitations on their ability to interfere with that right. I will revisit this point again when introducing the distinction between claim rights and liberty rights in the following Section.

One can think of other treaties, such as certain counter-proliferation and counter-terrorism treaties which establish intelligence collection and sharing obligations,[177] or treaties for environmental protection and for the preservation of Antarctica, which similarly introduce certain monitoring and observations rights and obligations on member states.[178] A particularly powerful example might come in the form of the Biological and Toxin Weapons Convention, which expressly depends on parties to bring complaints before the Security Council showing any breach by another party of the obligations enshrined therein. Each complaint must include "all possible evidence confirming its validity."[179]

But the buck does not just stop at treaty frameworks. The Security Council too has acknowledged the role that member states play in its ability to fulfill its mandate. Most recently it adopted Resolution 2396, a Chapter VII resolution concerning threats to international peace and security caused by terrorist acts.[180] In that Resolution the Council not only called on member states to "intensify and accelerate" their peacetime intelligence collection

174. *Id.*

175. Treaty on Open Skies, Mar. 24, 1992, S. TREATY DOC. 102.37. The Treaty on Open Skies establishes a regime of unarmed aerial observation flights over the territories of its signatories. The Treaty is designed to enhance mutual understanding and confidence by giving all participants, regardless of size, a direct role in gathering information through aerial imaging on military forces and activities of concern to them.

176. *See, e.g.*, Steve Liewer, *Rollback of Open Skies Treaty Comes as Relationship Between Russia, U.S. Gets Chillier*, OMAHA WORLD HERALD (Jan. 13, 2018), https://perma.cc/R7RU-SPVU.

177. *See, e.g.*, International Convention for the Suppression of the Financing of Terrorism, 2178 U.N.T.S. 228 (Dec. 9, 1999) (establishing certain obligations for the cooperation between states in the prevention of terrorist financing, including through the collection and exchange of information); Model Protocol Additional to the Agreement(s) between State(s) and the International Atomic Energy Agency for the Application of Safeguards, U.N. DOC. INFCIRC/540 (Sept. 1, 1997) (requiring states to provide the IAEA with information about a variety of nuclear-related activities that supplements the information already provided by the states pursuant to their comprehensive safeguards agreements).

178. *See, e.g.*, Convention on Biological Diversity, 1760 U.N.T.S. 69, art. 17 (June 5, 1992) (requiring member States to facilitate the exchange of information relevant to the conservation and sustainable use of biological diversity); The Antarctic Treaty, 402 U.N.T.S. 71, arts. III(1) and VII(6) (June 23, 1961) (setting obligations for the sharing of information between members).

179. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, 1015 U.N.T.S. 163, art. VI (Apr. 10, 1972).

180. S.C. Res. 2396, ¶ 5 (Dec. 21, 2017).

efforts, but went on to suggest exactly what measures they should employ.[181] The Council decided that member states "shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data."[182] Other measures ordered by the Council were the collection of passenger information,[183] the development and implementation of watch lists and databases on suspected terrorists,[184] and increased cooperation with technology companies in gathering a myriad of digital records.[185]

A final example comes in the form of the guidelines that control the workings of the 1267 Committee (the ISIL (Da'esh) and al Qaida Sanctions Committee of the Security Council). Paragraph 6(h) of the most recent guidelines cover the obligations of listing states. The Committee relies on statements from these states which should cover a demonstration that the individual or entity meet the criteria for listing, including details of any connections with currently listed individuals or entities, information about relevant activities, and information about relevant court cases and proceedings brought against the subject. The guidelines directly mention "intelligence" as one of the sources to be relied on in compiling the application (alongside information from law enforcement, judicial proceedings, and open source data).[186]

It is this increased level of engagement with intelligence sources necessary for the functioning of collective security mechanisms in the 21st century, that brought Professor Chesterman to advocate for reforms within international agencies in the area of their assessment and verification capabilities.[187] After all, the intelligence shared with U.N. agencies may not always be accurate or truthful. Indeed, "interested policy-makers quickly learn that intelligence can be used the way a drunk uses a lamp post – for support rather than illumination."[188] Increasing international organizations' capacity to properly examine the intelligence they receive, if not providing them their own limited intelligence gathering capabilities, thus seems desirable.

D. International Human Rights Law

The international community has taken significant steps to enhance privacy protections since the signing of the ICCPR in 1966 and the Human

181. *Id.*
182. *Id.*, at ¶ 15.
183. *Id.*, at ¶¶ 11–12.
184. *Id.*, at ¶ 13.
185. *Id.*, at ¶ 21.
186. S.C. Comm. Pursuant to Res. 1267 (1999), 1989 (2011), and 2353 (2015) concerning ISIL (Da'esh), Al-Qaida, and associated individuals, groups undertakings, and entities, Guidelines of the Committee for the Conduct of its Work, ¶ 6(h) (last amended Dec. 23, 2016), https://perma.cc/RAV7-B5V4.
187. *See* Chesterman, *supra* note 165, at viii–ix.
188. Thomas Lowe Hughes, The fate of facts in a world of men: Foreign policy and intelligence-making, 22 (The Foreign Policy Ass'n ed., 1976).

Rights Committee's adoption of General Comment No. 16 on the right to privacy in 1988. These accomplishments include, since 1999, a significant body of work on human rights and surveillance practices by the U.N. High Commissioner for Human Rights and the U.N. Special Rapporteurs on Freedom of Expression and Counter-Terrorism.[189] The repeated adoption of both U.N. General Assembly Resolutions and U.N. Human Rights Council Resolutions, by consensus, on the right to privacy in the digital age also marks a significant step forward.[190] The 2015 creation of the position of U.N. Special Rapporteur on the Right to Privacy is itself a reaffirmation of the international privacy agenda, and his reports to the Council further signify the importance of his new role as an international intelligence watchdog.[191] The Human Rights Committee has too begun to routinely address surveillance legislation and practices in its Concluding Observations to States, beginning in 2014.[192] On the regional level, the ECtHR, the Court of Justice of the European Union, and the Inter-American Commission and

189. *See, e.g.*, Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009); Rep. of the Special Rapporteur on the Promotion and Prot. of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/17/27 (May 16, 2011); Rep. of the Special Rapporteur on the Promotion and Prot. of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/20/17 (June 4, 2012); Rep. of the Special Rapporteur on the Promotion and Prot. of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013); Rep. of the Office of the U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (June 30, 2014); Rep. of the Special Rapporteur on the Promotion and Prot. of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (Sept. 23, 2014); Rep. of the Special Rapporteur on the Promotion and Prot. of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/29/32 (May 22, 2015); Rep. of the Special Rapporteur on the Promotion and Prot. of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/32/38 (May 11, 2016); Report of the Special Rapporteur on the Promotion and Prot. of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/HRC/34/61 (Feb. 21, 2017).

190. G.A. Res. 69/166, U.N. Doc. A/RES/69/166 (Dec. 18, 2014); Human Rights Council Res. 28/L.27, U.N. Doc. A/HRC/28/L.27 (Mar. 24, 2015); G.A. Res. 71/199, U.N. Doc. A/HRC/71/199 (Dec. 19, 2016); Human Rights Council Res. 34/L.7/Rev.1, U.N. Doc. A/HRC/34/L.7/Rev.1 (Mar. 22, 2017). *See also* Human Rights Council Res. 33/L.6, U.N. Doc. A/HRC/33/L.6 (Sept. 26, 2016).

191. *See, e.g.*, Rep. of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/HRC/31/64 (Mar. 8, 2016); Rep. of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/71368 (Aug. 30, 2016). Kinfe Michael Yilma, *The United Nation's Evolving Privacy Discourse and Corporate Human Rights Obligations*, 23(4) ASIL INSIGHTS (May 17, 2019), https://perma.cc/CM8Q-BKD5 (describing the installation of a new mandate for the special rapporteur as reflecting an emerging and novel discourse around privacy at the United Nations); for a critique of the work of the Special Rapporteur to date, see Marc Rotenberg, *Urgent Mandate, Unhurried Response: An Evaluation of the UN Special Rapporteur on the Right to Privacy*, 3 EUR. DATA PROT. L. REV. 47 (2017).

192. For further reading see Yuval Shany, *On-Line Surveillance in the Case-law of the UN Human Rights Committee*, HEBREW UNIV. CYBER SEC. RESEARCH CTR. (July 2017), https://perma.cc/BW4H-K55R (noting that "whereas questions relating to [surveillance] were raised with respect to two states between 2007-2014, since 2014 they have been addressed with respect to 15 different states (representing more than 25% of the states reviewed by the Committee during this period). This sharp rise is suggestive both of the growing resort to on-line surveillance powers by governments due to advances in available technology, and of growing awareness to their human rights implications by the Committee.").

Court on Human Rights have all developed authoritative jurisprudence on surveillance and privacy.[193]

At the same time, however, it would be wrong to assume that international human rights law is focused only on the constraints. The High Commissioner for Human Rights had acknowledged that the need to collect intelligence is a "legitimate aim" for governments to pursue.[194] Article 8 of the European Convention of Human Rights further establishes that the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of public health or morals, and the protection of the rights and freedoms of others, can all be considered grounds for interferences with the right to privacy.[195] In the leading judgment on this issue from 1978, *Klass and Others v. Germany*, the ECtHR acknowledged the need of states to "undertake . . . secret surveillance" and its necessity "in a democratic society."[196] Similarly, in *Leander v. Sweden* the ECtHR observed that national authorities enjoy "a margin of appreciation" in collecting and storing in "registers not accessible to the public information on persons" for the purpose of protecting national security.[197]

While both of *Klass* and *Leander* concerned domestic targeted surveillance operations, the ECtHR has also applied this rationale in foreign mass surveillance cases. Most recently in *Centrum För Rättvisa v. Sweden* the ECtHR noted that "bulk interception regimes did not per se fall outside" intelligence agencies' margin of appreciation.[198] They argued further that in view of advancements of communications technology, the rise of global terrorism and serious crime, and the "unpredictability of the routes via which electronic communications are transmitted," the decision to operate a bulk interception regime was justified.[199]

International Human Rights law further recognizes the right of states to take certain extreme measures, which derogate from the rights enshrined in

193. For a complete study including proper citation to all of these recent developments, see PRIVACY INTERNATIONAL, GUIDE TO INTERNATIONAL LAW AND SURVEILLANCE (Feb. 2019), https://perma.cc/VU84-4DEY.

194. Rep. of the Office of the U.N. High Comm'r for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37, ¶ 24 (June 30, 2014).

195. European Convention for the Protection of Human Rights and Fundamental Freedoms, 213 U.N.T.S. 221, art. 8 (Nov. 4, 1950).

196. *Klass & Others v. Germany*, App. No. 5029/71, Eur. Ct. H.R., ¶ 48 (Sept. 6, 1978).

197. *Leander v. Sweden*, App. No. 9248/81, Eur. Ct. H.R., ¶¶ 58–59 (Mar. 26, 1987).

198. *Centrum Fo?r Rättvisa v. Sweden*, ECtHR, App. No. 35252/08, Eur. Ct. H.R., ¶ 112 (June 19, 2018). *See also Big Brother Watch and Others v. the United Kingdom*, ECtHR, App. No. 58170/13, Judgment, ¶ 317 (Sep. 13, 2018) ("[R]equiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would be inconsistent with the Court's acknowledgment that the operation of a bulk interception regime in principle falls within a State's margin of appreciation. Bulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible. Similarly, the requirement of "subsequent notification" assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime.").

199. *Id.*

the corpus, in times of emergency threatening the life of the nation (ICCPR, Art. 4, ECHR, Art. 15).[200] In those exceptional situations[201] international law anticipates that states will take preventative and restorative steps to protect their polity (note that both the right to privacy and the right to freedom of expression, are in fact derogable rights). There is nothing in the Conventions that expressly prohibits these derogations from taking place in an extraterritorial fashion (*e.g.* in a foreign surveillance context). In conclusion, international human rights law recognizes the right of states to spy when necessary and only in a proportionate manner. In fact, in recognizing that the collection of intelligence is necessary for the protection of rights, such as the right to life, and for preserving national security and public order, human rights law might be said to introduce a due-diligence duty on the state to spy.

E. International Humanitarian Law

Article 57(2)(a)(i)-(ii) of the first Additional Protocol (API) to the Geneva Conventions is reflective of customary international law in both international and non-international armed conflicts.[202] The Article establishes that those who plan attacks "must *do everything feasible to verify"* that the objectives to be attacked are neither civilians nor civilian objects, nor subject to special protection, and "must take *all feasible precautions* in the choice of means and methods of attack" with a view to avoiding and minimizing incidental and collateral damage.[203] Pictet's Commentary to Article 57 clarifies further that by "feasibility" the drafters indeed thought about intelligence analysis and verification as one primary measure to be taken.[204] This was further expanded on in the report of the ICTY's Expert Committee to investigate the 1999 NATO Bombing. The Committee noted that "a military commander must set up *an effective intelligence gathering system to collect and evaluate* information concerning potential targets. The commander must also direct his forces *to use available technical means to properly identify* targets during operations."[205]

200. *See also* American Convention on Human Rights, 144 U.N.T.S. 123, art. 27 (Nov. 21, 1969) (providing for the suspension of guarantees "[i]n times of war, public danger, or other emergency that threatens the independence or security of a State Party").

201. *Lawless v. Ireland*, ECtHR, App. No. 332/57, Eur. Ct. H.R., ¶ 28 (July 1, 1961).

202. Protocol I Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflicts, 1125 U.N.T.S 3, arts. 57(2)(a)(i)–(ii) (1977) [hereinafter API]; ICRC, Customary International Humanitarian Law, Rule 15 (vol. I, 2005).

203. *Id.*

204. International Committee of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, 681 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

205. Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, ¶ 50 (June 13, 2000), https://perma.cc/LGZ9-DQGD [hereinafter "ICTY's Expert Report"].

Needless to say, the only relevant time to begin establishing such an "effective intelligence gathering system" is in preparation for war and not after the armed conflict had already begun. Indeed, under IHL militaries are expected to be able to engage in lawful targeting that is both discriminate and proportionate from the first frame of the belligerent theater of conflict onwards.

Consider, the specific issue of aerial operations. The targets of such attacks range from a warehouse to a rocket launcher, from the vehicle or home of a particular insurgent, to a secret meeting of top military leaders or terrorists in a distant hideout. It might also include potential dual-use targets, such as power grids, broadcasting stations, oil refineries, airports, marine ports, highways, and bridges. Intelligence information collected for the purposes of targeting these types of objects will usually cover six unique features: (1) The GPS coordinates of the target and its geophysical location; (2) Continuous aerial footage of the target and its surroundings, establishing "patterns of behavior"; (3) Classification of the various functions the target plays in the machinery of the adversary's war efforts; (4) The existence of "sensitive sites" surrounding the target;[206] (5) The military advantage to be gained from attacking the target; and (6) The expected incidental harm to civilians and civilians object from such an attack.[207]

Much of this intelligence will be collected and collated in peacetime.[208] This information will be stored in military archives in order to ensure operational readiness and in preparation for a prospective war. In Israeli military jargon, for example, these archives are often referred to as "target banks," and they contain "targeting cards" for each individual target.[209] To guarantee that the information remains accurate, these cards are routinely inspected, reviewed, and updated on the basis of new intelligence.[210]

What is reflected in the above analysis is the idea that the principal pillars of IHL—distinction, necessity, proportionality, humanity, and precautions in attack—heavily depend on a supporting beam, that of an adequate, sufficient, and reliable stream of intelligence information that is collected

206. These would be objects that receive special protections under IHL. *See, e.g.*, Strobe Talbot, Letter of Submittal, Message from the President Transmitting the 1954 Hague Cultural Property Convention (May 12, 1998), https://perma.cc/UQS2-H42S.

207. As the principle of proportionality dictates, any expected civilian harms must not be excessive in relation to the military advantage anticipated. API, *supra* note 202, at art. 51(5)(b).

208. *See, e.g.*, H.B. Keightley, Air Powers Studies Centre, Intelligence Support for Air Operations 12–13, 22 (1996).

209. On the use of "target cards," see The 2014 Gaza Conflict (7 July – 26 August 2014): Factual and Legal Aspects, Israeli Ministry of Foreign Affairs, ¶ 246 (May 2015), https://perma.cc/PL6S-XZD8.

210. *Id.*

and maintained in peacetime. The wartime "license to kill" thus requires a derivative – and quite unusual[211] – peacetime extension.

III. The Nature of the JUS AD Explorationem

One of the most common challenges raised by scholars as to why customary law cannot materialize in the context of espionage, concerns the fact that the "vast majority of States both decry it and practice it."[212] As explained by Buchan, when challenged about their espionage activities, states "overwhelmingly refuse to admit responsibility for this conduct, let alone attempt to justify it as permissible under international law."[213]

The common claim is thus that state practice and *opinio juris* are running in opposite directions.[214] Yes, we all spy, but we all refuse to acknowledge it, further criminalizing spying domestically and pushing against the practice when done against us. There is, therefore, no sense of a legal right associated with the practice, but rather a sense of a legal wrong. This, however, is a false characterization and the result of a misunderstanding as to the nature and scope of the "right to spy."

A. On Hohfeldian Claim Rights and Liberty Rights

Newcomb Hohfeld, in his seminal work *Fundamental Legal Conceptions*, introduced the distinction between claim rights and liberty rights as put forward by Wesley. In one of the footnotes in the book Hohfeld engages in a conversation with Sir Fredrick Pollock's prior writing in his volume *Jurisprudence* on the meaning of rights. According to Pollock, Hohfeld says, a "liberty" is only a right "in the popular and rudimentary sense of not being forbidden."[215] Hohfeld then proceeds to respond to Pollock's claims: "It is difficult to see, however, why, as between X and Y, the 'privilege + no right' situation is not just as real a jural relation as the precisely opposite 'duty + right' relation between any two parties." Hohfeld ponders that perhaps the reason for our habit of recognizing only the latter as a jural

211. For more on the need for a theoretical separation between *Jus Ad Bellum* and *Jus In Bello*, see Jasmine Moussa, *Can Jus Ad Bellum Override Jus In Bello? Reaffirming the Separation of the two Bodies of Law*, 90 Int'l Rev. Red Cross 963 (2008).

212. *See* Chesterman, *supra* note 4, at 1072.

213. Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage, in* International Cyber Norms: Legal, Policy & Industry Perspectives 65, 84 (Anna-Maria Osula & Henry Rõigas eds., 2016).

214. *Id.*

215. Welsey Newcomb Hohfeld, Fundamental Legal Conceptions 48 n.59 (Walter Wheeler Cook ed., 2003). Elsewhere on the same page, Hohfeld cites the opinion of Cave J in *Allen v. Flood*, a leading case in English tort law. Cave wrote the following: "[I]t was said that a man has a perfect right to fire off a gun, when all that was meant, apparently, was that a man has a freedom or liberty to fire off a gun, so long as he does not violate or infringe any one's rights in doing so, which is a very different thing from a right, the violation or disturbance of which can be remedied or prevented by legal process." *Id.* at 48.

relationship is found in "traditional tendency to think of the law as consisting of "commands," or imperative rules." He then clarifies the fallacy, noting that "[a] rule of law that *permits* is just as real as a rule of law that *forbids.*"[216] In simple terms liberty is thus merely an absence of a duty to abstain from action, and therefore the person against whom the liberty is held has a "no-right" concerning the action in question. On the other hand, that very person also has a liberty right of his own – to interfere in the activity.

Lazarev employs the imagery of a smoking neighbor to explain the value of "liberty rights" and the elegance of Hohfeld's analysis. Lazarev describes meeting a smoking neighbor (S) in the street. When Lazarev asks the man to stop, S responds that he has a 'right' to smoke, as there is no legal prohibition forbidding said smoking. Lazarev notes that in this context "S is confusing his entitlement. He does not have a right (in the Hohfeldian sense) to smoke, but merely a liberty (a weaker right)."[217] At the same time Lazarev also has a liberty, to impede on his neighbor's smoking, "by raising [his] voice or encouraging other people to make fun of S for his smoking habit, which may make him stop."[218] As Lazarev concludes, Hohfeld provided us with a "precise vocabulary" for understanding everyday jural relationships. "Had it not been for Hohfeld . . . S would mistake his liberty for a right, and accordingly would be unable to accurately report the effect of his entitlement."[219]

B. Spying as a Liberty Right

Scholars who reject the existence of a sovereign right to spy under customary international law, much like the smoker at the end of Lazarev's story, mistake a liberty for a hard claim right. They see the world from Sir Pollock's perspective: States either have a right to spy which would impose a duty to respect that right on third parties, or they have nothing – there can be no middle ground. Instead one might conceive of spying much like smoking. I have a weaker liberty right to spy in your territory, but that right doesn't create a duty on you to suffer the asphyxiating vapors of my surveillance. In fact, you have the liberty to interfere with my spying by engaging in counter-espionage operations, enacting legislation, bringing criminal proceedings against my spies, or taking retaliatory diplomatic measures – declaring my diplomats *persona non grata*.

---

216. *Id.*

217. Nikolai Lazarev, *Hohfeld's Analysis of Rights: An Essential Approach to a Conceptual and Practical Understanding of the Nature of Rights*, MURUEJL (2005), https://perma.cc/579X-HUD9.

218. *Id.*

219. *Id.* Another common imagery provided is that of a race. Person X has the liberty to win the race. Nobody has a claim-right against X winning the race but, at the same time, nobody has a duty to let X win the race. Quite the opposite, the other racers have a liberty to do everything they can (within the rules of the race) to prevent X from winning.

Introducing the concept of "liberty rights" opens the door for custom around espionage to evolve as it helps fulfil the elements required for the identification of custom. Indeed as of current state of drafting, consensus seems to be building at the ILC around a definition of *opinio juris* as encompassing a "sense of a legal right or obligation."[220] If a sense of a legal right makes for *opinio juris*, then articulating States' entitlement as a type of right becomes foundational for achieving those customary modifications that the ICJ described. Currently intelligence agencies, and the governments that control them, lack the "precise vocabulary" for explaining their international jural nature to the general public. Nonetheless, one should not equate a lack of proper vocabulary with a lack of actual *opinio juris*.[221]

Recall the Obama-Merkel spying scandal of 2013. When German Chancellor Merkel learned of the fact that the U.S. was monitoring her communications, she expelled a top U.S. official from the embassy in Berlin, stating in a press conference that "Spying among friends — that is simply not done."[222] She then joined hands with Brazil (whose leader was too a victim of American surveillance) to pass a U.N. General Assembly Resolution protecting the right to privacy in the digital age in the face of mass surveillance.[223] As readers of spy novels know all too well, it was only a matter of time before the other shoe dropped. Two years later it was revealed that the German foreign intelligence agency (BND), at the request of the NSA, surveilled European ministries, institutions, and corporations.[224] Even the pope was not immune from BND's spying, nor were charities like Oxfam.[225]

220. *See* Michael Wood (Special Rapporteur), Int'l Law Comm'n, Fifth Rep. on Identification of Customary Int'l Law, UN Doc. A/CN.4/717, ¶¶ 73, 76–77 (Mar. 14, 2018). Note that the United States "suggested that the express reference to the concept of a legal right in the definition of acceptance as law should be omitted." It claimed that this would prove "potentially confusing" because it would give the false impression that States might be required "to establish *opinio juris* or that a general and consistent practice of States support an action as lawful, before they can lawfully engage in a practice that is not otherwise legally restricted." *Id.* at ¶ 73 n.207.

221. *Cf.* Navarrette and Buchan, *supra* note 62, at 942 (suggesting that "most States may be motivated to spy for their own benefit, but reluctant to see these benefits generalized to more powerful peers." Navarrette and Buchan therefore conclude "there is a lack of opinio juris on espionage." But instead it could be that States lacking the necessary Hohfeldian vocabulary are struggling to articulate their unique jural relationship with a spying state. It is not that they are "reluctant" to recognize the customary nature of spying, it is that they are refusing to accept that such spying could be legitimized when done unto them, and that is precisely what they are expected to do in the Hohfeldian sense of spying as a liberty right or privilege).

222. *See, e.g.*, Philip Oltermann & Spencer Ackerman, *Germany Asks Top US Intelligence Official to Leave Country Over Spy Row*, The Guardian (July 10, 2014), https://perma.cc/KL4S-FDFS; Bruno Waterfield, Christopher Hope, & Raf Sanchez, *Angela Merkel: Spying Between Friends is Unacceptable*, The Telegraph (Oct. 24, 2013), https://perma.cc/4KDA-VDRB.

223. *See, e.g.*, Katitza Rodriguez, *Brazil and Germany Proposed UN Resolution Against Mass Surveillance*, Electronic Frontier Found. (Nov. 12, 2013), https://perma.cc/U9ZE-U73E.

224. *See, e.g.*, Alison Smale, *Germany, Too, Is Accused of Spying on Friends*, N.Y. Times (Nov. 12, 2013), https://perma.cc/E6LT-2N7N.

225. *See, e.g.*, Janet Mines and Stephen Brown, *Germany Spied on Friends, Allies and the Vatican*, Politico (Nov. 8, 2015), https://perma.cc/BL4L-DTR7.

For those who argue against the law of espionage as a *lex specialis* customary subfield of international law, this episode offers the perfect example of the cynicism that surrounds the practice. However, one can alternatively suggest that these events reflect the custom at its finest. The US exercised its liberty right to spy on Germany until such time as the operations were exposed, at which point Germany, as if on cue, began heckling America (like Lazarev did in the smoker story). Later it was Germany's exercise of her liberty right to spy that was exposed, and in turn, it was her European allies who were lampooning her. Explaining espionage law and practice in this way helps "accurately report the effect of [the] entitlement" and also the limits of the right. It also proves that state practice and *opinio juris* do in fact go in tandem, as opposed to the position held by certain relativist accounts above discussed (*supra* Section II.C.). All countries spy, and all countries legislate against spying done unto them, and that makes perfect sense within a liberty right framework. In keeping their spying the subject of plausible deniability states engage in a clever dance: the "spy block tango." By doing so, they tacitly accept the rules of the game, a set of "unexpressed but generally accepted norms and expectations."[226]

To my knowledge, the only other scholar to suggest thinking of spying through Hohfeldian lenses was Professor Chesterman.[227] In a single paragraph in his 2006 Article "*The Spy Who Came in From the Cold*"—one that hasn't been picked up in the literature since—Chesterman shows how through bilateral and multilateral treaties we might be able to turn the liberty right to spy into a claim right or alternatively be able to prohibit spying. After citing the provisions on "national technical means of verification" from both the ABM and SALT I reciprocal spying regimes, Chesterman writes:

> These provisions effectively establish a right to collect intelligence, at least with respect to assessing compliance with the arms control obligations. . . It then prohibits interference with such activities and limits concealment from them. Drawing on Wesley Newcomb Hohfeld's analytical approach to rights, this amounts to a claim-right (or a "right" *stricto sensu*) for state A to collect intelligence on state B's compliance, as state B is under a corresponding duty not to interfere with state A's actions. This may be contrasted with the treatment of spies in the laws of war . . .

226. Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. Rev. 217, 226 (1999).

227. In a 2006 article on the ethics of torture, Professor Fritz Allhoff had a footnote reference to Hohfeld's categories of rights, though the analysis there was far more limited to the question of the relationship between the torturer and the tortured and did not address interstate relations. *See* Fritz Allhoff, *Ethical Defense of Torture in Interrogation*, *in* Ethics of Spying: A Reader for the Intelligence Professional 126, 138 n.9 (Jan Goldman ed., 2006). *See infra* note 230, at 45 for another scholar, Ronald E. Watson, referring to Hohfeld in his analysis of espionage regulation, though his engagement with Hohfeld is far from clear.

> where state A may have a *liberty* to use spies – state B is unable to demand that A refrain from using spies but is not prevented from interfering in their activities.[228]

Following Chesterman's logic we can argue that the Treaty on Open Skies, discussed above, is a multilateral treaty that turns the liberty right to spy into a claim right, whereas the infamous "No Spy Agreement" that allegedly exists between the 5-Eyes member states,[229] turns the liberty right to spy into a no right. In other words, through contracting we may be able to change the reciprocal expectations and affirm a new jural relationship between spy and spied.

Note that the liberty right conceptualization of governmental surveillance applies only at the interstate level, not the intrastate. The Hohfeldian theory of liberty rights – the notion that one has a "liberty" to do X, when one has a "no duty" not to do X – while useful in the foreign surveillance context, doesn't extend to domestic surveillance activities where certain constitutional and administrative constraints apply as to the power of the state to surveil its own nationals. Those domestic constraints make it so that the government can no longer claim to have a liberty, rather it has a "no right."[230]

IV. The Limits of the JUS AD Explorationem

Recognizing the existence of the right to spy is an important first step towards regulation, as it opens the door for possible limitations introduced through the doctrine of abuse of rights. The doctrine has its origins in canonical Roman law. The legal maxim "*neminem laedit qui suo jure utitur*, es-

228. *See* Chesterman, *supra* note 4, at 1091.

229. The 5-Eyes is an intelligence alliance encompassing the United States, the United Kingdom, Canada, Australia, and New Zealand. For further reading on the alliance, *see, e.g.*, Andrew O'Neil, *Australia and the 'Five Eyes' Intelligence Network: the Perils of an Asymmetric Alliance*, 71 Aust. J. Int'l. Aff. 529 (2017). An arrangement for no-spying is allegedly contained within the UKUSA arrangement that binds the 5-Eyes Member States. Kady O'Malley, *From the Order Paper Question Archives: Do the "Five Eyes" Watch Each Other?*, CBC News (October 10, 2012), https://perma.cc/WL4F-MNQK. *But cf.* Zeke J. Miller, *Obama: "There's No Country Where We Have a No-Spy Agreement,"* Time Magazine (Feb. 11, 2014), https://perma.cc/5UCS-E36W.

230. Ronald Edward Watson, Spying: A Normative Account of the Second Oldest Profession (May 2013) (unpublished Ph.D. dissertation, Washington University in St. Louis) , https://perma.cc/27MX-R4YM (suggesting that countries have no "liberty (in the Hohfeldian sense) to spy," Watson relies only on a domestic surveillance example: "[Y]ou spot a police officer furtively peering through your neighbor's window. You approach the officer and you ask her why she is secretly investigating your neighbor. She shrugs and says "you can't prevent crimes you don't know about." Most people would conclude (on the assumption that the officer is sincere) that her spying is wrong since she has no good reason for it. Peering into the windows of more or less randomly chosen people is unlikely to prevent crime – at least not efficiently."). Watson's intuition only holds water in the domestic context. If the Officer was an American NSA agent and the peering was done through the telecommunications networks of Saudi Arabia I doubt most would similarly conclude "the spying is wrong."

tablishes that nobody may harm another in exercising their rights."[231] The doctrine has since been established as a general principle of international law,[232] and is commonly cited in the writings of publicists and early cases of the PCIJ.[233]

Professor Kiss suggested that in inter-state relations "the concept of abuse of rights may arise in three distinct legal situations."[234] For the purposes of this paper let me just address the first of these categories,[235] concerning situations where Country A exercises its right intentionally "for an end which is different from that for which the right has been created, with the result that injury is caused."[236] This situation echoes the well-established concept of *détournement de pouvoir* (misuse of powers) in administrative law.[237]

Of course, an evidentiary difficulty arises in proving state "intention." As noted by G.D.S. Taylor, the necessary first step in the establishment of an abuse of rights, is our ability to "ascertain the decision-maker's reasons. He may actually state them, or, alternatively, his failure to state them may be an abuse of right."[238] And where the reasons are not stated, continues Taylor, "they must be inferred from the surrounding facts."[239] The PCIJ had further clarified in *Certain German Interests in Polish Upper Silesia* that any abuse of rights "cannot be presumed, and it rests with the party who states that there has been such misuse to prove its statement."[240] I will return to these evidentiary challenges later in my analysis. For now, suffice to say that the doctrine introduces a basic necessity requirement whereby a country is banned from exercising a right for a purpose not authorized by the international community in the formation of the right.[241]

---

231. Alexandre Kiss, *Abuse of Rights*, *in* 1 Max Planck Encyclopedia of Public International Law ¶ 4 (2006).

232. *See, e.g.*, Brownlie's Principles of International Law 562 (James Crawford ed., 8th ed. 2012); Oppenheim's International Law 407–09 (Robert Jennings & Arthur Watts eds., 1992); Kotuby & Sobota, *supra* note 134, at 107–14.

233. *Fourth Report on State Responsibility by Mr. F.V. Garcia-Amador, Special Rapporteur*, [1959] 2 Y.B. Int'l L. Comm'n 8, U.N. Doc. A/CN.4/119, at http://legal.un.org/ilc/documentation/english/a_cn4_119.pdf

234. Kiss, *supra* note 231, at ¶ 5.

235. The second category concerns cases where Country A exercises a right in such a way that hinders Country B's ability to enjoy its own rights and, as a consequence, Country B suffers an injury. *Id.* These cases involve "bad faith" or "an intention to do harm." They are thus distinguishable from the third category of cases whereby the reckless exercise of the rights of one State, causes injury to other States. *Id.* at ¶ 6. While both these categories might have relevance for the purposes of the analysis of the *JAE* and *JIE*, I will constrain myself only to the first category for reasons of succinctness.

236. *Id.*, at ¶ 5; *see also* Garcia's Report, *supra* note 233, at 8 (citing R. L. Bindschedler, *La Protection de la Propriete Privee en Droit International Prive*, 90 Recueil Des Cours De L'Academie De Droit International 212–13 (1958)).

237. *See, e.g.*, Robert Kolb, Good Faith in International Law 170–72 (2014).

238. G.D.S. Taylor, *The Content of the Rule Against Abuse of Rights in International Law* 46 Brit. Y.B. Int'l L. 323, 331 (1972–73).

239. *Id*. at 332.

240. Certain German Interests in Polish Upper Silesia (Ger. v. Pol.), Judgment, 1926 P.C.I.J. (ser. A) No. 7, at 30 (May 25).

241. *Cf.* Hersch Lauterpacht, The Development of International Law by the International Court 164 (1958) (suggesting that the abuse of rights doctrine places "considerable power, not

Crawford identifies one set of cases where the doctrine of abuse of rights should be most frequently utilized. These are cases where the doctrine "represents a plea for legislation or the modification of rules to suit special circumstances."[242] Indeed, abuse of rights is a classic general principle in the sense that its primary function is to clarify standards in the law and by doing so push forward the rule-making processes of our international system. It is truly, one of the "bees of law" as Robert Kolb once described general principles.[243] Given that the law on espionage is filled with a myriad of legal gaps, and that it is unlikely that a rule-based system will emerge organically through treaty or custom, this field of inter-State activity becomes most ripe for elucidation through the use of a general principles the like of abuse of rights.

A. Just Causes for Spying

The right to spy is a weaker liberty right, in part because it is only a derivative of harder claim-rights (for example, the rights of states for survival and individual and collective self-defense, above discussed).[244] In their book, *The Internationalists*, Professors Shapiro and Hathaway describe the shift that occurred in the international legal order from the days of Grotius to the days of Luaterphacht. From a world order centered around a privilege to use force, where "might made right," to a new world order centered around a prohibition on the use of force. They describe this new order as a "photo negative of the Old World Order."[245] To the extent that the right to spy is a derivative of the right to self-defense, we should expect to see it morphed as part of Shapiro and Hathaway's "photo negative." I put to you, that the right to spy had evolved in the post-Charter era. We witnessed a dual shift around interstate peacetime spying, both an expansion in utilization and a simultaneous imposition of a limit on the scope of circumstances justifying the operation.

---

devoid of legislative character, in the hands of a judicial tribunal." Lauterpacht thus suggests that, as a legal instrument the doctrine "must be wielded with studied restraint.").

242. *See* Brownlie's Principles of International Law, *supra* note 232, at 562.

243. Robert Kolb, *Principles as Sources of International Law*, 53 Netherlands Int'l L. Rev. 1, 27 (2006).

244. The idea that state rights might be derived from other rights, when the former are necessary to operationalize the latter, is not new. For example, in the Provisional Measures Order in *Timor Leste v. Australia*, the ICJ accepted the idea that States enjoyed a right to communicate with their counsel in a confidential manner over "issues forming the subject-matter of pending arbitral proceedings and future negotiations between the parties." *See Questions Relating to the Seizure and Detention of Certain Documents and Data*, Timor-Leste v. Austl., Request for the Indication of Provisional Measures, 2014 I.C.J. Rep. 167, ¶ 27 (Mar. 3). The Court reasoned the existence of such a right on the fact that it "might be derived from the principle of the sovereign equality of States." *Id.* In other words, the Court identified the existence of an attorney-client privilege based on the fact that it was necessary for the operationalization of the claim right to sovereign equality. *See Id.*

245. *See* Oona A. Hathaway and Scott Shapiro, The Internationalist: How a Radical Plan to Outlaw War Remade the World 97, 304 (2017).

On the one hand, certainly the prohibition on the use of force carried with it a move towards greater reliance on espionage. If in the past force was used to ensure that one's neighbors were complying with their international obligations, once that power was revoked, spying became the new pressure valve.[246] Anecdotally, one can certainly cite to the Cold War as proof of the intensification of spying in the post-Charter era. As La-Carré had noted, it was a period in which individuals:

> were being shadowed, their phones were being tapped, their cars and houses bugged, neighbors suborned. Their letters were arriving a day late, their husbands, wives, and lovers were reporting on them, they couldn't park their cars without getting a ticket. The taxman was after them and there were men who didn't look at all like real workmen doing something to the drains outside the house, they'd be loitering there all week and achieved nothing.[247]

However, at the same time, the prohibition on the use of force and the erection of the new Charter-based international security system reshaped states' expectations, by limiting tolerable spying to a specific set of justifications and use restrictions. The Cold War period was also the time where these expectations got tested, perfected, and solidified.[248]

Under the new world order, one centered around a prohibition on the use of force with self-defense being a limited exception, there are only two possible ways to justify acts of peacetime espionage (or two *Just Causes* to borrow language from JWT): the advancement of national security or the advancement of international security (and thereby of international peace and stability). Both of these justifications were echoed in a speech made by President Eisenhower in the wake of the U-2 spy planes incident, a watershed moment for the crystallization of the international right to spy. In that speech Eisenhower claimed that to avoid another Pearl Harbor, a surprise attack, requires knowledge. Ensuring "the safety of the whole free world" and allowing the United States to "make effective preparations for defense" justified Eisenhower's issuance of "directives to gather, in every feasible way, the information required."[249]

---

246. This was echoed by Baker, "Where verification and assurance measures may not illuminate noncompliance with a treaty until it is too late to remedy the derogation, espionage allows for real-time detection of violators . . . espionage encourages and enables international security agreements that parties would otherwise be hesitant to broker." *See* Baker, *supra* note 49, at 1110, 1112.

247. JOHN LE CARRÉ, THE PIGEON TUNNEL: STORIES FROM MY LIFE 165–66 (2016).

248. Joseph R. Soraghan, *Reconnaissance Satellites: Legal Characterization and Possible Utilization for Peacekeeping*, 13(3) MCGILL L. J. 458, 471–72 (1964) (discussing the Soviet "Danger Theory" which suggested that any foreign spying on the Soviet Union regardless of whether it is taking place from within or outside Soviet territory constituted an endangerment of Soviet interests and therefore a violation of its sovereignty. This theory was floated in the wake of the U-2 spy plane incident and MIDAS, only to be ultimately rejected with the adoption of SALT I and ABM, both solidifying the notion that spying to ensure compliance with disarmament regimes was acceptable).

249. *See, e.g.*, Felix Belair Jr., *President Asserts Secrecy of Soviets Justifies Spying*, N.Y. TIMES, (May 12, 1960), https://perma.cc/J98U-QXKP.

Baker, summarizing the writing of Reisman on the topic, identified three goals for the intelligence function in our global order: (1) intelligence should inform decision; (2) intelligence should offer a source of stability in maintaining international public order; and (3) intelligence should guard against surprise.[250] I agree with Baker and Reisman's analysis. That said, the fact that intelligence should inform decision is a misnomer for our purposes, for the question is what kind of decisions should it inform? The second and third goals answer that question. Intelligence should only inform those decisions necessary to guard against surprise or to increase international stability. Let us examine both of these justifications closely.

1. *National Security*

The first basis for the right to spy derives its legitimacy from the individual states – a bottom-up model grounded in self-preservation. What are the limits of this justification? Surely the term national security should not to be confused with a "Garrison State,"[251] some Machiavellian notion of power maintenance. If we merely accepted as fact that princes truly had "no other aim or consideration, nor seek to develop any other vocation outside war, the organization of the army and military discipline,"[252] then any act of government could potentially be painted with broad national security brushes and trumped up to the march of the cavalry.[253] In other words, an overtly expansive theory of national security will result in the concept drawing more and more matter inwards to the center of the mass, contracting beyond that which it can carry. It will inevitably lead to a gravitational collapse where the very justification could no longer serve its purpose.

Instead, espionage operations that serve national security interests should be understood to mean those operations that are directly linked to threats to the polity. Those are potential dangers to the Charter values of territorial integrity and political independence. In this sense national security is distinguished from mere "national interests," and even more clearly it is to be distinguished from "the interests of some nationals."[254]

At the same time the term cannot be so restrictive as to only apply to information necessary "to prevent organised violent attacks that are motivated by a political, ideological or religious cause, and that are so serious that they require a national response, normally involving military action."[255]

250. *See* Baker, *supra* note 111, at 76.

251. Harold D. Lasswell, *The Garrison State*, 46(4) Am. J. Soc. 455, 455 (1941) (discussing a world of "garrison states" in which the specialists of violence are the most powerful group in society).

252. Machiavelli, *supra* note 46, at 57.

253. *See also* Hobbes, *supra* note 39, at 27 (deriving from the right of "self-preservation," a corollary right "to use any means and do any action" to achieve such preservation).

254. *See* Tony Pfaff, *Bungee Jumping off the Moral Highground: The Ethics of Espionage in the Modern Age*, *in* 1 Ethics of Spying, *supra* note 45, at 98.

255. Toby Mendel, *Defining the Scope of National Security: Issues Paper for the National Security Principles Project,* Centre for Law and Democracy 12 (Mar. 2013), https://perma.cc/M7XB-MU3D.

This definition of national security, adopted by the Centre for Law and Democracy, is too restrictive to be applied as a broader test for the ILI, as it will significantly limit the ability of states to engage many of the legitimate operations which they conduct today in the name of protecting their nationals. Consider, for example, less articulable threats ("unknown unknowns")[256] that intelligence agencies are tasked with thwarting within the foggy environment of foreign espionage.[257]

Instead of binary definitions, it might be better to consider national security on a spectrum, where there will be cases clearly falling within the core national security interests of the state, cases that clearly fall outside that definition, and a lot of grey area in the middle. Spying on the military capabilities of an adversary would surely be considered an act in the service of national security. Spying to advance the economic interests of one's tourism industry should surely be considered outside that scope. Close call cases would involve spying for the purpose of advancing the foreign affairs interests of the state, or certain forms of economic espionage necessary to protect a state's economic well-being.[258]

The national security test thus inevitably introduces grey zones where rule-appliers are likely to face significant hurdles in reaching consensus over the drawing of legal limits, and as a result rule-abusers will see an opening to exploit the system for their own immediate gains. This fact, however, should not deter us. After all, we are accustomed in international law to such standards and have learned to deal with their ambiguity. Consider the principle of proportionality under the Geneva Conventions and Additional Protocols. In applying the principle, a small group of test cases might easily and conclusively be determined as proportionate or disproportionate, but then there is a large middle group of "close cases" where (to paraphrase the ICTY's Expert Committee) not even two military commanders, with different doctrinal background, could reach consensus.[259]

I therefore wish not to make any categorical determinations as to whether an espionage operation that is aimed at advancing a "grey area" interest could be said to result *ipso facto* in an abuse of the right to spy. This will have to be determined on a case-by-case basis, taking into account the degree to which the surveilling state's needs could be articulated in national security terms. For those who believe that introducing such a national secur-

256. Donald H. Rumsfeld, Department of Defense News Briefing (Feb. 12, 2002, 11:30 AM), https://perma.cc/T5ZP-2DCM.

257. For a discussion of the need for greater leniency in applying the principle of necessity in the foreign surveillance context, see generally Asaf Lubin, *"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18 CHI. J. INT'L. L. 502 (2018).

258. Note in this regard that, for example, both the German and the French foreign surveillance legislation expressly authorize the collection of intelligence for the purposes of advancing foreign policies. For further reading, see Asaf Lubin, *A New Era of Mass Surveillance is Emerging Across Europe*, JUST SECURITY (Jan. 9, 2017), https://perma.cc/48WU-M7FQ.

259. ICTY's Expert Report, *supra* note 205, at ¶ 50.

ity test into the ILI would result in exploitation of the term by intelligence agencies to a point of collapse, one need only cite the domestic foreign surveillance laws of certain countries who have already put the test into statutory language. Take as only one example the Swedish Signals Intelligence Act. The Act establishes eight possible justifications for foreign SIGINT collection in Section 1(2), which may be summarized in the following way: (1) military threats; (2) threats to international peacekeeping or humanitarian missions; (3) international terrorism and cross-border crimes; (4) the development and proliferation of weapons of mass destruction and similar military equipment; (5) threats to society's infrastructures; (6) foreign conflicts with consequences for international security; (7) counter-espionage; (8) foreign actions and intentions of importance to Swedish foreign, security, or defense policy.[260]

Here you have it. A country has successfully managed to translate the term "national security" into a specific set of eight well-articulable and reasoned categories of legitimate spying. It is true that certain operations under categories 5 and 8 might fall into the "gray area" in our above spectrum by pulling away from core national security concerns. That, however, does not entail a collapse of the *JAE* system as a possible constraint on peacetime espionage.

2. *International Stability and Cooperation*

The second justification for the right to spy garners its support from the structures of our international system as a whole – a top-bottom model grounded in the functions that intelligence plays in our public world order. For an operation to meet this test, it must be in the service of the *raison d'être* of the system, the fundamental goals of all law: "the minimization of violence, the maintenance of minimum order, and as approximate an achievement of the policies of human dignity as each situation allows."[261] Examples of such spying operations have been already discussed above, and may include *inter alia* the gathering and sharing of intelligence with the U.N. Security Council prior to a vote authorizing the use of force, collection efforts in relation to counter-proliferation, arms control and sanctions regimes, supporting blue helmets with information about threats to the forces, and assisting investigations by international courts, tribunals, and fact-finding missions.

Both national security and international security, as the two justifications of espionage, are of equal strength, and often their application will converge. If Germany were to launch a surveillance operation on DPRK's nuclear pro-

260. *See supra* note 198 (summarizing the Swedish law).

261. W. Michael Reisman, *Editorial Comment: Assessing Claims to Revise the Laws of War*, 97 Am. J. Int'l. L. 82, 83 (2003); *see also* W. Michael Reisman, The Quest for World Order and Human Dignity in the Twenty-First Century: Constitutive Process and Individual Commitment 442–45 (2012).

gram, such an operation would be justified both in the protection of the national security of Germany and in service of broader international stability.

At the same time when the U.S. and the U.K. spy on every member of the Security Council in the lead up to the vote authorizing the use of force on Iraq,[262] such spying might serve the national security interests of those states but run counter to the interests of the international community in maintaining an independent and impartial collective security system. Such an operation should be cautioned but nonetheless tolerated because it continues to serve at least one of the two legitimizing rationales.

B. The Application of the Just Causes

By recognizing that a liberty right to spy exists as a matter of customary international law, the international community inexplicitly created a caveat to the myth system. Countries are willing to accept as tolerable certain assaults on their territorial sovereignty, their jurisdiction to determine their domestic affairs, as well as their and their officials' immunities and privileges, in the name of maintaining the important functions that intelligence plays in public life.[263]

This entails that the relativist accounts that link legality and illegality to territoriality or to certain privileges to which the targets of surveillance are entitled, are adopting the wrong standard. Instead, those operations which serve one of the two legitimizing aims (*JAE*) and which operate within generally agreeable bounds of action (*JIE*), regardless of their geography or questions of immunity, will be stomached even by those who have been discontentedly subjected to them. The Israeli Mossad operation in Teheran, above discussed, offers one such example.

C. Unjust Causes for Spying

It follows from our analysis until now that those practices that serve neither national security interests nor the interests of the international community writ large should be considered an abuse of the right to spy and therefore condemned. As I have already alluded to, such an analysis will be directly dependent on questions of intentionality.[264]

Spying is thus not *malum in se*, rather our motivating purpose in the collection of intelligence will determine legality distinguishing right from wrong. The lawfulness of an intelligence gathering operation, as a derivative right, depends on its source. We can thus think of the right to spy as a river of legal permissibility. So long as the river's floodgates stay open, the water

262. *See* Bright & Beaumont, *supra* note 86 and accompanying text.

263. Recall that this position was suggested by a minority of the experts in Tallinn Manual 2.0. *See* TM 2.0, *supra* note 12, at 19; *see also* Schmitt, *supra* note 104, at 5 n.28.

264. *See* Baker, *supra* note 49, at 1097; *see also* Falk, *supra* note 10, at 58.

flows downstream; but when the gates are shut, the water downstream dries up. When the purpose of spying is legal, the river's gates open, and the derivative, downstream, right of spying likewise becomes available. But when the purpose of spying is illegal, it is like leaving the gates shut; the river of permissibility is blocked up, the water dries out, the downstream right to spy is lost as is the action's legality.

Below I have identified, what I believe to be, the four most salient categories of ends which fall outside the permissive structures, and therefore should not be tolerated by the international community. This is not an exhaustive list but one that, so it is hoped, could allow others to continue the conversation as to legal line drawing. I invite future scholars to both expand on the categories in this list and add new categories in light of their observations of the law and practice.

1. *Spying as a Means to Advance Personal Interests*

In November 2017 the Prague 1 District Court sentenced Jana Nagyová to two years in prison for a "misuse of intelligence" and "abuse of power."[265] Dubbed by the media as the Czech "femme fatale"[266] she was convicted for her involvement in a national spy scandal worthy of a bestselling novel. According to the indictment, in 2012 while serving as the Chief of Staff to then Prime Minister Petr Neèas, the two began a romantic affair, all behind the back of the latter's wife, his high-school sweetheart Radka Neèasová. In an attempt to speed the divorce Nagyová ordered the Czech Republic's military intelligence to gather damning information about the wife, arguing unconvincingly that spying on the home of the PM was necessary to thwart threats to his personal safety. Furthermore, to keep the affair under wraps she ordered the military to spy on a number of governmental employees, including the PM's personal driver.[267] In June 2013 Nagyová was arrested alongside eight other individuals, including the three intelligence officials who carried out her orders. The scandal triggered a political firestorm that forced PM Neèas to resign.

The Nagyová scandal concerns violations of many domestic laws. Nonetheless, under my analysis of the *JAE*, these acts would also trigger a separate violation of international law (to the extent that any of the spying was carried out outside the territory of the Czech Republic). The operation was launched not to advance the national security of the Czech Republic nor in the service of international peace and stability. Rather national resources

265. *See* Dominik Jùn, *Guilty Verdict in Case that Brought Down Neèas Government*, Radio Praha, (Nov. 23, 2017), https://perma.cc/6MVC-3DJG.

266. *See Court Finds Czech 'Femme Fatale' Guilty in Spy Scandal*, The Jakarta Post, (Nov. 22, 2017), https://perma.cc/YK2J-YVYE.

267. *See Czech ex-PM's Mistress Guilty of Setting Spies on Love Rival*, BBC, (Nov. 22, 2017), https://perma.cc/LB2S-HCUM.

were devoted towards the gathering of intelligence for the purpose of advancing personal interests of a particular political figure.

Calling such a behavior an international delinquency will thus follow in the footsteps of the gradual criminalization at the international level of other self-serving acts by government officials, such as bribery and corruption.[268] The reason behind this prohibition is rooted in an understanding that the right to spy belongs to the state, to the polity, not to any particular ruling elite.[269]

2. *Spying as a Means to Commit an Internationally Wrongful Act*

On the night of February 22–23, 2014, Russian President Vladimir Putin met with his security services chiefs to discuss the extrication of deposed Ukrainian President Viktor Yanukovych. At the end of the meeting Putin remarked that "we must start working on returning Crimea to Russia." Four days after that meeting, unidentified soldiers took over the local parliament in Crimea and deputies hurriedly voted in a new government. The Ukrainian province was formally annexed by Moscow on March 18, triggering international condemnation.[270] It is safe to assume that in the days leading up to the forceful annexation, Russian intelligence agencies were working overtime to advance Putin's declared agenda. They had a lot of fertile ground to operate from, as in the years leading up to the annexation Russian intelligence gradually took control over and enlisted spies from within the Ukrainian Security Service (SBU) and military intelligence in Crimea.[271] It raises the question, does an intelligence operation launched in immediate preparation for an unlawful annexation and with the intention of enabling such annexation, lawful under international law?

The long practiced legal doctrines of *ex turpi causa non oritur actio* ("from a dishonorable cause an action does not arise")[272] and *ex injuria jus non oritur* ("law does not arise from injustice")[273] both reflect a deep-seeded moral commitment according to which "a right cannot stem from a wrong."[274]

---

268. *See generally* Ilias Bantekas, *Corruption as an International Crime and Crime against Humanity: An Outline of Supplementary Criminal Justice Policies*, 4 J. Int'l Crim Just. 466, 468–74 (2006); *see also World Duty Free Co. Ltd. v. The Republic of Kenya*, ICSID Case No. ARB/00/7, ¶ 157 (Oct. 4, 2006).

269. *See* Jones, *supra* note 94, at 41 ("While nations may sometimes use intrusive measures to collect information, individuals may not. Thus, espionage as a form of acceptable statecraft would be considered mere theft if practiced by individuals.").

270. Agence France-Presse, *Vladimir Putin Describes Secret Meeting when Russia Decided to Seize Crimea*, The Guardian, (Mar. 9, 2015), https://perma.cc/CDG9-EWNA.

271. Taras Kuzio & Paul D'anieri, *Annexation and Hybrid Warfare in Crimea and Eastern Ukraine*, E-International Relations (June 25, 2018), https://perma.cc/F3N3-3X55.

272. Holman v. Johnson, 98 Engl. Rep. 1120, 1121, 1. Cowp. 341, 343 (1775); *World Duty Free Co. Ltd. v. The Republic of Kenya*, ICSID Case No. ARB/00/7, ¶ 179 (Oct. 4, 2006).

273. *See, e.g.*, Gabcíkovo-Nagymaros Project (Hung. v. Slovk.), Judgment, 1997 ICJ Rep. 7 ¶ 133; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1984 I.C.J. Rep. 392, 558, ¶ 268 (Nov. 26) (Schwebel, J., dissenting).

274. Legal Status of Eastern Greenland (Den. v. Nor.), Judgment, 1933 P.C.I.J. (ser. A/B) No. 53, ¶ 95 (Apr. 5) (separate opinion of Anzilotti, J.) ("[A]n unlawful act cannot serve as the basis of an action at

Our derivative right to spy necessitates an independent source that would open the floodgates of the river of permissibility, thereby legitimizing the inevitable harms associated with the practice. But if it is a wrongful activity from which our spying stems, the spying will be tainted with that illegality. Spying conducted in the immediate and necessary service of an act of aggression or annexation or in material preparation for a crime against humanity, must itself be deemed unlawful.

Put a different way, if a specific act of espionage is a constitutive element in a larger wrongdoing, if it is an integral and indispensable element in a chain of events unequivocally leading to the commissioning of an internationally wrongful act, to a point where one cannot conceive of the wrongful activity without imagining the intelligence gathering that came before it, and if such intelligence was gathered with knowledge of and intent to commit that wrongful activity, then that act of espionage must be deemed unlawful.

Consider for example the crime of genocide. It requires a showing that the perpetrator both "intended to destroy, in whole or in part, [a] national, ethnical, racial or religious group" and that that perpetrator engaged in conduct that "took place in the context of a manifest pattern of similar conduct directed against that group."[275] A constitutive element of the crime of genocide is a meticulous plan and preparation involving all of the organs of the state, including its intelligence arm.[276] Nazi Germany couldn't execute the demonic plot to round up all the Jews and rush them onto the death trains to the killing centers in Auschwitz, without the Sicherheitsdienst (SD, the intelligence arm of the SS), the criminal police, and the Gestapo engaging in information gathering - carefully drafting intelligence reference books and routinely listing and tallying those persons to be amassed, herded and killed across the Reich's Lebensraum.[277] This intelligence operation was thus wrongful twice over: first, because it lacked a *legitimate* source from which to derive its legality, but second (and more egregiously), since it formed an integral part of that very illegal act.

3. *Spying as a Means to Advance Corporate Interests*

Following the Snowden revelations, President Obama passed Presidential Policy Directive 28 on Signals Intelligence Activities. PPD-28 was unique insofar as it offered "principles and doctrines of surveillance permission and

law."). *See also* William Thomas Worster, *The Effect of Leaked Information on the Rules of International Law*, 28 Am. U. Int'l. L. Rev. 443, 447 (2013).

275. *See* Elements of Crimes of the International Criminal Court, Rep. of the Preparatory Commission for the Int'l Crim. Ct., U.N. Doc. PCNICC/2000/1/Add.2, Art. 6(a) (2000).

276. *See* XXII Trial of the Major War Criminals before the International Military Tribunal, Nuremberg, 14 November 1945 - 1 October 1946 226 (1948) ("This plan could only be executed by the use of the whole of the SS, of every branch of the SS working in unison and in cooperation with each other.").

277. *Id.* at 340–41, 346–47.

restraint"[278] to be applied by U.S. intelligence agencies in the course of their routine foreign SIGINT gathering.[279] PPD-28 expressly prohibited the collection of intelligence for the purposes of affording "a competitive advantage to U.S. companies and U.S. business sectors." In so doing it limited the reliance on economic espionage only to those cases where "the collection of private commercial information or trade secrets" is done in the service of protecting the national security of the U.S. or its allies.[280] Similarly, the 2016 German Foreign Intelligence Law prohibited the gathering of information for the purpose of achieving "competitive advantages (industrial espionage)."[281] This trend is further in line with the approach laid down in the U.S.-China "common understanding" against cyber economic espionage adopted in 2015, as well as a similar commitment adopted by the G20 the same year.[282] The IGE further entertained the possibility of a prohibition on economic espionage in Tallinn Manual 2.0, though ultimately failed to recognize it as a binding customary rule.[283]

These recent developments in state practice have led some commentators to suggest that a new norm, albeit not a legal rule, against economically motivated cyber espionage has emerged.[284] My articulation of the right to spy helps provide normative reasoning as to why such activities must be condemned. Spying to advance one's corporate competitive advantage cannot be deemed in service of either a country's national security or the stability of the international community and thus lacks legitimizing authority.

As Libicki clarifies, however, this norm should not be confused with a broader rule prohibiting all spying on commercial entities.[285] Indeed, spying on economic entities when there is an articulable national security need (e.g. to help track terrorists who used commercial systems or to identify weakness in those commercial systems necessary to develop new SIGINT capabilities to exploit them) will be tolerated for the same reason that any other form of spying to protect the nation from surprise attacks should be deemed permissible.

---

278. Benjamin Wittes, *The President's Speech and PPD-28: A Guide for the Perplexed*, LAWFARE (Jan. 20, 2014, 11:02 AM), https://perma.cc/W6N8-4JQF.

279. *Id.*

280. The White House Office of the Press Secretary, *Presidential Policy Directive/PPD-28—Signals Intelligence Activities* (Jan. 17, 2014), https://perma.cc/LU7V-92CA. PPD-28 further clarifies that "certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage." *Id.*

281. §6(5) Gesetzzur Ausland-Ausland-Fernmeldeaufkla?rung des Bundesnachrichtendienstes, [Law on Foreign telecommunications of the Federal Intelligence Service] Dec. 23, 2016, BGBI I no. 67 2016 at 3346, §6(5) (Ger.).

282. *See* Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L L. & COM. REG. 444 (2015); David Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, ASIL INSIGHT (Mar. 20, 2013), https://perma.cc/WH8U-UQLQ.

283. *See* TM 2.0, *supra* note 12, at 169 n.386.

284. Martin Libicki, *The Coming of Cyber Espionage Norms*, *in* 9TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 1, 2–4 (Henry Rõigas, Raik Jakschis, Lauri Lindstro?m, Tomáš Minárik eds., 2017).

285. *Id.* at 4.

In this regard, spying on technological innovation developed by or for the purposes of advancing a nation's military capabilities would always be a legitimate target for espionage. This was the case during World War I when spies of opposing sides were sent to collect intelligence on the industrial and scientific sectors of the adversary to secure information around the development of new secret weapons systems, including certain poisonous gasses.[286]

4. *Spying as a Means to Exploit Post-Colonial Relations*

Finally, consider the Australia-Timor Leste spy scandal. In 2004 Australia mounted a spying operation to gather information about the negotiating positions of its poor neighboring country, Timor Leste. Australia sought to rely on the information it collected to rob its neighbor in a treaty on gas extractions in the seabed between the two. This was the first natural resource found in the territory of Timor Leste, and its extraction became strategic to the economic wellbeing of the state. To facilitate the surveillance four operatives of the Australian Secret Intelligence Service pretended to be aid workers sent to assist in the "renovations" of Timor Leste's government complex. The four then bugged the walls and phones of the prime minister's office and that of the entire cabinet.[287]

As part of a provisional measures application before the ICJ, Timor Leste submitted a memorial which began by detailing its history of colonization, first in the hands of the Dutch and Portuguese and later under the control of Indonesia.[288] Part of this history concerns the Timor Gap Treaty signed in 1989 between Indonesia and Australia under which both countries jointly exploited petroleum resources in part of the Timor Sea bed. The memorial introduces all of this on purpose to highlight what it calls a "tragic story" and to exemplify "Australia's role therein."[289]

This exposition is important as it puts the Australian spying operation during treaty negotiations and later seizure of certain documents from Timor-Leste's legal counsel into context. Australia's intelligence gathering cannot be justified through either a substantiated claim of national security needs nor an argument surrounding the enhancement of collective security. Quite the opposite, Australia's spying was a destabilizing act, serving the

286. Hedieh Nasheri, Economic Espionage and Industrial Spying 12 (2005); *see also* Volkman, *supra* note 3, at 68–70 (discussing the development of food preservation through sterilization by French entrepreneur Nicholas Appert for use by the French Revolutionary Army and the theft of his intellectual property by English spies only to be reverse engineered and mass produced to support the British Royal Army).

287. *See, e.g.,* Matthew Happold, *East Timor Takes Australia to ICJ Over Documents Seized by Australian Intelligence*, EJIL: Talk! (Dec. 19, 2013), https://perma.cc/HNR3-DRWR. The two parties have since resolved their disputes surrounding the scandal. *See* Helen Davidson, *Australia and Timor-Leste Sign Historic Maritime Border Treaty*, The Guardian (Mar. 6, 2018), https://perma.cc/J79K-44J9.

288. *See* Memorial of the Democratic Republic of Timor Leste, Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Austl.), 2014 I.C.J. Pleadings ¶¶ 2.5–2.17 (Apr. 28, 2014).

289. *See id.* at ¶ 2.10.

sole purpose of weakening an already fragile society in dire need of economic resilience, all in the name of enrichening its treasury. Such an operation is a direct assault against the spirit and wording of the customary 1960 Declaration on the Granting of Independence to Colonial Countries which affirmed that the subjection of peoples to alien exploitation constitutes a denial of fundamental human rights, contrary to both the U.N. Charter and the promotion of peace and cooperation.[290] Spying of this nature thus does not serve the purposes for which the right to spy was introduced, and should be considered abusive.

V. Conclusion

Middleton's *A Game At Chess* begins with a classic opening move, the Queen's Gambit Declined, in which black refuses a pawn offered by white.[291] To explain the *lex specialis* of the law of espionage it would perhaps be better if we analogize to the opposite move, the Queen's Gambit Accepted. After all this is a field of law saturated with unvoiced yet communally endorsed constitutive structures, reciprocal expectations, and essential rules of the road. Spying and the grand old game of kings and philosophers share a thing in common, as Charles Buxton once put it: "in life, as in chess, forethought wins."

More than anything, I hope this article serves as a call for action, inviting practitioners and international scholars to join the effort of thinking creatively in tackling existing blind spots around the regulation of peacetime espionage. Cicero believed that *inter arma enim silent leges* (in times of war the law falls silent). A group of brave lawyers proved him wrong when they launched the campaign to regulate war which culminated with the adoption of the Geneva Conventions. We are now being indoctrinated into thinking that when the spies connive the laws fall silent. It didn't make sense at the time of Cicero; it certainly should not make sense to us now.

In proposing a new normative framework for thinking about the international law of intelligence, I hope to invite other scholars to further expand on this work. The list of categories of spying that might trigger an abuse of rights, for example, is far from exhaustive and may be expanded in light of new realities in spycraft. Similarly, while the adoption of an Hohfeldian liberty rights lens through which to examine the jural relations between states is innovative, such a theory may need to be reconciled with conventional accounts of how state practice and *opinio juris* shape the formation and application of customary international law on espionage. Within the limits of this piece, the paper falls short of pursuing this thread.

290. G.A. Res. 1514 (XV), ¶ 1 (Dec. 14, 1960).
291. Middleton, *supra* note 1, at 10 n.1.

Ultimately, this paper introduces three temporal paradigms for controlling espionage: *Jus Ad Explorationem, Jus In Exploratione*, *Jus Post Explortionem*. This paper focused on only the first of these three. The two remaining paradigms—law that governs the particular choice of means and targets in the conduct of spying, and the law that governs attribution and accountability regimes once spying operations have ceased or were discovered—hold the other important pieces of the regulatory puzzle.

We should reject the forces of intellectual stagnation and speak up against what Iñaki Navarrete aptly called the "Politics of Silence."[292] It is indeed the responsibility of every generation of academics to push the boundaries of the discourse that came before us, thereby challenging the collective conceptions and misconceptions surrounding the fundamental dogmas of our political life. The international law of intelligence should not be immune from such scrutiny.

292. *See* Navarrete, *supra* note 62, at 17.