The Liberty to Spy

Asaf Lubin

Abstract

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 attained the status of a dogma.

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 adopts a diagnosis of 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 rich history of Just War Theory. Adopting the Jus Ad, Jus In, Jus Post model makes for an appropriate choice, given the unique symbiosis that exists 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 operations, 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 proceeds to discuss the nature of the JAE. It argues that 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 two sole 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 (exploiting one’s right to spy not for the purposes for which it was intended). The paper thus concludes by introducing five 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; (4) spying as a means to facilitate a dictatorship; and (5) spying as a means to exploit post-colonial relationship.

---

1 Asaf Lubin is a Lecturer at Yale University, Cybersecurity Postdoctoral Policy Fellow at the Fletcher School of Law and Diplomacy at Tufts University, Visiting Fellow at the Information Society of Yale Law School and Visiting Scholar at the Hebrew University of Jerusalem. I wish to thank Michael Reisman, Matthew Waxman, Fabien Lafouasse, Curtis Bradley, and Laurence Helfer for comments on previous drafts of this piece. I also wish to thank those who attended previous workshops of this paper at events before the Harvard Law School, Yale Law School, Naval War College, and the American Society of International Law.
Table of Contents

I. INTRODUCTION........................................................................................................................................................................3
II. THE FAULTLINES OF THE EXISTING DISCOURSE ......................................................................................................................7
   A. Defining Espionage........................................................................................................................................................................7
   B. Old-School Absolutist Scholarship...............................................................................................................................................10
   C. New-School Relativist Scholarship...........................................................................................................................................14
   D. Introducing the Lex Specialis of the ILI........................................................................................................................................21
III. THE SOURCES OF THE JUS AD EXPLORATIONEM ..................................................................................................................25
   A. The Right of States to Survival and Collective Self-Determination..........................................................................................25
   B. The Inherent Right of Individual or Collective Self Defense.......................................................................................................28
   C. Collective Monitoring Obligations under UN and Treaty Law.....................................................................................................30
   D. International Human Rights Law.................................................................................................................................................35
   E. International Humanitarian Law......................................................................................................................................................37
   F. International Accountability Regimes ...........................................................................................................................................39
IV. THE NATURE OF THE JUS AD EXPLORATIONEM .....................................................................................................................41
   A. Hohfeldian Claim Rights and Liberty Rights.................................................................................................................................41
   B. Spying as a Liberty Right.................................................................................................................................................................42
V. THE LIMITS OF THE JUS AD EXPLORATIONEM ....................................................................................................................45
   A. Just Causes for Spying.......................................................................................................................................................................47
      1. National Security..............................................................................................................................................................................49
      2. International Stability and Cooperation .......................................................................................................................................51
   B. The Application of the Just Causes.............................................................................................................................................52
   C. Unjust Causes for Spying.................................................................................................................................................................52
      1. Spying as a Means to Advance Personal Interests..........................................................................................................................53
      2. Spying as a Means to Commit an Internationally Wrongful Act...............................................................................................54
      3. Spying as a Means to Advance Corporate Interests....................................................................................................................56
      4. Spying as a Means to Facilitate a Dictatorship.............................................................................................................................57
      5. Spying as a Means to Exploit Post-Colonial Relationship ......................................................................................................59
VI. CONCLUSION..................................................................................................................................................................................59
I. INTRODUCTION

Thomas Middleton’s satirical play, *A Game At Chess*, was first performed in August 1624 in the Shakespearean Globe Theater and had “an unprecedented run, the longest on the Jacobean stage”. 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 crawling with spies”. What triggered this lavish expansion in spycraft were the European Wars of Religion. The Protestant Reformation sought to erode loyalty to the papacy by calling for *sola scriptura* and *sola fide*. These provocative assertions triggered the rise of the Counter-Reformation movement as a religious and political crusade centered on the Catholic sacramental practice and a return to the spiritual foundations of devotional life. Together these battling agendas turned Europe into a “maelstrom of entities warring over religion” which brought with it a “constant danger that put a premium on intelligence”. The Westphalian legal order that emerged at the end of the Thirty Years’ War – and which was established on the principles of sovereignty, non-intervention, and the equality of states – was thus an order extremely cognizant of and susceptible to the moral debauchery of interstate intelligence gathering. The intricate webs of spies that were weaved over Europe at that time simultaneously helped shape Westphalia and were shaped by it, as an inevitable byproduct.

The intelligence profession, the shadowy work of spooks and saboteurs operating in disguise, played a massively important role in maintaining the 17th century’s balance of power and has continued to do so over the decades. From the days of Sir Francis Welsingham, 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 myriad ways by which intelligence is to be ordered, collected, processed, analyzed, verified, and disseminated. Instead, as noted by Professor

---

3 Thomas Cogswell, *Thomas Middleton and the Court 1624: A Game at Chess in Context*, 47(4) Huntington Library Quart. 273, 273 (1984). The play ran for nine performances and seen by an estimated audience of 30,000 spectators before it was shut down by the authorities for its scandalous political content.
5 Chesterman cites Garrett Mattingly to suggest that the practice is grounded in modern diplomacy as it evolved since the days of Renaissance Italy, and certainly expanded post-Westphalia, where “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” (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)).
6 See Volkman, supra note 4, at 58.
7 Hungarian adventurer and former spy Trebitsch-Lincoln describes in his book 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 Marienbad, 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)).
Chesterman, intelligence exits in a "legal penumbra, lying at the margins of diverse legal regimes and at the edge of international legitimacy".8

This should come as no surprise for those who have mastered the arts of “the second oldest profession” and the regulations that compound them.9 The literature surrounding the international law of espionage has historically been marked with a degree stagnation coalescing around three contradictory accounts each branding spying as either innately “legal” or “illegal” or “neither legal nor illegal”.10 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 at Ohio State University. The articles cover the commentaries of a number of prominent legal scholars to both the U2 spy plane incident of 1960 as well as the American program of early warning reconnaissance satellites (the Missile Defense Alarm System, or MIDAS). Whereas Julius Stone took a permissivist point of view (suggested 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).11

---

8 Chesterman, supra note 5, at 1130. See also David Silver, Intelligence and Counterintelligence, in National Security Law 935, 965 (John Norton Moore & Robert F. Turner eds., 2nd ed., 2005) (“there is something almost oxymoronic about addressing the legality of espionage under international law”).

9 Michael J. Barnett, Honorable Espionage, 2(3) J. Def. & Pol. 14, 14 (“Espionage is the world’s second oldest profession and just as honorable as the first”). Brian Steward and Samantha Newbery, Why Spy? The Art of Intelligence 1-2 (“It is often suggested that prostitution is the oldest profession in the world. But from the dawn of history people have been seeking to discover the intentions and secrets of their enemies; to penetrate the security barriers behind which their enemy works”).

10 See e.g. John Radsan, The Unresolved Equation of Espionage and International Law, 28 Mich. J. Int'l L. 595, 602 (2007) (“The literature that does exist on peacetime espionage can be split into three groups. One group suggests peacetime espionage is legal (or not illegal) under international law. Another group suggests peacetime espionage is illegal under international law. A third group, straddled between the other two, maintains that peacetime espionage is neither legal nor illegal); Peyton Cooke, Bringing the Spies from the Cold: Legal Cosmopolitanism and Intelligence Under the Laws of War, 44 U. San Fran. L. Rev. 1, 9 (2010) (“Intelligence-as-intelligence occupies very murky place in international law that might be characterized as either legal but discouraged or illegal but not enforced.”); Ashley Deeks, An International Legal Framework for Surveillance, 55(2) Va. J. Int'l L. 291, 300-313 (in discussing what she calls the “three approaches” Deeks distinguishes between those scholars that argue that international law is permissive with regards to peacetime espionage, those who argue that it is prohibitive, and those who adopt what she calls the Lotus approach). Captain M. E. Bowman, Intelligence and International Law, 8(3) Int'l J. Intelligence & Counterintelligence 321, 328 (cites back to the debate between Stone and Wright to suggest that there exist two views, one which considers territorial espionage a per se “non-innocent sovereign activity unacceptable under the basic tenants of international law” and another which Bowman considers as “clearly the more logical” which finds that “without additional effort” such practice cannot be considered a breach of the law). Cf. Craig Forcese, Pragmatism and Principle: Intelligence Agencies and International Law, 102 Va. J. Int'l L. 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…. examining law governing specific conduct”. Forcese places himself and İnaki Navarrete in this camp).

11 Essays on Espionage and international Law (Roland J. Stranger ed., 1962). Julius Stone claimed that espionage may in certain circumstances “represent not the divisive interests of each side against the other, but the common interest of both”. He distinguished between espionage’s “destructive ... green-light function” which should be limited, and espionage’s “salutary red-light function” which should be embraced (what I describe later in this paper as the distinction between the stability enhancing and stability thwarting functions of intelligence). Stone therefore concludes that we live in a “system of reciprocally tolerated espionage”, but 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, in Id, 29, 42-43. Quincy Wright, on the other hand, argued that that “in the modern world … ideological war ought to be avoided”. He claimed that for the success of democracies in winning the “confidence in their peaceful intentions” the “rule of international law, requiring mutual respect by states for the territorial integrity and political independence of other states, should be observed”. He therefore 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. See Quincy Wright, Espionage and the Doctrine of Non-Intervention in
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, concluding rather that the practice is “sometimes legal and sometimes illegal”. 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, namely distinguishing between territorial and non-territorial forms of spycraft. For example, as was most recently put forward by the International Group of Experts (IGE) who drafted Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 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 UN Charter principle of territorial sovereignty and therefore violate 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 literature, rooted in moral philosophy and intelligence ethics, which 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, moral 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 doing so, these writers adopt the traditional paradigms of international law and the use of force, which themselves are grounded in the rich history of Just War Theory (JWT). Using the Jus Ad, Jus In, Jus Post models for intelligence regulation, makes for an appropriate choice given the unique symbiosis that exists between espionage, fundamental UN Charter principles, and the control over international violence. As noted by Darrell Cole:

Spies may not be moral philosophers measuring everything they do by the word of God, to recall the language used by Le Carré’s burned-out spy, but they need to be people of moral virtue if they wish to be good and useful citizens. They must also internalize moral principles that serve as useful check in extreme circumstances. The just war criteria serve that purpose and, therefore, ought to be foundational for the moral formation for any spy. 15

Internal Affairs, in Id., 3, 23-26. Falk took a third approach concluding that “it is probably not useful to debate “the legality” of espionage in the traditional international law. For espionage, as such, possesses the peculiar quality of being tolerated but illegal”. He therefore settled on applying the Lotus doctrine to suggest that states may spy on each other subject only to the right of another state to act in self-defense. See Richard A. Falk, Space Espionage and World Order: A Consideration of the Samos-Midas Program, in Id., 45, 57, 68. At the same time, however, he argued from a policy perspective that the destabilizing nature of espionage (Falk namely focused on outer space espionage in the context of the Midas program) challenges the rationality of any of the justifications raised in favor of it. See Id., at 74-75. Ronald Stanger seemed sympathetic to Stone’s argument, in particular in the wake of the nuclear arms race and the growing need for covert unauthorized inspections, but also accepted the destabilizing nature of unilateral acts of espionage. He therefore called on international lawyers to contribute to the shaping of new arms control regimes that will be accepted by both the Cold War superpowers. See Roland J. Stranger, Espionage and Arms Control, in Id., 83, 99-100.

12 Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations 168 (Michael Schmitt ed., 2nd 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”).

13 Id., at 19.

14 See David C. Martin, Wilderness of Mirrors 10 (1980).

This article attempts to lay the foundations for the translation of these moral accounts into a revolutionary lex specialis subfield of international law, what I call the International Law of Intelligence (ILI). While diametrically opposing the existing scholarship, this articulation of the ILI maintains a clear-eyed view of the important functions that intelligence plays in our legal world order, further framing these functions within a larger global constitutive process. While investigating the phenomenon of peacetime espionage, my research does not seek to offer a naïve articulation of some unattainable lex feranda. Instead, it aims to learn from the mistakes made in previous academic endeavors, which either erred by over-emphasizing the myth system or over-simplifying the operational code.

This article focuses only on the first of the three paradigms that comprise the ILI – introducing the Jus Ad Explorationem (JAE), a sovereign’s prerogative to engage in peacetime espionage 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 derivative right to spy. To prove this point, Section III analyzes a plethora of international legal sources including the rights of states to survival, self-defense, and self-determination, collective security obligations under UN and treaty law, international human rights law, international humanitarian law, and international accountability regimes. Ultimately, this Section reaffirms what Professors Meyers S. McDougal, Harold D. Lasswell, and W. Michael Reisman argued some 45 years ago, that “[t]he key to the contemporary global security system is a reliable and unrelenting flow of intelligence to the pinnacle elites.” In the absence of hierarchal global structures and 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. What more, lacking a world “Interspy” (“a service that draws upon the sources available to all organizations willing and able to

---

16 This paper is an adaptation of a chapter of my J.S.D. doctoral dissertation titled: The Law on Espionage: From Unilateral Agencies to Multilateral Mechanisms Governing the International Law of Intelligence (ILI), supervised by Professor W. Michael Reisman at Yale Law School.

17 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 and one which is actually applied”. Reisman describes the tension between the myth and the code as a “dynamic process” and a “symbiotic relationship”. For further reading 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 44-45 (Tomer Broude & Yuval Shany eds., 2008).

18 Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, The Intelligence Function and World Public Order, 46 Temp. L.Q. 365, 434 (1973). See also Michael Warner, Intelligence as Risk Shifting, in Intelligence Theory: Key Questions and Debates 16, 17 (Peter Gill, Stephen Marrin and Mark Phythian eds., 2009) (“Several scholars over the last generation have explained in passing that intelligence helps decisionmakers cope with the ambiguity of a chaotic world”).

19 Former director-general of MIS, Sir Stephen Lander, argued that: “intelligence services and intelligence collection are at heart manifestations of individual state power and of national interest (Sir Stephen Lander, International Intelligence Cooperation: An Inside Perspective, 17(3) Cambridge Rev. Int’l Aff. 481, 481 (2004)). Former U.S. Deputy Assistant Secretary of State for Intelligence Coordination, Jennifer E. Sims had similarly contended that: “intelligence systems collect, analyze, and disseminate information on behalf of decisionmakers engaged in protecting and advancing a state’s interests in the international system. This process is inherently competitive and secretive, even among allies, because the international system is essentially one of self-help and anarchy.” (Jennifer Sims, Foreign Intelligence Liaison: Devils, Deals, and Details, 19(2) Int’l J. Intelligence & Counterintelligence 195, 196 (2006)). See also, Don Munton, Intelligence Cooperation Meets International Studies Theory: Explaining Canadian Operations in Castro’s Cuba, 24(1) Intelligence & Nat’l Sec. 119, 126-128 (2009).
work together to expose threats to world public order”), international institutions in the fulfillment of their mandate of maintaining international stability, peace and security, continue to rely almost entirely on intelligence produced by their member States. In other words, the gathering of intelligence becomes a necessary pre-requisite for the functioning of our broader legal order. States thus enjoy a derivative right, and indeed under certain circumstances even an obligation, to continuously engage peacetime espionage so to achieve these communal goals.

Section IV 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 exemplify 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. In doing so this Section further challenges our existing perceptions of the Lotus doctrine.

Section V 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 very limits of the practice – those cases in which the right may be abused by serving illegitimate purposes. Relying on the abuse of rights doctrine as a general principle of international law, this Section identifies five 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 (4) Spying as a means to facilitate a dictatorship; and (5) Spying as a means to exploit post-colonial relations.

II. 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

---

20 McDougal, Lasswell & Reisman, supra note 18, at 447. See also James L. Tyron, International Organization and Police, 25(7) 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”).

21 See e.g., Bassey Ekpe, The Intelligence Assets of the United Nations: Sources, Methods, and Implications, 20(3) Int’l J. Intelligence & Counterintelligence 377, 378-379 (2007) (“the assumption is that members of both the Security Council and the General Assembly, in their daily proceedings, come equipped with 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”); Admiral Guido Venturoni, The Washington Summit initiatives: Giving NATO the "tools" to do its job in the next century, 47(3) NATO Rev. 8, 11 (“[i]n 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 Technology Assessment (OTA), Nuclear Safeguards and the International Atomic Energy Agency, United States Congress, 5 (April 1995), at https://www.princeton.edu/~ota/dis1k/1995/9530/9530.PDF (hereinafter: OTA Report) (“The IAEA is exploring a number of means to improve its ability to determine whether states are pursuing undeclared nuclear weapon programs. However, it is not an intelligence organization, and its ability to discover undeclared activities that states wish to keep hidden from it will depend significantly on the willingness of other member states to share their own intelligence with the IAEA, as well as on the ability of the IAEA to evaluate and analyze all such information”).

22 S.S. Lotus (France v. Turkey), 1927 P.C.I.J (ser. A) No. 10, para. 46 (“international law leaves states in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable”). 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 administrative rule of law systems that require, through a principle of legality, that state agencies possess statutory authorization prior to taking an action.
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 Surveiling 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’èpée (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.

For example Miriam 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). 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”).


See Michael Warner, Wanted: A Definition of “Intelligence”, 6(3) Stud. Intel. 15 (2002). Elsewhere Warner argues that intelligence definitions tend to “group themselves in one of two camps. One follows twentieth-century American military nomenclature and holds that intelligence is information for decisionmakers; it is anything from any source that helps a leader decide what to do about an adversary. The second camp defines intelligence as warfare by quieter means.” (Warner, supra note 18, at 16).

The definition mirrors in some respects, and departs in others, from the definition put forward in Geoffrey Demarest, Espionage in International Law, 24 Denv. J. Int’l. L. & Pol’y 321, 326 (1996) (“espionage can be defined as the consciously deceitful collection of information ordered by a government or organization hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the collecting”) and another put forward in Raphael Bitton, The Legitimacy of Spying Among Nations, 29(5) Am. U. Int’l L. Rev. 1009, 1011 (2014) (“Espionage between states is [...] an undercover state-sponsored intrusion into the restricted space of another state or organization for the sake of collecting information.”).

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)). To provide such a tailored and nuanced definition,
A few observations emerge from examining this definitional structure. Most important, this 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.28 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.29

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). 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 and 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 he is doing so in support of some confidential objective.30 However, if that same diplomat relies on

---


30 As a general rule, humdrum routine diplomatic engagements would fall outside the scope of the ILI. That said a specific diplomatic engagement which involves both the concealment of the actual intentions of the diplomat in question as well as the means by which she plans to acquire the information sought (which would often entail the utilization of a degree of deceit by the diplomat), should be covered by the ILI. Consider in this regard the 1961 Profumo Affair, one of the biggest spy scandals and political controversies of the early-days of the Cold War. At the center of that public blunder stood John Profumo, then the British Secretary of State for War, who was discovered to have had a sexual affair with model and showgirl Christine Keeler. Keeler was also romantically involved with Evgenii Ivanov, a senior naval attaché at the Soviet Embassy and an officer of the Soviets’ Main Intelligence Directorate. At Keeler’s invitation, Profumo and Ivanov met and soon became friends. Relying on his intimate access to Profumo’s home and office, Ivanov was able to photograph highly classified documents pertaining to allied contingency plans for the Cold War defense of Berlin, as well top-secret specifications of U.S. spy planes and nuclear weapons. Secretary Profumo initially denied the allegations of impropriety levied against him, but eventually was forced to resign from his post, a fact that played a role in hastening the end of Harold Macmillan’s term as Prime Minister (For further reading see Jonathan Haslam, *Near and Distant Neighbors: A New History of Soviet Intelligence*, 207-209 (2015); Leon Watson, *I Did Betray My Country: Fifty Years After Profumo’s Resignation, Christine Keeler Confesses She Passed Secrets to Russians*, Daily Mail (June 9, 2013), at http://www.dailymail.co.uk/news/article-2338338/I-betrayed-country-Fifty-years-Profumos-resignation-Christine-Keeler-reveals-played-role-passing-secrets-Russians.html). There can be no doubt that the events described above form the basis of traditional espionage. Ivanov hid both the agenda behind his befriending of Profumo, and the means by which he collected the intelligence (covertly bringing a camera to a friendly meeting and then secretly photographing documents from the office). But assume now, as a hypothetical, that the relationship between Profumo and Ivanov was such that the two would meet occasionally for dinner at the former’s home. During those routine dinners political shoptalk would ensue and certain information exchanged that had some intelligence value to the Soviets. I argue that such should not pass the *de minimis* test, so to be the subject of international regulation. While Ivanov’s agenda is still concealed the means by which he engages in the collection of intelligence, an open conversation
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.  

Finally, notice that this definition focuses only on interstate and peacetime activities. The definition excludes both domestic forms of surveillance (subject to ever-increasing constitutional and administrative frameworks and regulations as well as some more amorphous structures undergirded in international human rights law) and wartime espionage (as a body of law with a greater degree of clarity surrounding it as enshrined in the treatises of IHL).

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 acts” that are “intrinsically despicable.” Two years later in the Metaphysics of Morals Kant expanded on his thinking:

A state against which war is being waged is permitted to use any means of defense except those that would make its subjects unfit to be citizens; for it would then also make itself unfit to qualify, in accordance with the rights of nations, as a person in the relation of states (As one who would enjoy the same rights as others). Means of defense that are not permitted include: using its own subjects as spies; using them or even foreigners as assassins or poisoners (among whom so-called snipers, who lie in wait to ambush individuals, might well be classed); or using them merely for spreading false reports – in a word, using such underhanded means as would destroy the trust requisite to establishing a lasting peace in the future.

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 for a treaty to be adopted, suppressing of all forms of espionage. That proposal led the former Dutch Minister of War and Rights, Jacobus Catharinus Cornelis den Beer Poortugael, to issue a strongly-worded note in response challenging the usefulness of such a prescriptive measure, which was indeed eventually rejected. Nonetheless, at that time
Among the most repulsive phenomena in the peaceful relations of States are espionage activities…. [as it] particularly suited to get in the way of reasonable reproachment among nations, which could lead to healthy relations and eventually to an, indeed, legally ordered cooperation of our.\textsuperscript{36}

Bekker, similarly referred to the idea of long-term mistrust resulting from espionage operations, when he argued that while States tend to forget aggressive “club strokes” relatively quickly, it is those low-blow to the ego that come in the form of more subtle “needle pinches”, like in the case of clandestine intelligence gathering, that carry a far more enduring memory.\textsuperscript{37} Modern prohibitionists include Professor Manuel Garcia-Mora,\textsuperscript{38} Quincy Wright,\textsuperscript{39} and the Dutch Court in \textit{Re Flesche}.\textsuperscript{40}

If the prohibitionist account began with Kant, it is not surprising to find Hobbes at the center of the permissivist camp. As Toni Erskine had summarized, Hobbes “likened intelligence agents both to spiders’ webs and to rays of light”:

\begin{quote}
[I]ntelligence agents [...] form an intricate web with which [...] rulers surround themselves and upon which they depend: “without intelligence agents,” Hobbes observed, “sovereigns can have no more idea what orders need to be given for the defence of their subjects than spiders can know when to emerge and where to make for without the threads of their webs.” Lest one take from this metaphor that Hobbes viewed intelligence agents or the activity of gathering intelligence as in any way lacking in virtue, it should be read alongside his other chosen image. “Reliable intelligence agents,” Hobbes asserted unequivocally, “are to those who exercise sovereign power like rays of light to the human soul.” Elaborating on this position, Hobbes made it clear that intelligence gathering is not only beyond reproach, but suggested that for the sovereign to fail to engage in it would be morally reprehensible.\textsuperscript{41}
\end{quote}

\textsuperscript{36} Professor Dr. E. I. Bekker, Staatsverträge wider die Spione (State Treaties Against Espionage), 17(5) DJZ 297, 297 (1912) (translated from the original German).

\textsuperscript{37} \textit{Id.}


\textsuperscript{39} See Wright, supra note 11.

\textsuperscript{40} Concluding that “[peacetime espionage] when taking place by order of a State, constitutes an international delinquency by that State against another State for which it is answerable under international law”. See \textit{In re Flesche}, Holland Special Court of Cassation (27 June 1949), reprinted in \textit{Annual Digest and Reports of Public International Law Cases for the Year 1949} 266-272 (Lauterpacht ed., vol. 16, 1955).

\textsuperscript{41} Roni Erskine, “\textit{As Rays of Light to the Human Soul}? Moral Agents and Intelligence Gathering, in 2 Ethics of Spying: A Reader for the Intelligence Professional 120, 120-121 (Jan Goldman ed., 2010).
Much like Sun Tzu,²² Nizam Al-Mulk,²³ and Hugo Grotius²⁴ before him, Hobbes shared the thinking that a leader who fails to spy is a lofty leader who had abrogated a core responsibility.²⁵ It follows 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”.²⁶ Modern permissivists have included Lassa Oppenheim,²⁷ Gary Sharp, Sr.,²⁸ Christopher Baker,²⁹ Julius Stone,³⁰ and the German Federal Court in the Espionage Prosecution Case.³¹

A third far more prominent and vocal absolutist movement considers espionage as existing outside the bounds of law, being “neither legal nor illegal”. Today many, if not most, international legal scholars share the ingenious contention that espionage, as a legal field, is devoid of meaning. For them, any attempt to extrapolate the lec lata corpus of the ILI, let alone its lec scripta, would inevitably flounder, as there is nothing to extrapolate – espionage is simply an extralegal construct.³²

---

²² Sun Tzu, The Art of War 124 (Lionel Giles Trans., 2015) (“what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. Now this foreknowledge cannot be elicited from spirits; it cannot be obtained inductively from experience, nor by any deductive calculation. Knowledge of the enemy’s dispositions can only be obtained from other men”)

²³ The 11th Persian scholar Abu Ali Hasan ibn Ali Tusi, or Nizam Al-Mulk had contended that “[i]t is indispenisible 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 everything which is occurring, be it small or great importance. If he does not do so, this will prove a disgrace, a proof of his negligence and neglect of justice... Sending out police agents and spies shows that the ruler is just, vigilant, sagacious. If he behave as I have indicated, his state will flourish”. Reprinted in Lathrop, Charles E. Lathrop, The Literary Spy: The Ultimate Source for Quotations on Espionage & Intelligence (2004).

²⁴ Hugo Grotius, De Jure Belli Ac Paeis Libri Tres 655 (Francis W. Kelsey trans., 1925) (1646).

²⁵ R. V. Jones, Intelligence Ethics, in 1 Ethics of Spying: A Reader for the Intelligence Professional 40, 41 (Jan Goldman ed., 2006). (“because a state has a 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. It order to do this, the state must gather information – openly if possible, buy using secret methods if necessary. In a world in which many societies are closed, or in which information does not circulate completely freely, the state must engage in clandestine information gathering to protect against foreign threats to its security. Historically, the notion that “Gentlemen do not read each others’ mail” has proven dangerous when applied to a state’s collection of information affecting national security”).


²⁷ Lassa Oppenheim, International Law: A Treatise 491 § 455 (vol. I, 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).

²⁸ Walter Gary Sharp, Sr., Cyberspace and the Use of Force 123 (1999) (Sharp was the first, to my knowledge, to recognize a right to spy under international law existed, 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”).


³⁰ See Stone, supra note 11.

³¹ Espionage Prosecution Case (Case No 2 BGs 38/91), German Federal Supreme Court (BGH) 94 ILR 68, 74-76 (30 January 1991) (“From the point of view of international law espionage can’t be considered illegal. No international accord has ever been reached on the subject. Nor does there exist any usage sufficient to establish a customary rule either authorizing, prohibiting, or regulating such activities in some other way”).

³² See e.g., Hays Parks, The International Law of Intelligence Collection, in National Security Law 433, 433-434 (John Norton Moore, Guy B. Roberts, Robert F. Turner eds., 1st ed., 1990) (highlighting the importance of intelligence in preventing surprise attacks and concluding that “no serious proposal ever has been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each.”); Jeffrey H. Smith, Keynote Address: State Intelligence Gathering and International Law, 28 Mich. J. Int’l L. 543, 544 (2007) (“most 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”); Report of the Special Rapporteur on the Promotion and Protection of Human Rights
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
attained the status of a dogma.\textsuperscript{53} This fiction forms the basis for a \textit{Lotus} world of action,\textsuperscript{54} one in which "states may spy on each other – and on each other’s nationals – without restriction",\textsuperscript{55} justifying their behavior through the \textit{argumentum ad hominem} of "\textit{tu quoque}".\textsuperscript{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 which begins in the following way:

Mortals should not attempt to perform miracles. We cannot convert water into wine at
weddings, turn lead into gold in a chemistry lab, or form a human being from a lump of clay.
To accept reality is to abide by the laws of physics .... Espionage and international law start
from different points. Espionage dates from the beginning of history, while international
law, as embodied in customs, conventions, or treaties, is a more recent phenomenon. They
are also based on contradictory principles. The core of espionage is treachery and deceit. The
core of international law is decency and common humanity. This alone suggests espionage
and international law cannot be reconciled in a complete synthesis. Perhaps we should leave
it at that.\textsuperscript{57}

The article’s conclusion ends in a similar tone:

\textsuperscript{53} Sulmasy & Yoo, \textit{supra} note 24, at 637-638 (2006) ("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, \textit{supra} note 10, at 293 ("why 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").

\textsuperscript{54} Falk clarifies the role that the \textit{Lotus} decision plays within the conventional account in explaining the practice of peacetime espionage: "a voluntaristic theory of international obligations, as formulated by the \textit{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". See Falk, \textit{supra} note 11, at 68.

\textsuperscript{55} Deeks, \textit{supra} note 10, at 301 ("Several government officials and scholars believe that the \textit{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").

\textsuperscript{56} Department of Defense, Office of General Counsel, \textit{An Assessment of International Legal Issues in Information Operations}, 46 (May 1999) at http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf ("The lack of strong international legal sanctions for peacetime espionage may also constitute an implicit application of the international law doctrine of "\textit{tu quoque}" (roughly, a nation has no standing to complain about a practice in which it itself engages)").

\textsuperscript{57} See Radsan, \textit{supra} note 10, at 596.
Around and around we go with the second oldest profession. What we do to them is "gathering intelligence" – something positive, worthy of praise. What they do to us is "performing espionage" – something negative, worthy of punishment. But without the negative sign that depends on the circumstances, X equals X. Gathering intelligence is just the flip side of performing espionage, and performing espionage is just one part of a country's broader effort for survival. Beyond any international consensus, countries will continue to perform espionage to serve their national interests. Negative or positive, it all depends on who does what to whom. International law does not change the reality of espionage.\(^{58}\)

Radsan thus sends a very clear message to future scholars interested in engaging in research and writing on espionage and international law: “move on 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 on the regulation of espionage. This camp may be described as the “sometimes legal sometimes illegal” camp, or the relativist piecemeal approach to the IIL. 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... examining law governing specific conduct”.\(^{60}\) We could place the works of the likes of Craig Forcese,\(^{61}\) Inaki Navarrete,\(^{62}\) Russel Buchan,\(^{63}\) and Fabien Lafouasse,\(^{64}\) in this camp,\(^{65}\) as well as Tallinn Manual 2.0.\(^{66}\) Two features are common in all of their writing.

---

\(^{58}\) Id., at 623.

\(^{59}\) Id.

\(^{60}\) See Forcese, supra note 10, 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).


\(^{63}\) See Russell Buchan, Cyber Espionage and International Law (forthcoming, 2018). Based on the abstract of the book and on a previous work produced by Buchan of a similar title (Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage*, in International Cyber Norms: Legal, Policy & Industry Perspectives 65 (Osula and Rõigas eds., 2016)) it is fair to assume that the coming book will follow the piecemeal approach, discussed below, which examines the law on espionage on the basis of the means employed and the geographical zones from which operations are taking place, which is opposed to the approach taken in this paper which rejects these factors as exclusively determinative as to the lawfulness of an intelligence operation.

\(^{64}\) Fabien Lafouasse, L’espionnage dans le Droit International (2012). Lafouasse wrote this book as a dissertation project as part of his studies at Université Paris 1 Panthéon-Sorbonne. 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. 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 and Robert Kovar, *L’espionnage en temps de paix*, 1960 Annaire Français de Droit Int'l 239, 246 (noting that the “subject of espionage is so dense, so congested with complex elements, that a uniform reply [to the question of the legality of peacetime espionage] can not, it seems, be given... 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, and 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).
First, these scholars sneer at the “lex specialis” just as forcefully as they scorn the “extralegalists.” For them there is no special customary body of international law that can be said to control the intelligence function. Rather we should only look within the broader lex generalis (namely the UN Charter Principles of sovereignty and non-intervention, human rights law, and diplomatic and consular law) to identify norms that control all of state behavior, and then apply those relevant among them irrespective of whether the activities under examination are classified as acts of “espionage”. As a result of their methodology the framework adopted by these scholars is one that puts significant emphasis on questions of territoriality. As such an undercover spy in a fedora hat and trench coat taking pictures of a foreign parliament house, or a diplomat conducting intelligence operations against her host country from within her embassy, will always violate international law, as they violate both general treaty provisions (e.g. those enshrined in the Vienna Convention on Diplomatic Relations) and general customary principles (e.g. the principle of territorial sovereignty). These scholars thus limit acts of lawful espionage only to those activities which take place either remotely (e.g. remote sensing from a satellite, aerial or naval vehicles, as well as remote interception of communications that just happen to cross through the surveiling state’s)

---

66 See TM 2.0, supra note 12, and accompanying text.
67 See e.g. Forcese, supra note 10, 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.”).
68 See e.g. TM 2.0, supra note 12, at 169-170 (the IGE agreed that “customary international law does not prohibit espionage per se”. Note that the Experts relied on a single source to make this claim, basing themselves on the Office of General Counsel, Department of Defense Law of War Manual. 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 is speaks clearly of “long-standing and well-established considerations” and “long-standing international norms” which govern this practice. See Department of Defense, Law of War Manual 990 (2016). In any event, the IGE concluded that while there is 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”. The experts cited amongst those the principle of sovereignty and the prohibition of intervention as well as the human right to privacy. Id., at 169-170. Note further that a minority of the members of the IGE were willing to entertain the idea that there exist a lex specialis of espionage law, but their position was ultimately rejected (“a few of the Experts were of the view that the extensive State practice of conducting espionage on the target State’s territory has created an exception to the generally accepted premise that non-consensual activities attributable to a state while physically present on another’s territory violate sovereignty.” Id., at 19). See also, Buchan, supra note 63, at 86 (“As espionage is a practice that is by definition committed in secret, and where states overwhelmingly refuse to admit responsibility for such conduct let alone justify it as acceptable under international law, I have concluded that there is no customary ‘espionage exception’ to the principles of territorial sovereignty and non-intervention”).
69 See e.g. the concluding tables provided in both Forcese’s (supra note 61, at 209) and Navarrete’s (supra note 62, at 63-64) papers, as well as the figure in Lafouasse’s book (supra note 64, at 311). They all establish distinctions of law based on the activity’s territorial or extraterritorial nature.
70 See e.g. TM2.0, 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, but nonetheless argued that “States have not defended such actions on the basis of international law”).
71 Id., at 211-212, 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 squred 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.
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, e.g. the documents or the communications, are located/taking place on the territory of another state, but the governmental agents are at home).
electromagnetic spectrum or internet infrastructure), or with the knowledge and authorization of the target State or the Security Council.

This framing of the ILI is unsatisfactory for four distinct reasons. Most significant of them, is the fact that this approach ignores the 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* customary principles, these scholars seem to give no weight to the operational code.

In doing so they fail to truly capture the practice, and thereby lose their target audience – the members of the intelligence community who are unlikely to accept their stringent normative structures. For this exact reason, McDougal, Lasswell, and Reisman took a completely different position, whereby they concluded that “[t]he gathering of intelligence within the territorial confines of the 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”.

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 today’s modern world.

Take for example the issue of diplomatic and consular law as one case study. As noted by Professor Chesterman:

Diplomacy and intelligence gathering have always gone hand in hand. The emergence of modern diplomacy in Renaissance Italy under-scored the importance of having agents to serve as negotiators with foreign powers, and 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.

This is why ambassadors were described as early as the 17th century as “honorable spies”. This type of diplomatic spying continues even more forcefully in the age of electronic communications. During the enactment of the U.S. Foreign Intelligence Surveillance Act in 1978, for example, the issue of electronic surveillance of diplomatic premises and its compatibility with the rules of the VCDR was discussed at length in Congress. As Forcese himself 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.”

There is significant evidence to back the administration’s argument,

---

73 Consider in this regard the European Court of Human Rights decision in Weber & Saravia v. Germany, ECtHR, App. No. 54934/00, Decision on Admissibility, para. 88 (June 29, 2006).
74 McDougal, Lasswell & Reisman, *supra* note 18, at 311.
75 See Chesterman, *supra* note 5, at 1087. See also, W. Michael Reisman, *Accord on Embassy Espionage would Ease U.S.-Soviet Tensions*, New Haven Registrar (11 September 1988) (“Diplomacy and espionage are related and sometimes even symbiotic. Every government realizes that a constant flow of accurate images of what other governments are doing and thinking is indispensable. Getting that kind of information requires placing people you can trust in your enemy’s capital. That’s why diplomacy was invented... Effective embassies are in the common interest. Embassies that can’t collect information and relay it back in secrecy to their governments are ineffective”).
77 See Forcese, *supra* note 61, at 197.
as the practice of spying from and on diplomatic missions is indeed as historical as it is commonplace.\textsuperscript{78}

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 U.S. and the U.K. spied on every single delegation to the Security Council;\textsuperscript{50} (2) During the G20 talks in Toronto in 2010, the U.S. and Canada spied on large numbers of heads of states and other diplomats in attendance,\textsuperscript{80} 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;\textsuperscript{81} (3) Between 2012-2017 Chinese agencies used backdoors into computer networks at the African Union Headquarters (networks which they paid for and installed as a gift) in order to spy on the various delegations.\textsuperscript{82}

If one wanted to apply the new school relativist 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”.\textsuperscript{83} Adopting this position seems to me to be completely skewed. It stays true to a zealous defense of textual provisions while failing to give any weight to the robust practice of States, not only conducting such surveillance operations, but indeed tolerating it as a component of international political life. 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”.\textsuperscript{84} If to quote Dinstein who wrote about certain LOAC 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 from in a telecommunications system. It must be separated from the genuine sound of law.”\textsuperscript{85} This is because, as Kelsen had taught us “the validity of the law presupposes a minimum efficacy of the law”.\textsuperscript{86} If the myth system becomes so disassociated with the operational code, it loses 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.

\textsuperscript{78} See Deeks, supra note 10, at 313 (citing Antonin Scalia who at the time of working for the DOJ OLC drafted a memorandum which 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).

\textsuperscript{79} See e.g. Martin Bright and Peter Beaumont, Britain spied on UN allies over war vote, The Guardian (Feb. 7, 2004), at https://www.theguardian.com/politics/2004/feb/08/iraq.iraq.

\textsuperscript{80} See e.g. Paul Owen, Canada 'allowed NSA to spy on G8 and G20 summits', The Guardian (Nov. 28, 2013), at https://www.theguardian.com/world/2013/nov/28/canada-nsa-spy-g8-g20-summits.


\textsuperscript{83} See Forcese, supra note 61, at 197.


\textsuperscript{85} See Yoram Dinstein, Keynote Address: The Recent Evolution of the International Law of Armed Conflict: Confusions, Constraints, and Challenges, 51 Vand. J. Transnat'l L. 1701, 1709 (2018) (he additionally writes: “it is necessary to acknowledge the existence of a cottage industry of law review articles trying to recast LOAC, reconciling it with conditions of some fantasy land in which war can be conducted without putting any civilian in harm's way. These writings are produced not only by preachers of human rights ascendancy but also by LOAC theorists who are constantly citing each other without much concern for battleground realities (of which they seem to know very little). For persons familiar with general state practice, this is a matter of bemusement or perhaps even amusement. It is accordingly advisable to keep in mind that LOAC-just like other branches of international law-is created solely by states, in treaties or in custom.”). Speaking more broadly Glennon has written that “Treaty 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).

\textsuperscript{86} See Hans Kelsen, Law and Peace in International Relations 16 (1942).
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 legality 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 determination of legality can be ascertained.87

A second reason as to why I reject the existing relativist account is that I find it ineffective in regulating the entire phenomenon of espionage. These scholars look only to address the law governing specific methods of spying in isolation from their programs as a whole. As is noted in Tallinn Manual 2.0 “while the International Group of Experts agreed that there is no prohibition of espionage per se, they likewise concurred that cyber espionage may be conducted in a manner that violates international law due to the fact that certain methods employed to conduct cyber espionage are unlawful”.88 In other words, relativist scholars only offer regulation of the Jus In Exploratione (that is 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 justifications for launching an espionage operation in the first place). In doing so they exacerbate the known problem whereby “the vast majority of the literature” seems to only be interested in “the ethical dilemmas raised during the collection of intelligence”89 while ignoring the ethical dilemmas raised during all the other stages of the intelligence cycle. By rejecting the idea that there exists a lex specialis of espionage law, piecemeal scholars have barred themselves from having any say about 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 intentions, 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 use of force, relativist thinkers seem eager to explain whether the use of chemical weapons or white phosphorus violate international law, before

87 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) (“Intelligence can claim no a priori entitlement to be excluded from the realm of ethics, and as such requires an ethical framework specifically designed for intelligence that outlines if and when its activities are justified... different intelligence collection activities can be spread along a metaphorical Ladder of Escalation according to the specific harm they cause to the individual. Once the level of harm is understood, the intelligence activity can be examined in the context of the Just Intelligence Principles to determine if the harm caused is justified or not. These principles are based on just war tradition and are designed to reflect the ethical good that intelligence can do while limiting the harm intelligence can cause.”); Y. Jones, Reflections on Intelligence 50 (1989); Loch K. Johnson, On Drawing a Bright Line for Covert Operations, 86(2) AJIL 1992 284, 305 (1992)). This also echoes Deeks approach in Confronting and Adapting, where she suggested that we adopt a pragmatist sliding scale which will take into consideration different variables to determine the degree of flexibility intelligence agencies should be given in interpreting relevant international law as part of their “margin of appreciation”. Those variables are: (1) risk of error and quantum of harm, (2) the identity and nature of the target; (3) the nature of the international rules potentially violated; (4) the existence of more overt and less intrusive means for achieving a similar aim. See Ashley Deeks, Confronting and Adapting: Intelligence Agencies and International Law, 102 Va. L. Rev. 599, 671-675 (2016). I completely endorse these factors, which she also calls “guideposts”, but go even further to suggest that Deek’s flexible analysis might have legal underpinning if one considers certain general principles of international law (such as rule of law, good faith, proportionality, effectiveness, fairness, and comity) as rule clarifiers.

88 See TM 2.0, supra note 12, at 169-170.

89 Hans Born & Aidan Wills, Beyond the Oxymoron: Exploring Ethics through the Intelligence Cycle, in 2 Ethics of Spying: A Reader for the Intelligence Professional 45 (Jan Goldman ed., 2010).
they address the analytically distinct and far larger question of if and when is it lawful to go to war? Before we engage in a tactical review of the legality of particular means of spying (such as 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.

A third concern I have 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”. 90 Western foreign surveillance laws that authorize these programs of bulk remote interception of communications offer an example of what Chimni was depicting. Third world countries are impacted twice by relativists’ conceptualization of espionage: once because they become the subject of these mass remote surveillance programs over which they have no control, and second because their own more primitive and less costly forms of territorial and diplomatic espionage have now been deemed unlawful.

What 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. 91 This trend triggers exactly what Chimni warned us from, “a global law without the state” a “lex mercatoria” where “the transnational corporate actor is the principal moving force in decentralized law-making”. 92 Piecemeal scholars have been completely ignorant to potential TWAIL-critiques of their articulation of the ILI which has helped “create a global system of government suited to the needs of transnational capital but to the disadvantage of third world peoples”. 93 It is worth recalling the writing of Ratna Kapur:

“The past remains the present, albeit in a different form, and the historical relationship with Empire continues to inform the way in which the relationships of dominance and subordination, inclusion and exclusion, are played out in the contemporary period.” 94

Finally, as data becomes more and more “un-territorial”, 95 and as espionage becomes more and more digital, 96 relying on territorial line drawing as the sole basis for the regulation of intelligence operations becomes less and less defensible or articulable. It should, therefore, not be surprising to find piecemeal scholars struggling to stipulate what rules should govern cyber-espionage (or as

---


92 See Chimni, supra note 90, at 58.

93 Id., at 60 (suggesting further that: “the entire ongoing process of redefinition of State sovereignty is being justified through the ideological apparatuses of Northern States and international institutions it controls. Even the language of human rights has been mobilised towards this end. If this trend has to be reversed in terms of equity and justice, the battle for the minds of the third world decision-makers and peoples has to be won.”).


95 For a further reading see Jennifer Daskal, The Un-Territoriality of Data, 125(2) Yale L. J. 326, 365-378 (2016).

96 See Forcese, supra note 10, 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 170-171 (“The Experts were incapable of achieving consensus as to whether remote cyber espionage reaching a particular threshold of severity violates international law”).
Forcese aptly called it – “the cyber headache”). 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 E. Or what to become of a scenario where Country A stores its data on servers located in Country B and transmits its information through internet architectures located in Countries C and D, as Country E intercepts those data transfers somewhere along this protracted chain. The Canadian courts seemed to have adopted the position that such operations would result in extraterritorial enforcement and therefore violate international law, but to suggest that these operations are either akin to or distinguishable from territorial spying is an exercise in analogizing and whatever analogy is eventually endorsed seems to me to be difficult to justify, hard to explain, and complicated to apply. Ultimately we should agree that such metaphors, as is the case for all

97 See e.g. Aaron Shull, Cyber Espionage and International Law, GigaNet: Global Internet Governance Academic Network, Annual Symposium 1 (2013), at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809828 (“The difficulty in assessing legality is amplified when analyzing cyber intrusions, because they do not offend the principle of territorial integrity in the same way that sending an actual state agent to gather human intelligence (colloquially referred to as “HUMINT”) would”). Shull does seem to suggest that the principle of non-intervention may play the role that territorial lines fail to play citing to the work of Mary Ellen O’Connell in this space: “Just because a cyber-attack or cyber espionage do not amount to an armed attack does not mean that international law has no law against such wrongs. Interference with a State’s economic sphere, air space, maritime space or territorial space, even if not prohibited by treaty is prohibited under the general principle of non-intervention. This is apparent in a number of treaties, UN resolutions and ICJ decisions that condemn coercion, interference or intervention that falls short of the use of force” (Mary Ellen O’Connell, Cyber Security without Cyber War, 2 J. Conflict & Sec. L. 187, 202-203 (Vol. 17) (2012.). Ultimately, however, Shull concludes that “the 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 International Law of Cyberspace, 42(2) YJIL 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).

98 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-23, 2018 F.C. 738, para. 119-147 (Can.).

99 Buchan had made the claim that “states exercise territorial sovereignty over cyber infrastructure that is physically located within their territory”. He further argued that “acts of cyber espionage that intrude on the cyber infrastructure of a state for the purpose of intelligence-gathering constitute a violation of the principle of territorial sovereignty”. See Buchan, supra note 63, at 73. To prove his point he relied heavily on what he claimed was sufficient state practice that “asserts that they exercise territorial sovereignty in cyberspace”. Id., at 71. This argument stands in stark contradiction with the collapse of the UN Group of Governmental Experts on Information Security failure to reach any agreement on the way the UN 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 (Jul. 31, 2017), at https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/; Michael Schmitt & Liis Vihul, International Cyber Law Politicized: The UN GGE’s Failure to Advance Cyber Norms, Just Security (June 30, 2017), at https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/) as well as the recent statement of the UK Attorney General who refused to apply the principles of sovereignty to cyberspace. See Jeremy Wright QC MP, Cyber and International Law in the 21st Century, Attorney General Office (May 23, 2018), at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (“Some have sought to argue for the existence of a cyber specific rule of a “violation of territorial sovereignty” in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government’s position is therefore that there is no such rule as a matter of current international law”). Terry had too claimed that cyberespionage might violate sovereignty basing his reasoning on the language adopted in both the Islands of Palmas and Lotus Cases. According to Terry “sovereignty undoubtedly encompasses a State’s right to exercise therein, to the exclusion of any other State, the functions of a State, which, of course, means that a State may not exercise its power in any form in the territory of another state”. Based on this definition, he concludes that remote espionage, in the context of intrusion of foreign officials into data stored on servers located on the surveilled State’s sole
analogizing in the field of law and technology, are susceptible to manipulation in the name of advancing particular policy agendas.\textsuperscript{100}

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 EEZ. Much like cyberspace the EEZ’s legal regime’s interaction with the principle of sovereignty is a tenuous one, as further highlighted by Galdorisi and Kaufman:

Like the transformation of a river’s fresh flowing water into that of the salty sea, the transition from territorial seas to high seas is not abrupt. There is no clear and bright line, but rather a region where the sea absorbs and dilutes the silty residue of sovereign ground, gradually replacing its fresh, muddy, provincial brown with salt and clear blue water freedom. Currents carrying elements of coastal State sovereignty and jurisdiction converge and combine in the EEZ with those containing freedoms of navigation and associated uses in favor of all States, swirling and twisting in sometimes competing directions. The EEZ is, in a juridical sense, brackish, murky and treacherous water; a 188 mile-wide band of turbulent ocean separating the territorial sea from the high seas in which competing desires for control and use meet, mix and merge. The EEZ is a zone of tension between coastal State control and maritime State use of the sea. The battle for control defines the exclusive economic zone.\textsuperscript{101}

It is this type of territorial legal duality, coupled with the advancement of new maritime surveillance technologies that make it possible for reconnaissance to be conducted from beyond the littoral, that have triggered multiple well-publicized confrontations around EEZ surveillance.\textsuperscript{102}

Adopting a piecemeal geographical zoning of espionage law fails to offer us a real panacea 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.

\textit{D. Introducing the Lex Specialis of the ILI}

The European Court of Human Rights in its groundbreaking Zakharov v. Russia decision laid the foundation for the regulation of clandestine intelligence gathering. The Court clarified that “[r]eview and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated.”\textsuperscript{103} A normative diagnosis of intelligence work 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 \textit{Jus Ad Bellum} (JAB), \textit{Jus In Bello} (JIB), and \textit{Jus Post Bellum} (JPB).

\begin{flushleft}
\footnotesize{\textsuperscript{100} Ryan Calo, \textit{Robots as Legal Metaphors}, 30(1) Harv. J. L. & Tech. 209, 214 (2016) (“the 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.”).}
\footnotesize{\textsuperscript{102} For further analysis of different legal interpretations as to the legality of maritime surveillance by third states in the EEZ of coastal states, see e.g. Asaf Lubin, \textit{The Dragon-Kings Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum}, 57(1) Washburn L.J. 17 (2018).}
\footnotesize{\textsuperscript{103} Roman Zakharov v. Russia, ECtHR, App. No. 47143/06, Judgment, paras. 233-234 (Dec. 4, 2015).}
\end{flushleft}
If peacetime espionage serves the dual role of being both the great political stabilizer (increasing the potential for pacific settlement of disputes and cooperation by reducing the chances for strategic surprises) 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 power” triggering an intelligence-driven security dilemma spiral) it makes obvious sense to tie its regulation to the same international structures that bind the use by States 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 the world of spycraft. In 1986 at a Conference on Military Ethics and Education in Washington D.C. Chomeau and Rudolph laid out 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 a right of one government to interfere in the affairs of another, so long as the principles of just cause, just means, proportionality, etc., prevail”. Similarly, in 1989 William E. Colby argued that, in the context of covert action, standards for the selection of just covert activities “can be developed by analogy with the long-standing effort to differentiate just from unjust wars.” 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 profound 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. What 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.

For these reasons, the argument goes, 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 legal framework, or in other words, to have JWT “regulate espionage and serve as its source of legitimacy”.

---

104 See Baker, supra note 49, at 76; 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.”).


106 See Harman, supra note 104, at 371 (Herman explains “intrusive collection may be intended to increase national security, but may produce its own spiral of increased threat perceptions among its targets, leading to more secrecy and more intrusive collection” in response to those perceptions.).


108 William E. Colby, Public Policy, Secret Action 3 Ethics and Int’l Aff. 61, 63 (1989). See also James A. Barry, Managing Covert Political Action: Guideposts from Just War Theory, 36(2) Stud. Intl. 19 (1992) (proposing an application of JWT to Covert Action he listed Just Cause, Just Intention, Proper Authority, Last Resort, Probability of Success, Proportionality, Discrimination and Control, as the criteria to be investigated during the initial approval process of all covert activities).


110 Bitton, supra note 26, at 1017 (“The prominent justification for espionage is the “Just Intelligence” argument, which rests on the state’s right of self-defense and on JWT. 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”).

111 Id., at 1017. See also Chomeau & Rudolph, supra note 107, 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
Two primary challenges have been raised in the literature against relying on JWT as the justification for espionage. The first is a general concern with the normative value of open-ended standards in international law. Mark Phytian, in direct response to David Omand, noted his skepticism as to the value of rooting the framework in JWT suggesting that the tests it adopts “involve subjective judgments taken in specific national contexts.” This is the classic realist argument against JWT, arguably against any international legal constraints on national political power:

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.113

Although realism undoubtedly has its adherents, few philosophers find it compelling. Walzer had noted that “for as long as men and women have talked about war, they have talked about it in terms of right and wrong.”114 Reaching moral judgments on war as on intelligence, no matter how difficult or problematic such a process might prove to be, is not a matter of futility. 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”115 – that does not mean that moralists must surrender their ultimate sense that war, as does intelligence, are “a human action, purposive and premeditated, for whose effects someone is responsible”.116

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.” Bitton makes this claim in an even more eloquent fashion:

As peacetime espionage is a continuous activity, the [application of JWT to intelligence] is analogous to attempting to use JWT to justify an indefinite use of force. Furthermore, JWT offers a clear method for achieving its dual-phase goal. According to JWT, aggressors must be deterred and even may be punished. However, a particular aggressor can only be deterred and punished if the aggressor can be identified. JWT facilitates identifying the aggressor by imposing a baseline norm of non-violence. Against a backdrop of routine peace and quiet, an illegitimate attack can be identified immediately, like the first drop of ink falling on a sheet of white paper. Unlike violence, peacetime intelligence is an ongoing operation. Identifying the “aggressor” in everyday espionage would be like reading white letters on that same sheet of white paper. The “aggression” espionage respond to is unobservable. As opposed to

---

113 Barrie Paskins, Realism and Just War Theory, 6(2) JME 117, 119 (2007).
115 Id., at 15.
116 Id.
117 Omand & Phytian, supra note 112, at 52.
threats of physical aggression, the threat during peacetime cannot be objectively ascertained.¹¹⁸

The counterargument, however, is twofold: rejecting both the notion that the act of launching an aggressive war is always “identifiable”, and that the act of launching an abusive spy campaign is always “unobservable”. The 21st century has seen a move towards the “forever war”, the perpetual fight against 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. 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.

Similarly, to argue that espionage is a one unitary continuous motion, and therefore unobservable, is completely divorced of the practice. The fact that we give codenames to our espionage operations (e.g. Operation Ivy 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 an end, derived directly from the different stages and organization of the intelligence process: from policymaker’s demands to agency 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 review which addresses both the justifications for the operation (the jus ad) and the operative methods employed in 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 some determined assessors might actually end up spotting what they were after, and their heads will certainly spin at the end of that laborious process, but just like Waldo’s red and white striped outfit so too will acts of aggressive wars and abusive spying reveal themselves to those with the right kind of patience, stamina, and loupes.

My proposed framework adopts the structures of the JWT. We can thus reconceive of the regulation of peacetime interstate espionage as a framework of three paradigms, distinguishing between 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,¹¹⁹ but 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 drafters as well as contemporary legal discourse as was constrained at the time by treaty norms, customary practices, and general principles. In other words, in the post-Westphalian age we needed international lawyers the likes of Grotius, Pufendorf, Bynkershoek, Wolff, Vattel, Oppenheim, and Lauterpacht who

¹¹⁸ Bitton, supra note 26, at 1018-1019.
translated the moral and theological doctrines of JWT into legal prescriptions.\textsuperscript{120} 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”.\textsuperscript{121} To my knowledge, there has yet to have come an international lawyer who has been willing to pick up the gauntlet and attempt to give such “expression in legal form” to the philosophical accounts around JWT and intelligence so that it too could have a bearing on the evolution of international law and an impact on the regulation of the practice.

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 don’t 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 \textit{non liquet}.\textsuperscript{122} 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.\textsuperscript{123} Indeed one of the most fundamental functions of general principles is in allowing for the “organic growth” of international law,\textsuperscript{124} especially when it is lagging behind new pressing problems or technological developments.\textsuperscript{125}

For the remainder of this paper, however, I will 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 (Section III), the scope of the right to spy as an Hohfeldian liberty right (Section IV), and the limits of the right to spy resulting from the application of the doctrine of abuse of rights (Section V).

\section*{III. THE SOURCES OF THE JUS AD EXPLORATIONEM}

\subsection*{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 had argued the following during the 1963 ASIL Annual Meeting:

\begin{quote}
I must conclude that the propriety of the Cuban quarantine is not a legal issue. The power, position and prestige of the United States had been challenged by another state; and 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.\textsuperscript{126}
\end{quote}

\begin{itemize}
\item\textsuperscript{120} For an historical account summarizing the evolution of JWT in international law see Joachim Van Elbe, \textit{The Evolution of the Concept of the Just War in International Law}, 33(4) AJIL 665 (1939). See also Oona A. Hathway and Scott Shapiro, \textit{The Internationalists: How a Radical Plan to Outlaw War Remade the World} (2017).
\item\textsuperscript{121} South West Africa (Second Phase) (Eth. V. S. Afr.) (Liber v. S. Afr.), 1966 I.C.J. 6, para. 49 (July 18).
\item\textsuperscript{122} For a criticism of this aggressive usage of general principles as adjudicative “gap fillers” see Johan G. Lammers, \textit{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).
\item\textsuperscript{124} Maarten Bos, \textit{The Recognized Manifestation of International Law}, 20 GYIL 9, 42 (1977) (noting that general principles “should be able to provide international law with a most welcome possibility for growth”).
\item\textsuperscript{126} Dean Acheson, Remarks, 57 Proceedings of the ASIL An. Meeting 13, 14 (1963).
\end{itemize}
In other words, Acheson takes a similar view to the one previously described by Professor Radsan.\footnote{See Radsan, supra notes 57-59 and accompanying text.} The latter places espionage beyond the bounds of mortal rules and regulations, the former does the same to the survival of States.

Close in proximity to Acheson’s normative position one might cite those scholars who recognize the right of self-preservation as 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 century and 20th century natural law thinkers.\footnote{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 Snads eds., 1999). See also See also Lassa Oppenheim, International Law: A Treatise 207 (Lauterpacht ed., 8th ed, 1955) (noting that “from the earliest time of the existence of the Law of Nations self-preservation was considered sufficient justification for many acts of a State which violate other States. Although, as a rule, all States are under a mutual duty to respect one another’s personality, and are therefore bound not to violate one another, as an exception certain violations of another State committed by a State for the purpose of self-preservation are not prohibited by the Law of Nations.”). Oppenheim then proceeds to cite scores of examples beginning with Vattel and ending with Weiden).}

That being said, the idea that the right of self-preservation is a “fundamental right” has been highly consented. Those who oppose this position argue that any finding according to which self-preservation is “an absolute and overriding right” 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”\footnote{See George Schwarzenberger, The Fundemental Principles of International Law, Recueil des cours de l’Academie de droit International, 87, 195 (1955); see also James Lesley 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”).}

Instead of a natural fundamental right, there are those, like Austrian international law professor and diplomat Alfred Verdross who consider the right of States for Survival to be a softer liberty right that does not impose obligations on third parties:

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.\footnote{Alfred Verdross, Règles générales du droit international de la paix, Recueil des cours de l’Academie de droit International, 30, 415 (1929) (translated from the original French). I address the notion of liberty rights later in this paper.}

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 customary international law, has been limited to what has been recognized under the UN Charter as the 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”.\footnote{International Law: A Treatise, supra note 128, at 298.}

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.\footnote{Id.}
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 Declaration 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”.133

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-defense, in accordance with Article 51 of the Charter when its survival is at stake.” 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 ratio.

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 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.135 This claim finds its historical underpinnings with Grotius who had acknowledged that: “whenever two people are united, their rights will not be lost but will be shared in common…. The same principles should be applied in the case of kingdoms which are united not by treaty or by the fact merely that they have a king in common, but in a true union.”136

It is accurate to suggest that such a “true union” is a mere fiction, a symbol of sovereignty, and yet it is also an “extremely powerful fiction” as it is on the behalf of this union, that segments of different societies around the world and throughout history have gradually claimed “popular sovereignty in order to create their own polity”.137

But what are those rights “shared in common” that Grotius is speaking of? Dinstein provides the example of the right to fend off existential threats to the polity. 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”138. 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 self-determination, for peoples to fight against any attempts at the obliteration of their sovereignty. This I believe was alluded to in the words of Professor and Diplomat Philip Marshall Brown who had 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.”139

133 See Kohen, supra note 128, at 295-296. For a complete review of the relevant international instruments which predominantly exclude language relevant to self-preservation, see id., at 295-298.


136 Grotius, De Jure Belli ac Pacis, Bk II, ch. IX (1625).


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 – simply all of them necessitate that States enjoy a corollary and derivative right to engage in peacetime intelligence gathering. You may be Acheson and seeking to exude your unconstrained power over the threat of Soviet ballistic missiles in Cuba, or Oppenheim who is only attempting to remain “informed” as to the immediate threat posed by an armed group in a neighboring territory, or Dinstein who in the name of a “true union” 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. In simple terms, this derivative right to spy 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 a State 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” has been extensively documented and analysed. Even those 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. 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.”

Regardless of what interpretation of “imminence” one adopts, from a classically restrictive “Pearl Harbor”-type position to a highly permissive “Bush doctrine”-type position, both ends of the spectrum, and everything in between, will embrace a State’s derivative right to engage in peacetime intelligence gathering. For how else will a State know when a threat reaches whatever level of imminence is deemed sufficient to justify military action? 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 necessary to reach that very conclusion.

142 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).
145 See Baker, supra note 49, at 1095-1096 (“Espionage may derive normative legitimacy as an extension of the state’s well-recognized right to self-defense... espionage may be justified by corollary: in order to ensure that the right to self-
Even were we to adopt the formalistic and, in my view, anachronistic approach that only Article 51 holds (and therefore that a State may only react to an imminent threat by seeking Security Council authorization) there would still be a derivative right for States to engage in peacetime intelligence gathering. For how else will a delegation be able to prove to the Security Council that a threat is mounting, so to convince its members to vote in favour of an authorization of the use of force? To the extent that the United Nations does not have its own intelligence capacities, the Security Council must rely on member States in order to fulfil its mandate of maintaining peace and security.

Recall the image of 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. At the same 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 has 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”.147

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, justifying an action in self-defence. 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.”

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”. Nonetheless, he focused his review on anticipatory self-defence, leaving the question open by suggesting that:

In order to provide legal justification for [an Israeli or American] attack against Iranian nuclear facilities it would therefore be necessary to prove that Iran was developing nuclear weapons, that such weapons would be a dire threat, that there was no other way to prevent such development, and that the circumstances allowed for no delay.  

I note this anecdotal example to show just 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 more, to build an effective and supportive international coalition around 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 when the same Netanyahu acted a similar 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 taken from Iran’s secret nuclear archives. While the Iranians scoffed at whether the materials revealed any actual new intelligence that was not previously known, not even they challenged the legality of Israel’s Mossad agents operating deep and undercover in Teheran in order to steal those documents. Quite the opposite European Delegations and the International Atomic Energy Agency welcomed the opportunity to review the trove of documents provided by the Israeli intelligence.

Our international legal order places the burden of proof, 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 intelligence apparatuses. In the context of the above case study and in line with this legal scheme Israel is incentivized, almost invited, to spy on Iran, and Iran in turn is equally motivated to spy back on Israel (so to be able to thwart in advance what it perceives as a potential act of aggression that may be launched against it). 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


154 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 (Croatia v. Serbia), Judgment, 2015 I.C.J. Rep. 3, para. 172 (Nov. 18); Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Jurisdiction and Admissibility, 1984 I.C.J. Rep. 392, para. 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 provide by evidence that is fully conclusive” (Genocide Case, Id., at para. 178; Corfu Channel (United Kingdom v. Albania), Judgment, 1949 I.C.J. Rep. 4, 17 (Apr. 9, 1949). That said, the Court has also noted in Corfu 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 circumsitancial evidence”. Id.

The Ghouta chemical attack occurred in the early hours of 21 August 2013. The first reported use of chemical weapons came at 02:45 local time in Ein Tarma, about 3.7 miles east of the center of Damascus, and again at 02:47 in Zamalka, an adjoining district. It has since been confirmed that surface-to-surface rockets containing the nerve agent Sarin were used in the attack, and while it has been difficult to establish a precise death toll, numbers range from 300-1300, with a large proportion of the victims being children and women. In a statement made by then Secretary General Ban Ki Moon the attack was described as “the most significant confirmed use of chemical weapons against civilians since Saddam Hussein used them in Halabja in 1988.”

Shortly after the attack western governments were quick to determine that the Assad regime was behind the chemical assault. The White House, for example, published a government assessment of the attack on 30 August 2013, which claimed based on unfurnished intercepted phone calls and social media postings, that the Syrian government was responsible and that it launched the attack in a “desperate effort to push back rebels from several areas in the capital's densely packed eastern suburbs”. However reports were also coming in claiming that the evidence on which that determination was based was far from a “slam dunk”, and that there was therefore a reason why the report was released as a White House government assessment as opposed to an intelligence community assessment from the desk of the Director of National Intelligence. Other statements, attributing the attack to Assad, came from the United Kingdom, France, and Germany. Nonetheless, none of these statements provided the needed “smoking gun”, nor fully


158 See Warrick, supra note 156.


160 Gareth Porter, Obama's Case for Syria Didn't Reflect Intel Consensus, Inter Press Service (Sept. 9, 2013), at http://www.ipsnews.net/2013/09/obamas-case-for-syria-didnt-reflect-intel-consensus/ (noting that “Former intelligence officials told IPS that that the paper does not represent a genuine intelligence community assessment but rather one reflecting a predominantly Obama administration influence.”).

161 Ian Black and Ian Sample, UK report on chemical attack in Syria adds nothing to informed speculation, The Guardian (29 August 2013), at https://www.theguardian.com/world/2013/aug/29/uk-report-chemical-attack-syria (referring to a Joint Intelligence Committee report which concluded that the Syrian regime was “highly likely” to be responsible to the attack).

162 National executive summary of declassified intelligence Assessment of Syrian chemical warfare programme, French Foreign Ministry (Sept. 3, 2013), at http://webeache.googleusercontent.com/search?q=cache:FJQeozapM5oJ:www.defense.gouv.fr/content/download/219128/2437985/file/National_executive_summary_of_declassified_intelligence.pdf+&cd=1&hl=en&ct=clnk&qgl=us&client=safari (the nine page intelligence report was produced by DGSE on the basis of satellite imagery and video images as well as samples collected. It found that “the 21 August attack can only have been ordered and lead by the regime” and that “our intelligence confirms that the regime feared a wider attack from the opposition on Damascus at that moment”).

163 Matthias Gebauer, Germany Offers Clue in Search for Truth in Syria, Der Spiegel (Sept. 3, 2013), available at http://www.spiegel.de/international/world/german-intelligence-contributes-to-fact-finding-on-syria-gas-attack-a-920123.html (“German intelligence agrees with other Western agencies that the Assad regime was behind the Aug. 21
resolved the central paradox as to the motivations of President Assad to launch such a large scale attack at that time (“given the presence of UN weapons inspectors on a pre-existing mission in Damascus when the attack took place and the likely knowledge that chemical weapons use would attract international opprobrium – and cross Barack Obama’s ‘red line’”).

On the other side both the Assad regime and the Russian Government rejected these claims. Russian officials said that there was no proof that the government of Syria had a hand in the chemical attack, with President Putin dismissing such talk as “utter nonsense”. Foreign Minister Sergei Lavrov described the American, British, French, and German intelligence reports as “unconvincing” claiming further that the Assad regime had provided actual evidence that the rebels were behind the attack.

With a potential western intervention on the line, the Secretary General decided to establish a UN Mission to investigate the allegations of a use of chemical weapons in the Ghouta Area with the purpose of ascertaining “the facts related to the allegations”. The investigation was comprised of mission visits to certain impacted neighborhoods, interviews with survivors and other witnesses, documentation of munitions and their sub-components, collection of environmental samples, assessments of the symptoms of the survivors, and collection of hair, urine, and blood samples. While the mission was able to conclude unequivocally that “chemical weapons have been used... against civilians, including children, on a relatively large scale”, a fact which left the mission members “with the deepest concern”, not a single sentence is provided as to the culprits.

It is important to consider two aspects of this cast study. First it proves the old tired statement attributed to Thomas Lowe Hughes that “interested policy-makers quickly learn that intelligence can be used the way a drunk uses a lamp post – for support rather than illumination”. Moreover, the example shows that while it is true that 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.), nonetheless, certain determinations – perhaps the ones of most significance, such as in the context of establishing attribution – could only be ascertained by consulting raw national security intelligence. In this regard it is important to recall the words of former Secretary General Butros Butros-Ghali who clarified in 1993 that the United Nations simply had no intelligence to call its own.

The World Health Organization’s capacity to investigate large-scale epidemics is dependent on cooperation and assistance from national health services, and as we have already witnessed the same is true for the needs of the IAEA in monitoring compliance with the Non-Proliferation

165 See Black and Sample, supra note 162.
166 See BBC News Report, supra note 156.
167 Id.
170 For a complete analysis of the sources of information available at the United Nations, see Ekpe, supra note 21 and accompanying text.
Treaty. As previously stated, international institutions, in the fulfillment of their varied mandates, continue to rely significantly on intelligence produced by their member States. From disarmament monitoring to counter-terrorism efforts, from running effective sanctions regimes to providing assistance in disaster relief and humanitarian crises, and from combatting illicit trafficking to protecting the environment, there isn’t an area of work within the broader umbrella of “collective security” that doesn’t require such information.

The international community, being 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, and the Anti-Balistic Missiles (ABM) Systems Treaty, both signed in 1972 between the United States and the Soviet Union. Those treaties laid down an interesting framework for reciprocal spying (“national technical means of verification” if to embrace the euphemism) between two superpowers:

1. For the purpose of providing assurance of compliance with the provisions of this Treaty, each Party shall use national technical means of verification at its disposal in a manner consistent with generally recognized principles of international law.
2. Each Party undertakes not to interfere with the national technical means of verification of the other Party operating in accordance with paragraph 1 of this Article.
3. Each Party undertakes not to use deliberate concealment measures which impede verification by national technical means of compliance with the provisions of this Treaty. This obligation shall not require changes in current construction, assembly, conversion, or overhaul practices.

The Treaty on Open Skies, with its 34 ratifiers, offers a contemporary example (despite some recent enforcement issues). This treaty does exactly what SALT I and the ABM Treaty did – 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.

---

173 See OTA Report, supra note 21 and accompanying text; See also, supra notes 151-153 and accompanying text.
174 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 (SALT I), 23 UST 3462, Article V (Oct. 3, 1972).
176 Treaty on Open Skies, S. Treaty Doc. 102.37 (Mar. 24, 1992). 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. As further explained by Chesterman, supra note 5, at 1092 (“The Open Skies Agreement followed a more regulated approach that established a regime of unarmed aerial observation flights over the entire territory of its participants. Rather than guaranteeing noninterference with unilateral intelligence collection, the agreement provides for a defined quota of flights using specific airplanes and photographic technology that must be commercially available to all state parties. Imagery collected is made available to any other state party”).
One can think of other treaties, such as certain counter-proliferation and counter-terrorism treaties which establish intelligence collection and sharing obligations,\(^ {178}\) or treaties for environmental protection and for the preservation of Antarctica.\(^ {179}\) 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”\(^ {180}\).

But the buck does not just stop at treaty frameworks. The Security Council has too acknowledged the role that member States play in its ability to fulfill its mandate and established Chapter VII legally binding regimes that govern the collection and exchange of certain information. Most recently it adopted Resolution 2396, concerning threats to international peace and security caused by terrorist acts. In that Resolution the Council did not only call on member States to “intensify and accelerate” their peacetime intelligence collection efforts, it 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 certain capabilities for the collection, processing, and analysis of passenger name record (PNR) and advance passenger information (API) data,\(^ {183}\) the development and implementation of watch lists and databases on suspected terrorists,\(^ {184}\) and increased cooperation with information communication technology companies in gathering a myriad of digital records and their later sharing through bilateral and multilateral arrangements.\(^ {185}\)

Another 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).\(^ {186}\)

\(^{178}\) 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).

\(^{179}\) See e.g., Convention on Biological Diversity, 1760 U.N.T.S. 69 (Jun. 5, 1992) (Article 17 establishes that member States shall facilitate the exchange of information, from all publicly available sources, relevant to the conservation and sustainable use of biological diversity, taking into account the special needs of developing countries); The Antarctic Treaty, 402 U.N.T.S. 71, Arts. III(1) and VII(6) (Jun. 23, 1961) (setting obligations for the sharing of information).


\(^{182}\) Id., at para. 15.

\(^{183}\) Id., at paras. 11-12.

\(^{184}\) Id., at para. 13.

\(^{185}\) Id., at para. 21.

\(^{186}\) Security Council Committee Pursuant to Resolution 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
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 assessment and verification capabilities:

Improving the ability of collective security institutions to handle intelligence will enhance international cooperation to combat terrorism and strengthen verification regimes to prevent the spread of weapons of mass destruction. It may also increase the ability of such institutions to prevent conflict and ameliorate natural and man-made disasters. It will not guarantee good policy. More effective use of information should, however, make it harder to ignore emerging crises or adopt unworkable policies. It may also facilitate cooperation between states to address threats that no one state can address alone.\textsuperscript{187}

\textit{D. International Human Rights Law}

When one considers the way international human rights law addresses government surveillance, one immediately thinks of checks and constraints. That is reasonable. The international community has taken significant steps to enhance privacy protections since the signing of the ICCPR in 1966 and the Human 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. 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. The 2015 creation of a 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. The Human Rights Committee has begun to routinely address surveillance legislation and practices in its Concluding Observations to States, beginning in 2014. On the regional level, the European Court of Human Rights, the Court of Justice of the European Union, and the Inter-American Commission and Court on Human Rights have developed considerable and authoritative jurisprudence on surveillance and privacy.\textsuperscript{188}

At the same time, however, it would be wrong to assume that international human rights law doesn’t recognize the right, indeed the duty, of States to spy. The High Commissioner for Human Rights had acknowledged that the need to collect intelligence is a “legitimate aim” for governments to pursue.\textsuperscript{189}

\textit{Conduct of its Work, para. 6(h) (last amended Dec. 23, 2016), at https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/guidelines_of_the_committee_for_the_conduct_of_its_work.pdf. Note that the framework also establishes that once the sanctions list is communicated to member States, they are required to circulate it widely, including to its intelligence agencies (para. 5(c)).

\textsuperscript{187} See Chesterman, supra note 171, at viii-ix.

\textsuperscript{188} For a complete study including proper citation to all of these recent developments see Privacy International, Guide to International Law and Surveillance (Aug. 2017), at https://privacyinternational.org/sites/default/files/2017-12/Guide%20to%20International%20Law%20and%20Surveillance%20August%202017.pdf.

freedoms of others, can all be considered grounds for interferences with the right to privacy. In the leading judgment on this issue from 1978, *Klass and Others v. Germany*, the European Court of Human Rights (ECtHR) acknowledged the need of States to “undertake [...] secret surveillance” and its necessity “in a democratic society”:

Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. Similarly in *Leander v. Sweden* the ECtHR observed:

> [T]hat the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved… There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power … to collect and store in registers not accessible to the public information on persons.

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 European Court noted that “bulk interception regimes did not per se fall outside” intelligence agencies’ margin of appreciation suggesting further that:

> In view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States’ margin of appreciation.

International Human Rights law further recognizes the right of States to take certain extreme measures, which derogate from the rights enshrined in the corpus, in times of emergency threatening the life of the nation (ICCPR, Art. 4, ECHR, Art. 15). In those “exceptional situations of crisis or emergency which affect the whole population and constitute a threat to the organised life of the community of which the State is composed” international human rights law anticipates that States will take preventative and restorative steps to protect their polity. There is nothing in the

---

194 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”).
Conventions that expressly prohibits these derogations from taking place in an extraterritorial fashion (e.g. in foreign surveillance context). This echoes the language on the right to survival and will trigger therefore the same types of expected responses, including the utilization of intelligence gathering (note that both the right to privacy and the right to freedom of expression, are in fact derogable rights).

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. 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 loss of civilian life, injury to civilians and damage to civilian objects”. 196

Jean 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. 197 This was further expanded on in the report of the ICTY’s Expert Committee to investigate the 1999 NATO Bombing. The Committee found that:

The obligation to do everything feasible is high but not absolute. 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. Both the commander and the aircrew actually engaged in operations must have some range of discretion to determine which available resources shall be used and how they shall be used.

Needless to say, that 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 belligerent frame within the theater of conflict onwards.

Consider, for example, the specific issue of aerial operations. The targets of such attacks range in nature 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”; 198 (3) Classification of the various functions the target plays in the machinery

198 Often times targeting operations rely on real-time surveillance (using unmanned aerial vehicles or UAVs, on-ground informants, pre-installed surveillance devices or a combination thereof) to accompany the archived materials. See Cora Currier and Peter Maass, Firing Blind, The Intercept (15 October 2015), at https://theintercept.com/drone-papers/firing-blind/ (discussing the “tyranny of distance” which limited U.S. surveillance flights in the horn of Africa.
of the adversary’s war efforts;\[202\] 4 The existence of “sensitive sites” surrounding the target;\[203\] 5 The military advantage to be gained from attacking the target;\[204\] and 6 The expected incidental harm to civilians and civilians object from such an attack.

Much of this intelligence will be collected and collated in peacetime.\[205\] 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.\[206\] To guarantee that the information remains accurate, these cards are routinely inspected, reviewed, and updated on the basis of new intelligence.

and Yemen causing the phenomenon of “blinking” and the greater need to rely on questionable signals intelligence to fill the gaps.

199 When the target is a person, intelligence will be collected to verify the “membership” of that individual in an organized armed group or his or her “direct participation in hostilities,” as these terms are defined under IHL. For structures and other physical objects, intelligence is used to verify the targets’ specific military objective (distinguishing between those which are military objectives by their nature and location and those which are military objectives by their purpose or use). This information helps confirm, with reasonable certainty, that the targeting of these objects will not violate the principle of distinction. For a critical analysis of the “apparatus of distinction” in the shaping of the relationship between actors on the battlefield as it relates to the broader use of new surveillance technologies and Focault’s notion of dispositif see Nicola Perugini and Neve Gordon, Distinction and the Ethics of Violence: On the Legal Construction of Liminal Subjects and Spaces, 49(5) Antipode 1385 (2017).

200 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 (12 May 1998), at https://www.gpo.gov/fdsys/pkg/CDOC-106doc1/html/CDOC-106doc1.htm (“During Operation desert Storm, for example, intelligence resources were utilized to look for cultural property in order to properly identify it. Target intelligence officers identified cultural property or cultural property sites in Iraq; a ‘no-strike’ target list was prepared, placing known cultural property off limits from attack, as well as some otherwise legitimate targets if their attack might place nearby cultural property at risk of damage”).

201 Lawful attacks under IHL are limited to those which target objects “whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time [of the attack], offers a definite military advantage” (Art. 52(2) API). Intelligence is needed to affirm the necessity of a particular aerial strike on the basis of the nature of a target or its military importance to the adversary. See The 2014 Gaza Conflict (7 July – 26 August 2014): Factual and Legal Aspects, Israeli Ministry of Foreign Affairs, para. 391 (May 2015), at http://mfia.gov.il/ProtectiveEdge/Documents/2014GazaConflictFullReport.pdf.

202 As the principle of proportionality dictates, any expected civilian harms must not be excessive in relation to the military advantage anticipated (Art. 51(5)(b) API). To conduct this balancing act between harms and advantages, military commanders must be presented with, as accurate and as genuine as possible, assessments of the potential collateral damage and potential military advantage to ensue from an attack. Id., at para. 326 (“the estimation of potential collateral damage can be very challenging. No military has perfect information regarding the presence of civilians in all the areas where attacks take place. This is all the more so when operating in a complex urban environment, with dense physical infrastructure and a mobile civilian population. While militaries are required to exercise due diligence and to devote reasonable efforts to collect information with respect to the collateral damage expected, information deficits are inevitable”).

203 See, e.g., Squadron Leader H.B. Keightley, Intelligence Support for Air Operations (Air Powers Studies Centre, 1996), at 12-13, 22 (noting that “Air forces may be called into action in a variety of contingencies and will often be first on the scene in a crisis. Intelligence must therefore identify potential adversaries in peacetime and gather intelligence for anticipated crises. Therefore intelligence is a core function in peacetime... warfighting intelligence structures, resources, methodologies and products should be established, viable and operational in peacetime so that they are available in any type of conflict or for any form of operation”. Speaking specifically about target intelligence support, notes that such information assists commanders in selecting targets and therefore should be “subject to regular [peacetime and wartime] review”).

204 On the use of “target cards” see Id. at para. 246.

205 See e.g., Special Interview: How IDF UAV’s Saved Lives in Gaza, Israeli Defense Forces Blog (31 August 2014), at http://www.idfblog.com/blog/2014/08/31/special-interview-how-idf-uavs-saved-lives-in-gaza/. (in an with the deputy commander of the Israeli Air Force UAV squadron, he noted that “every few months, it is essential to check that the
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 forgotten supporting beam, that of an adequate, sufficient, and reliable stream of intelligence information that is collected and maintained in peacetime. The wartime “license to kill” thus require a derivative (and quite unusual) peacetime extension.

F. International Accountability Regimes

As the Ghouta chemical attack case study already showed, questions of attribution depend highly on intelligence collected by individual states. But as we move from traditional questions of state responsibility, to attribution of technological forms of wrongful activity the need to rely on the expertise of intelligence analysts only increases. One such example comes in the form of attribution in the cyber domain. Professor Schneier had noted that: “When you're attacked by a missile, you can follow its trajectory back to where it was launched from. When you're attacked in cyberspace, figuring out who did it is much harder”. For this reason the RAND Corporation had proposed the establishment of a “Global Cyber Attribution Consortium” as an organization that would engage in “independent investigation of majority cyber incidents, by a broad team of international experts, for the purpose of attribution”. In the absence of such an organization we are likely to see more state-driven efforts, either unilaterally or within regional security organizations for cyber-driven intelligence gathering.

Much like the law on state responsibility, international criminal law is too dependent on different types of information to assign individual criminal liability. As clarified by Moranchek:

When Nuremberg prosecutor Robert Jackson was assembling his case against top Nazi leaders, he had access to the full treasure trove of documents from a vanquished enemy that was known for its meticulous bureaucratic record-keeping... prosecutors in modern criminal trials who seek to link the "big fish" to atrocities on the ground have to rely on very different kinds of evidence than their target is still relevant. If you find a weapons storage facility today, tomorrow they could take all of the weapons out of the building and build a kindergarten. If I don’t know about that change, I might accidentally target it. That’s why we don’t only find new targets; we also keep track of the existing ones”).

206 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).

207 Bruce Schneier, *Attack Attribution in Cyberspace*, Schneier on Security Blog (8 January 2015), at https://www.schneier.com/blog/archives/2015/01/attack_attribut.html (nothing further than “[p]ackets don’t come with return addresses, and you can never be sure that what you think is the originating computer hasn’t itself been hacked. Even worse, it’s hard to tell the difference between attacks carried out by a couple of lone hackers and ones where a nation-state military is responsible. When we do know who did it, it’s usually because a lone hacker admitted it or because there was a months-long forensic investigation”). See also, Directorate-General for External Policies of the Union, Cybersecurity and Cyberpower: Concepts, Conditions, and Capabilities for Cooperation for Action Within the EU, European Parliament, Doc. No. EXPO/B/SEDE/FWC/2008-01/LOT6/09 (April 2011).


209 See e.g., Wiesław Goździewicz et. al., NATO Road to Cybersecurity 41 (The Kosciuszko Institute, 2016) (“NATO and its member states should focus their efforts on the development of cyber reconnaissance and intelligence structures equipped with enough technical and political expertise to track down actors responsible for cyber incursions. Such a system should combine CYBINT (cyber intelligence, especially techniques for cyberattack attribution), HUMINT (“conventional” human intelligence), SIGINT (signals intelligence, e.g. satellite imagery), OSINT (open source intelligence), as well as a political analysis”).
predecessors at Nuremberg and Tokyo. Witness testimony and, increasingly, intelligence information now play the roles formerly held by captured memoranda and signed orders.210

In 2001 an ICTY Judge described as “astounding” certain “satellite photography furnished by the U.S. military that pinpointed down to the minute the movements of men and transport around Srebrenica”.211 One can only imagine what the same judge would say today about modern intelligence capabilities from the hacking of computer networks to big data analysis of intercepted communications. Examples abound of reliance by international courts and tribunals on both intelligence provided to them by national authorities,212 and on their own use of quasi-intelligence collection techniques (namely open source intelligence collection and forensic analysis of digital evidence such as videos and imagery).

Consider the Special Tribunal for Lebanon’s controversial use of an exorbitant amount of telephone metadata for indicting the alleged perpetrators in the Hariri assassination,213 or the more recent arrest warrant for of Al-Werfalli, an alleged commander within the Al-Saiqa Brigade, who was charged largely on evidence collected from social media – a first of its kind for the International Criminal Court (ICC).214

With this obvious trend it should come as no surprise that the ICC Office of the Prosecutor’s 2016-2018 Strategic Plan on Prosecutorial Strategy notes further that “[t]he high pace of technological evolution changes the sources of information, and the way evidence is obtained and presented in court”.215 As a result, the OTP’s Strategic Goal 4 involves adapting the Office’s investigative capabilities and network to “the technological environment” and has included hiring cyber investigators and digital forensic analysts as well as more training and capacity building.216 To the extent that the Court intends to increase its usage of digital evidence, including through reliance on the collection, storage, (algorithmic) analysis, verification, and promulgation of intercepted communications, bulk data sets, or computerized digital depositories, to name but a few examples,

211 Id., at 479 (citing Patricia M. Wald, The International Criminal Tribunal for the Former Yugoslavia Comes of Age: Some Observations on Day-to-Day Dilemmas of an International Court, 5 Wash. U. J.L & Pol’y 87, 101 (2001)).
212 For a discussion of the problems of relying on States to share such intelligence with international tribunals see Id.
213 The Prosecutor relied on call data records (“CDRs”) pertaining to the metadata of every mobile phone call and text message in Lebanon between 2003 and 2010 so to create call sequence tablets that helped prove the identity and location of the perpetrators at the time of the assissination. The CDRs were transferred from Lebanese telecommunications providers to the United Nations International Independent Investigation Commission ("UNIIIC") and the Tribunal's Prosecution. Both the Trial Chamber and the Appeals Chamber agreed that the Prosecutor could legally request and obtain the CDRs without judicial authorization because such authorization was not required under their respective governing legal instruments. The Appeals Chamber further held that while there is a compelling case as to the CDRs protection by international human rights standards concerning the right to privacy, the transfer of the CDRs in the absence of judicial control in the particular case did not violate the right because it followed the requirements of legality, necessity, and proportionality. For further reading see, The Prosecutor v. Salim Jamil Ayyash et. al., Special Tribunal for Lebanon, The Appeals Chamber, Decision on Appeal by Counsel for Mr. Oneissi Againsnt the Trial Chamber's Decision on the Legality of the Transfers of Call Data Records, STL-11-01/T/AC/AR126.9 (Jul. 28, 2015).
216 Id., at paras. 23, 59.
collaborating with both the private sector and governments in obtaining this evidence will become inevitable. This again creates incentives, if not expectations, for governments to collect this intelligence and assist those international courts and tribunals in getting access to it.

IV. 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”. As explained by Buchan:

[When engaging in espionage] states do not generally express the belief that it is permissible under international law. Furthermore, when challenged about their espionage activities, states overwhelmingly refuse to admit responsibility for this conduct, let alone attempt to justify it as permissible under international law.

The common claim is thus that state practice and opinio juris are running in opposite directions. 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, 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

The distinction between claim rights and liberty rights was put forward by Wesley Newcomb Hohfeld, in his seminal work: Fundamental Legal Conceptions. In one of the footnotes in the book Hohfeld engages in a conversation with Sir Fredrick Pollock’s prior writing on the meaning of rights. This exchange is worth recalling in full. Hohfeld begins by summarizing his learned colleague’s approach:

Sir Fredrick Pollock, in his volume on Jurisprudence, seems in effect to deny that legal liberty represents any true legal relation as such. Thus he says, inter alia: The act may be right in the popular and rudimentary sense of not being forbidden, but freedom has not the character of legal right until we consider the risk of unauthorized interference. It is the duty of all of us not to interfere with our neighbors’ lawful freedom. This brings the so-called primitive rights into the sphere of legal rule and protection. Sometimes it is thought that lawful power or liberty is different from the right not to be interfered with; but for the reason just given this opinion, though plausible, does not seem correct.

---

217 See Chesterman, supra note 5, at 1072.
218 See Buchan, supra note 63, at 84.
219 Id.
220 Wesley Newcomb Hohfeld, Fundamental Legal Conceptions 48, fn 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: “...it 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.”
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. Perhaps the habit of recognizing exclusively the latter as a jural relation springs more or less from the traditional tendency to think of the law as consisting of “commands,” or imperative rules. This, however, seems fallacious. A rule of law that permits is just as real as a rule of law that forbids... That this is so seems, in some measure to be confirmed by the fact that the first sort of act would ordinarily be pronounced ‘lawful,’ and the second ‘unlawful’.\(^{221}\)

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:

Suppose that I am irritated by people who smoke in my vicinity. I meet S (smoker) in a public place, who starts to smoke in my presence. I ask him to stop, but S tells me he has a ‘right’ to smoke here (given the absence of any legal prohibitions). S is confusing his entitlement. He does not have a right (in the Hohfeldian sense) to smoke, but merely a liberty (a weaker right). Although I have a no-right concerning his activity of smoking, I do have a liberty myself ... to impede his smoking, say, by raising my voice or encouraging other people to make fun of S for his smoking habit, which may make him stop... Hohfeld's analysis therefore provides a clear understanding as to what the legal position of S is (i.e. what rights he has). As we can see, had it not been for Hohfeld providing us with a precise vocabulary, S would mistake his liberty for a right, and accordingly would be unable to accurately report the effect of his entitlement. He would be wrong in saying to me that I cannot stop him from smoking because he has a right to smoke in a public place, since it puts me under no duty not to interfere with his smoking.\(^{222}\)

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, or smoke in your presence, but that right doesn’t create a duty on you to suffer the asphyxiating vapors of surveillance. In fact, you have the liberty to interfere with my spying by engaging in counter-espionage, enacting legislation, bringing criminal proceedings against my spies, or taking retaliatory diplomatic measures – declaring my diplomats persona non grata.

\(^{221}\) Id.

\(^{222}\) Nikolai Lazarev, Hohfeld’s Analysis of Rights: An Essential Approach to a Conceptual and Practical Understanding of the Nature of Rights, 9 MurUEJL (2005), at http://classic.austlii.edu.au/au/journals/MurUEJL/2005/9.html. 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” would open the door for custom around espionage to evolve as it will assist in the fulfillment of the elements required for the identification of custom under international law. Indeed, as of current state of drafting, consensus seems to be building at the ILC around a definition of opinio juris, the subjective element of custom, as encompassing a “sense of a legal right or obligation”.\(^{223}\) As the ICJ noted in the Military and Paramilitary Activities case “indications of a practice illustrative of belief in a kind of general right for States [to act a certain way]... [could involve] a fundamental modification of [...] customary law principle[s]”.\(^{224}\) If a sense of a legal right makes for opinio juris, then articulating States’ entitlement as a type of right becomes foundational to achieving those customary modifications that the ICJ describes.

Recall the Obama-Merkel spying scandal of 2013. When German Chancellor Angela Merkel learned of the fact that the U.S. was engaged in the monitoring of her devices and communications, she decided to expel a top U.S. official from the embassy in Berlin, and stated in a press conference that “Spying among friends — that is simply not done”\(^{225}\). She further proceeded to join hands with Brazil (whose leader was too a victim of American monitoring) to pass a U.N. General Assembly Resolution that sought to protect the right to privacy in the digital age and challenge mass surveillance.\(^{226}\) Of course 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.\(^{227}\) Even the pope was not immune from BND’s spying, nor were charities like Oxfam.\(^{228}\)

For those who argue against the regulation of espionage as a lex specialis customary field under international law this episode offers the perfect example of the cynicism that is part and parcel of 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 her activities were revealed, at which point Germany, as if on cue, began heckling and lampooning 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 making sport of 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 conventional wisdom. All countries spy, and all countries legislate against spying done unto them –

\(^{223}\) See Fifth Report on Identification of Customary International Law, Michael Wood, Special Rapporteur, UN Doc. A/CN.4/717, paras. 73, 76-77 (Mar. 14, 2018). Note that the United State “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 para. 73 fn. 207

\(^{224}\) Military and Paramilitary Activities, supra note 154, at 206.


and that makes perfect sense within a liberty right framework. All countries keep their spying the subject of plausible deniability and engage in a clever dance, the “spy block tango”, when caught red-handed. By doing so they tacitly accept the rules of the game, a set of “unexpressed but generally accepted norms and expectations”.

To my knowledge, the only other scholar to suggest thinking of spying through Hohfeldian lenses was Professor Chesterman. 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 makes the following claim after citing the provisions on “national technical means of verification” from both the ABM and SALT I reciprocal spying regimes:

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, discussed earlier, 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.

What Chesterman highlights is the fact that through bilateral and multilateral treaties we might be able to turn the liberty right to spy into a claim right (e.g. the Treaty on Open Skies above discussed) or alternatively be able to prohibit spying (e.g. the infamous No Spy Agreement that allegedly exists between the 5-Eyes Member States). In other words, through contracting we may be able to change the reciprocal expectations and affirm a new jural relationship around spying.

Moreover, it is important to clarify that treating governmental spying as a liberty right has logic only insofar as the interstate level is concerned. These rationales, however, don’t extend to the intrastate level. This is because the traditional Hohfeldian conceptualization of a liberty right (one has a liberty to do X when one has no duty not to do X) doesn’t apply to domestic surveillance activities where certain constitutional and administrative constraints apply as to the power of the state to surveil it own nationals.

---

230 Professor Fritz Allhoff in a 2006 Article on the Ethics of Torture had a footnote reference to Hohfeld’s categories of rights, though the analysis was far more limited to the question of the relationship between the torturer and the tortured and didn’t address interstate relations. See Fritz Allhoff, Ethical Defense of Torture in Interrogation, in Ethics of Spying: A Reader for the Intelligence Professional 126, 138, fn 9 (Jan Goldman (ed.), 2006).
231 See Chesterman, supra note 5, at 1091.
232 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 (10 October 2012), at http://www.cbc.ca/newsblogs/politics/inside-politics-blog/2012/10/from-the-order-paper-question-archives-do-the-five-eyes-watch-each-other.html. However, when Germany and France demanded to be included in the “no-spy” pact then President Obama insisted that the United States has no such arrangement with any country. See Zeke J. Miller, Obama: “There’s no country where we have a no-spy agreement”, Time (11 February 2014), at http://time.com/6398/obama-theres-no-country-where-we-have-a-no-spy-agreement/.
233 Ronald Edward Watson, Spying: A Normative Account of the Second Oldest Profession, A dissertation presented to the Graduate School of Arts and Sciences of Washington University in partial fulfillment of the requirements for the degree of Doctor of Philosophy (2013), at https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=2106&context=etd (suggesting that Countries have no “liberty (in the hohfeldian sense) to spy”, Watson relies only on a domestic surveillance example: “you 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.
Finally, the liberty right conceptualization of spying provides us an opportunity to take a broader look at the *Lotus* Case. Judge Simma's critique in the *Kosovo Advisory Opinion*, was that to leap from a lack of a prohibition directly to a permission “ignores the possible degrees of non-prohibition, ranging from ‘tolerated’ to ‘permissible’ to ‘desirable’”. While Simma suggested therefore that we should move away from *Lotus*, it is possible to also reconceive our understanding of the *Lotus* holding.

The doctrine need not be confused with the notion that that “every door is open unless it is closed by treaty or by established custom”. Rather *Lotus* could be read to suggest that every door is open unless your neighbor shuts it. Everything that is not expressly prohibited isn’t allowed, it is a privilege that a Sovereign may continue to enjoy until such time when another Sovereign loses interest in tolerating the behavior and develops the needed political power and resources to enforce against her. This understanding of *Lotus* might help us reintroduce the different “colour[s] of legality” that Judge Simma was so concerned about.

For example, returning to the original subject matter of the *Lotus* proceedings, we can concur with the PCIJ’s finding that the power of Turkey to extend its laws and jurisdiction to persons, property, and acts outside its territory is subject to a wide margin of discretion. Nonetheless, that discretion should not be confused with some claim-right that Turkey might possess, as there is no corollary obligation imposed on France to tolerate the gall of Turkish extraterritorial adjudication and enforcement in the High Seas. Quite the opposite, assuming for a moment that France had a way to get Monsieur Demons out of Turkish prison and into their possession, they would be under no obligation to enforce the judgment of the criminal court in Istanbul. This proves that the derivative extraterritorial jurisdiction of States to legislate, enforce, and adjudicate (derived directly from their claim right to sovereignty) is in fact a weaker privilege that those countries enjoy and that is subject to the same type of analysis proposed in this Article in the context of the right to spy.

V. THE LIMITS OF THE JUS AD EXPLORATIONEM

Acknowledging the existence of the right to spy is an important first step towards its 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 which recognized the legal maxim “*neminem laedit qui suo jure utitur*, meaning that nobody harms another when he exercises his rights.” The doctrine has since been recognized as a general principle of international law, and is commonly cited in the writings of publicists and in early cases of the PCIJ.

---


235 *Lotus*, supra note 22 (Dissenting Opinion of M. Loder, at 34).

236 Declaration of Judge Simma, *supra* note 234.

237 *Lotus*, *supra* note 22, at 19.


Professor Kiss suggested that in inter-State relations “the concept of abuse of rights may arise in three distinct legal situations”. For the purposes of this paper let me just address the first of these categories, 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.” This situation echoes the well-established concept of détournement de pouvoir (misuse of powers) in administrative law. Of course a difficulty arises in proving “intention.” As noted by G.D.S. Taylor:

[The fact] that a person is tempted to act in bad faith or otherwise abuse his rights does not invalidate the action taken. The action is invalid only if the abuse was integral to the action taken and led to it in some way. The reasons for the action must be bad... The necessary first step is 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... [W]here the reasons are not stated they must be inferred from the surrounding facts.

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.” Regardless of these important evidentiary difficulties, the doctrine nonetheless introduces a basic necessity requirement whereby a country is banned from exercising its right for purposes not authorized by the international community in the formation of the right.

Whenever abuse of rights is discussed, Lauterpacht’s sobering words about the needed delicacy in its application often follow:

These are but modest beginnings of a doctrine which is full of potentialities and which places a considerable power, not devoid of a legislative character, in the hands of a judicial tribunal. There is no legal right, however well established, which could not, in some circumstances, be refused recognition on the ground that it has been abused. The doctrine of abuse of rights is therefore an instrument which . . . must be wielded with studied restraint.

---

241 See Kiss, supra note 238, at para. 5.
242 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. As an example, Kiss notes the “inconsiderate use of . . . the radio-electronic spectrum,” whereby one of the two states sharing the spectrum will feel a reduction in their enjoyment of the resource because of the behavior of the other State. See Kiss, Id., para. 5. In those situations, Kiss concludes, a “balance of interests” test should be introduced in such a way that abuses will only be found in cases “when the injury suffered by the aggrieved States exceeds the benefit resulting for another State from the enjoyment of its own right.” Id. These cases involve a degree of “bad faith” or “an intention to do harm”. They are thus distinguished from the third category of cases whereby the reckless exercise of the rights of one State, causes injury to other States. Id., para. 6. While both these categories might have relevance for the purposes of the analysis of the JAE, I will constrain myself only to the first category for reasons of succinctness.
243 Id., at para. 5; see also García’s Report, supra note 240, at 8 (citing R. L. Bindschedler, La Protection de la Propriete Privee en Droit International Prive, in 90 Recueil Des Cours De L’Academie De Droit International 212-213 (1958)).
246 Hersch Lauterpacht, The Development of International Law by the International Court 164 (1958).
While these are important guidelines to remember, Crawford identifies one set of cases where the doctrine should be most utilized. These are cases where the doctrine “represents a plea for legislation or the modification of rules to suit special circumstances.”247 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. Given that the law on espionage is one that is characterized by 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 or privilege, in part because it is only a derivative of harder claim-rights (such as the rights of States for survival, the right of individual and collective self-defense, the right for collective security, the right to engage in discriminate and proportionate attacks in times of armed conflict – above discussed). 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 as plausible 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”. 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, which is one of the fundamental principles of the international legal order”.248 In other words, the Court identified the existence of an attorney-client privilege between States and their counsel based on the fact that it was necessary for the operationalization of the claim right to sovereign equality.

Indeed one thing that both Hobbes and Kant could agree on is the notion that a right to an end might trigger the right to the means necessary to achieve that very end. Hobbes noted that “it is in vain for a man to have a Right to the end, if the Right to the necessary means be denied him.”249 Kant similarly claimed that “whoever wills the end also wills (in so far as reason has decisive influence on his actions) the indispensably necessary means to it that is in his control”.250 Of course the right to an end does not mean the right to every possible means to achieve that end (which in our case will entail the Jus In Explorations constraints on the broader right to spy).

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”:251

---

247 See Brownlie’s Principles of International Law, supra note 239, at 562.
250 Immanuel Kant, Groundwork of the Metaphysics of Morals (1797) 127 (Mary Gregor and Jens Timmermann ed. and trans., 2012). This quote should be read in light of Kant’s broader understanding of personal rights laid down in The Science of Right in 1790. See Immanuel Kant, The Philosophy of Law: An Exposition of the Fundamental Principles of Jurisprudence as The Science of Right 100 (W. Hastie trans., 1887).
251 See Oona A. Hathway and Scott Shapiro, The Internationalist: How a Radical Plan to Outlaw War Remade the World 97, 304 (2017)
Grotius’s system had rules governing conquest, criminal liability, gunboat diplomacy and neutrality. As we can see, Lauterpacht’s rules were the same as Grotius’s except in one simple respect: They were the opposite. … The legacy of Hersch Lauterpacht was nothing less than a system of rules embodying the idea that war is an illegitimate tool for establishing or enforcing legal rights. Now, there would only be one way for states to get what they wanted from other states – they had to offer those states something that they wanted in return. Compulsion by war was over. The era of global cooperation had begun.252

Missing from their review was an analysis of the way the shift to the new world order impacted the old Westphalian right to spy. I argue that what we’ve witnessed is a dual effect – both a shift towards an expansion in utilization while at the same time limiting the scope of circumstances justifying operation.

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. This is echoed in Christopher Baker’s Functional Approach: “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.”253 Anecdotally, one can certainly cite to the Cold War as proof of the intensification of spying in the post-Charter era. 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.254

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 were teased out, tested, perfected, and eventually solidified.255

Going back to our sources of the derivative right to spy it becomes clear that there are two possible ways to justify acts of espionage in the new world order (two Just Causes if 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:

No one wants another Pearl Harbor. This means that we must have knowledge of military forces and preparations around the world, especially those capable of massive surprise attacks. Secrecy in the Soviet Union makes this essential. In most of the world no large-scale attack could be prepared in secret, but in the Soviet Union there is a fetish of secrecy and concealment. This is a major cause of international tension and uneasiness today. Our deterrent must never be placed in

---

252 Id., at 305.
253 See Baker, supra note 49, at 1110, 1112.
255 Joseph R. Soraghan, Reconnaissance Satellites: Legal Characterization and Possible Utilization for Peacekeeping, 13(3) McGill. L. J. 458, 471-472 (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 around in the wake of the U2 spy plane incident and MIDAS, only to be rejected with the ultimate adoption of SALT I and ABM which solidified the notion that spying from outerspace was tolerated even by the Soviets).
jeopardy. The safety of the whole free world demands this. As the Secretary of State pointed out in his recent statement, ever since the beginning of my administration I have issued directives to gather, in every feasible way, the information required to protect the United States and the free world against surprise attack and to enable them to make effective preparations for defense.256

James Baker while summarizing Reisman had identified three goals for the intelligence function in the world public order: (1) intelligence should inform decision (which improves decision); (2) intelligence offers a source of stability in maintaining international public order; (3) intelligence should guard against surprise.257 I completely agree with both Baker and Reisman’s analysis but based on my review of the sources I simply collapse goals one and three together.

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 is not to be confused with a Garrison State Machiavellian notion of power maintenance.258 If we merely accepted as fact that princes truly had “no other aim or thought, [nor did they] take up any other thing for [their] study, but war and its order and discipline”259 then any act of government could potentially be painted with broad national security brushes and trumped up to the march of the cavalry. In other words, an overtly expansive understanding of national security will result in the term 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”.260

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”.261 This definition of national security, adopted by the Centre for Law and Democracy in the context of States’ disclosure obligations in national security cases, 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. This particularly

257 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).
258 Harold D. Lasswell, The Garrison State, 46(4) Am. J. Soc. 455 (1941) (Lasswell considers in this article the possibility that we are moving toward a world of “garrison states” in which the specialists of violence are the most powerful group in society).
259 Machiavelli, supra note 46, at 57.
applies to those less articulable threats (the “unknown unknowns”) that intelligence agencies are tasked with thwarting within the fogger environment of foreign espionage.

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, and 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, but spying to advance 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.

The national security test thus inevitably introduces grey zones where rule-appliers are likely to face significant hurdles in reaching consensus over any 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 be the basis for a rejection of the test wholesale. After all in international law we are familiar with such controversial rules and have learned to deal with them. Consider the principle of proportionality under the Geneva Conventions and Additional Protocols. In applying the principle we are likely to find that a small group of cases might easily and conclusively be determined as proportionate or disproportionate, but then there will be a large middle group of “close cases” where (if to paraphrase the ICTY’s Expert Committee) not even two military commanders could reach any consensus.

Perhaps an even better example may come in the context of the right for anticipatory self-defense against imminent threats, above discussed. Bethlehem had noted that “there is little scholarly consensus on what is properly meant by “imminence” in the context of contemporary threats”. While that is certainly true, “at the same time we must recognize that there may well be situations in which the imminence of an attack is so clear and the danger is so great that defensive action is essential for self-preservation of a state”. Again, we shall see a small set of threats that the common sense of most would treat as sufficiently imminent thereby justifying the use of force or sufficiently amorphous thereby prohibiting recourse to armed violence – but the far larger grouping of threats would be “in the middle” cases that would only trigger hours of interpretive debate providing permanent employment to scores of governmental lawyers, human rights advocates, and legal thinkers. However, this innate complexity within the normative enterprise, common to so many fields of practice in international law, should not be the basis for the enterprise’s rejection.


264 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. The German law speaks of “intelligence that is important for foreign and security policy” and the French law speaks of intelligence necessary to defend and promote “France’s major interests in foreign policy, the implementation of the European and international commitments of France, and the prevention of all forms of foreign interference”. For further reading, see Asaf Lubin, A New Era of Mass Surveillance is Emerging Across Europe, Just Security (Jan. 9, 2017), at https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/..


266 See Bethlehem, supra note 144, at 5.

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 surveiling State’s needs could be articulated in national security terms. For those who believe that introducing such a national security test into the law of espionage would result in an over-expansion of the term by intelligence agencies to a point of collapse – one needs 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):

1) external military threats to the country, 2) conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations, 3) strategic circumstances concerning international terrorism or other serious cross-border crimes that may threaten essential national interests, 4) the development and proliferation of weapons of mass destruction, military equipment and other similar specified products, 5) serious external threats to society’s infrastructure, 6) foreign conflicts with consequences for international security, 7) foreign intelligence operations against Swedish interests, and 8) the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy.268

Here you have it. A country has translated the term “national security” into a specific set of eight well-articulable and reasoned categories of legitimate spying. It is true that categories 2, 3 and 8 might fall into the gray area in our above spectrum for lacking sufficient specificity or stepping outside the scope of pure and core national security concerns. That, however, does not entail a collapse of the 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”.269 Examples of such spying operations, have been already discussed above, and may include *inter alia* the gathering of information and its disclosure to the Security Council prior to a vote authorizing the use of force, intelligence gathering in relation to counter-proliferation, arms control and sanctions regimes, providing intelligence in assistance of blue helmet...

---

269 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* 442-445 (Hague Academy of International Law, 2012). Reisman defines the principle of minimum order as the “sine qua non for all other goals” in our legal system. *Id.* at 442. On the basis of this principle we may appraise “past and prospective arrangements and prospective decisions concerning security, not in terms of the interests of a single participant or group of participants but in terms of everyone’s security.” *Id.* at 443 (emphasis in original). Minimum order entails both “a low expectation of violence” as well as the “avoidance of surplus violence.” *Id.* at 442, 445 (emphasis in original).
peacekeeping operations and humanitarian aid missions, and supporting ongoing investigations by international courts, tribunals, and fact-finding missions.

B. The Application of the Just Causes

Both national security and international security, as two justifications of espionage operations, are of equal strength, and most often their application will converge. For example if Germany were to launch a surveillance operation on DPRK’s nuclear program, 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, such spying might serve the national security interests of those States but run counter to the interests of the international community in maintaining either a perception or a reality of 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.

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, political independence, 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 our public world order. Note that this position was suggested, though ultimately not adopted, by a minority of the experts in Tallinn Manual 2.0:

A few of the experts were of the view that the extensive state practice of conducting espionage on the target State’s territory has created an exception to the generally accepted premise that non-consensual activities attributable to a State while physically present on another’s territory violate sovereignty. They emphasized, however, that this exception is narrow and limited solely to acts of espionage.271

This confirms that the relativist accounts that link legality and illegality to territoriality or to the privileges enjoyed by the targets of that surveillance, are adopting the wrong approach. 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.

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 intentional 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

270 See Bright and Beaumont, supra note 79 and accompanying text.
271 See TM 2.0, supra note 12, at 19. See also Schmitt, supra note 97, at 5 fn. 28 (“Some of the experts opined that the widespread practice of conducting espionage while abroad, although a violation of the target State’s domestic law, creates a “carve out” in the law of sovereignty and therefore does not, in and of itself, amount to a sovereignty violation”).
directly dependent on questions of intentionality. As noted by Christopher Baker: “the lawfulness of a particular act of spying may depend on the sponsor state's motivation. If the information sought "contributes to defensive rather than aggressive policies of national defense," the act of espionage arguably would claim greater legitimacy under international law.”

Spying is 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. Spying within the permissive structures of the ILI will involve only those operations that are done in the name of either of the two just causes and which are launched with the right intention. On the other hand spying which seeks to achieve other means, of any kind, will be deemed impermissible and abusive.

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 flows downstream; but when the gates stay 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 is likewise open. 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 and the action is thereby made illegal.

Below I have identified the five most salient categories of ends which I believe clearly fall outside the permissive structures, and therefore will not be “stomached” or tolerated by the international community. This is not an exhaustive list but one that, so it is hoped, could allow us to begin a conversation as to the legal line drawing of the JAE. 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.”273 Dubbed by the media as the Czech “femme fatale”274 she was convicted for her involvement in a national spy scandal worthy of a bestselling novel. According to the indictment, in 2012 while she was serving as the Chief of Staff to then Prime Minister Petr Nečas, the two began having a romantic affair, all behind the back of the latter’s wife, his high school sweetheart Radka Nečasová. 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 some unsubstantiated 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.275

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 Nečas to resign. Prague district court judge Pavla Hájková wrote in her guilty verdict that

---

272 Baker, supra note 49, at 1097. See also Falk, supra note 11, at 58.
the main motivation prompting the criminal conduct of the accused was “her deep hatred” towards the PM’s wife.276

Now consider the reports that President Trump contemplated a proposal made by Blackwater founder, Erik Prince, for the establishment of a “global private spy agency”. The network would have utilized “an army of spies with no official cover in several countries deemed “denied areas” for current American intelligence personnel” and served the purpose of circumventing official U.S. intelligence agencies thereby “countering “deep state” enemies in the intelligence community seeking to undermine Donald Trump’s presidency”.277 Imagine, for the sake of the argument, that this scenario had materialized and that President Trump were to utilize this private spy ring to surveil foreign nationals who brought legal challenges against his businesses in foreign jurisdictions or those foreigners who were cooperating with the Muller investigation into possible collusion with Russia during Trump’s campaign for presidency.278

Both these acts of espionage, the real Nagyová scandal and the fictional Trump scenario, are clear violations of domestic administrative and constitutional laws. Under my analysis of the right to spy, however, these acts would additionally trigger a separate violation of international law. Both of these operations were not launched in service of either the national security of the Czech Republic or the U.S. (regardless of whether the accused would try to tell a different story) nor are they done in the service of international peace and stability. These are both examples where national resources are devoted towards the gathering of intelligence for the purposes of advancing personal interests of particular political figures. 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.279 The reasoning behind this prohibition is rooted in an understanding that the right to spy belongs to the collective, not to any particular ruling elite. As clarified further by Jones:

[W]hat is morally acceptable behavior for the government in protecting the nation as a whole may not necessarily be acceptable for the individual; in fact, quite the opposite may be true. 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.280

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

On the night of 22–23 February 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".

276 See Jůn, supra note 273.


278 It is important to note that officials clarified that "the idea was going nowhere" and that "the White House does not and would not support such a proposal". See Jim Sciutto and Zachary Cohen, US official: Erik Prince proposed private spy network to Trump administration, CNN (Dec. 5, 2017), at https://www.cnn.com/2017/12/05/politics/erik-prince-private-spy-network-trump-administration/index.html.


280 See Jones, supra note 45, at 41.
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 then formally annexed by Moscow on 18 March, triggering international condemnation”.281 It is safe to assume that in the days leading up to the forcible 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.282 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”)283 and *ex injuria jus non oritur* (“law does not arise from injustice”)284 both reflect a deep-seeded moral commitment according to which “a right cannot stem from a wrong”.285 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. This alone, would explain why any spying conducted in the immediate and necessary service of an act of aggression or annexation or in material preparation for a crime against humanity, naming but a few examples of clearly wrongful acts, must be deemed unlawful as well.

I am willing to entertain an additional related claim. 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 necessarily 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 considered an extension of the wrongful act and therefore unlawful.

Consider for example the crime of Genocide. It requires 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”.286 A constitutive element of the crime of genocide is thus a meticulous planning and preparation involving all of the organs of the State, including its intelligence arm.287 You couldn’t conceive of the demonic plot to round up all the Jews and rush them on the

---


287 See Trial of the Major War Criminals before the International Military Tribunal, Nuremberg, 14 November 1945 - 1 October 1946, vol. XXII, at 226 (1948) (“We are dealing in this Trial not with the murder of 10 men here or 20 there. In this Indictment is charged not only the murder of millions but a demonic plan of genocide, of the planned murder of
death trains to the killing centers in Auschwitz, if you didn’t have the Sicherheitsdienst (SD, the intelligence agency of the SS) and the criminal police and the Gestapo engaging in all of the prerequisite 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. The intelligence operation is thus wrongful twice over: first because it lacks a legitimate source from which to derive its legality, but second (and more egregiously), it forms 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 restraint” to be applied by U.S. intelligence agencies in the course of their routine foreign SIGINT gathering. 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 partners and allies. Similarly the 2016 German Foreign Intelligence Law prohibited the gathering of foreign information for the purpose of achieving “competitive advantages (industrial espionage)”. 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. 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.

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. 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

---

288 Id., at 340-341, 346-347.
290 Id.
291 President Barack Obama, Presidential Policy Directive/PPD-28—Signals Intelligence Activities (Jan. 17, 2014), at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. 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”.
294 See TM 2.0, supra note 12, at 169, fn 386.
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.296 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.

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.297

Note that my comments don’t address competitive intelligence, corporate-corporate industrial espionage, even if it carries with it a transnational element (e.g. an employee of a German company steals blueprint designs and sells them to a competing firm in Italy; a Dutch firm removes 10,000 pages of documents from a dumpster on its Canadian competitor’s property).298 These are domestic crimes between private entities lacking the involvement of or nexus to States necessary to trigger the ILI.299 As such the vast majority of acts of theft of intellectual property, private appropriation of foreign-created intellectual goods, cybercrime, the stealing of trade secrets and technological know-how, and piracy and counterfeiting – should not be understood to be acts of espionage as the term is defined under this Article. This is true, even in those rare occasions where the activities might result in certain international legal obligations under trade or intellectual property regimes on the part of the State in whose territory the perpetrators are registered.300

4. Spying as a Means to Facilitate a Dictatorship

Twice a month when the tides are right Korean activists “toss hundreds of bottles into the Han River to be carried downstream in the hope that some will end up in the hands of North Koreans,

296 Id., at 4.
297 Hedieh Nasheri, Economic Espionage and Industrial Spying 12 (2005). See also Volkman, supra note 4, 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 reversed engineered and mass produced to support the British royal army).
298 For further reading about the ethics surrounding competitive intelligence gathering see Linda K. Trevino & Gary R. Weaver, Business: Ethical Issues in Competitive Intelligence Practice, in 1 Ethics of Spying, supra note 45 at 343; Darren Charters, Business: The Challenge of Completely Ethical Competitive Intelligence and the “CHIP” model, in 1 Ethics of Spying, id., at 362.
299 More complicated are cases where either the spy or spied are a state owned enterprise (SOE) and where the technologies being poached are of dual use. In those scenarios its harder to determine whether the necessary direction and control requirements were met, especially when there are multiple companies down a chain or corporate veils.
300 This distinction is also in line with the Economic Espionage Act, 18 U.S. Code § 1831 (1996) which defines the crime of economic espionage as an offense where the perpetrator intends or knows that his actions will “benefit any foreign government, foreign instrumentality, or foreign agent”. Foreign instrumentality is defined as “any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government”. For further reading see Hedieh Nasheri, Economic Espionage and Industrial Spying 12 (2005).
who are hungry for both food and information”. The bottles are filled with rice, worm medicine, and USB sticks containing videos and songs censored by the regime in Pyongyang.\textsuperscript{301}

Imagine a group of DPRK operatives instructed to collect intelligence about the activists and their operations, as well as monitor the river and recover any bottle they see. They are told that the regime, which is built on an Orwellian system of public oppression, misinformation, starvation, and fear,\textsuperscript{302} considers these bottles to be subversive and treasonous. Should we deem such a surveillance operation lawful? In defining lawful espionage, leaders need not conflate the national security interests of the State with their own individual interest in protecting their seat in power. As a first step towards the ultimate eradication of dictatorships as a form of legitimate governance in international affairs,\textsuperscript{303} we must better articulate the law that controls the means that these dictators employ to sustain their atrocities. Spying in such a scenario cannot be objectively argued to serve the national security of the State, regardless of whether the controlling party believes it does.

Of course it is worth noting that international law lacks a precise definition of dictatorial regimes. As Posner and Vermeule had noted:

> The term is slippery in a family-resemblance sort of way, with many competing definitions and a great deal of vague usage. One recent treatment distinguishes “tinpot” dictators, who maximize personal consumption, from “totalitarian” dictators, who maximize power. In general usage, “dictatorship” takes many forms. In one version, dictatorship is the endpoint of a continuum that runs from fully autocratic rule by one person alone, through oligarchy, to democracy. In this version, talk of democratic dictatorship, or perhaps even constitutional dictatorship, would be oxymoronic. In another version, dictatorship refers to the nature of the policies that government institutes; a “democratic” or populist government that violated civil liberties and arbitrarily confiscated property could coherently be called dictatorial. A third theme, especially pronounced in Anglo-American discourse, focuses on the executive and equates dictatorship with unchecked executive power, in which case legislative dictatorship would be the oxymoron.\textsuperscript{304}

It could very well be that the only working definition of a dictatorship is one that is so narrow that it covers only those regimes that engage in different forms of genocide and other gross human rights abuses and acts of cruelty. If that is the case, surely the prohibition on espionage as a means to facilitate a dictatorship becomes redundant, as it would be subsumed by the broader prohibition on spying as a means to commit an internationally wrongful act introduced above. I leave this matter open for others to elaborate on.

---


Finally, consider the Australia-Timor Leste spy scandal. In 2004 Australia mounted a spying operation to gather information about the negotiating positions of its extremely poor neighboring country, Timor Leste. Australia sought to rely on the information it collected to rip its neighbor off 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.305 When

As part of a provisional measures application before the ICJ, Timor Leste’s submitted a memorial that began by detailing its history of colonization first in the hands of the Dutch and Portuguese and later under the control of Indonesia.306 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. This is a treaty which Timor Leste considers an infringement of its people’s right of self-determination, its territorial integrity, and right of permanent sovereignty over its natural resources.307 The memorial introduces all of this on purpose to highlight what it calls a “tragic story” and to exemplify “Australia’s role therein”.308

This exposition is important because it puts the Australian spying operation during treaty negotiations and later seizure of certain documents and electronic data from Timor-Leste’s legal counsel into context. Australia’s intelligence gathering, which launched this episode, cannot be justified through either a substantiated claim of national security needs or an argument surrounding the enhancement of collective security. Quite the opposite, Australia’s spying was a destabilizing act, serving the sole purpose of weakening an already fragile government in dire need of economic resilience, all in the name of enriching the treasury of a regional superpower. 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 subjugation, domination, and exploitation constitutes a denial of fundamental human rights, contrary to both the United Nations Charter and the promotion of peace and cooperation.309 Spying of this nature thus does not serve the purposes for which the right to spy was introduced, and should be considered an abuse of a State’s intelligence powers.

VI. CONCLUSION


306 See Memorial of the Democratic Republic of Timor Leste, supra note 248, at paras. 2.5-2.17.

307 On 22 February 1991, Portugal commenced proceedings against Australia before the ICJ for these infringements. The Court found that it could not exercise the jurisdiction conferred upon it, because of the absence of Indonesia from the proceedings. See Case concerning East Timor (Portugal v. Australia), Judgment, ICJ Reports 1995, p. 90, at paras. 10, 38.

308 See Memorial of the Democratic Republic of Timor Leste, supra note 248, at para. 2.10.

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.\(^{310}\) 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. It is truly the walking and berating version of the grand old game of kings and philosophers, or as Charles Buxton put it, “in life, as in chess, forethought wins”.

More than anything, I hope this article could serve as a call for action, inviting practitioners and international scholars to join the effort of thinking creatively in tackling existing blindspots around the regulation of spycraft. Cicero said that *nec arma enim silent leges* (when the cannons roar the muses are silent). A group of brave lawyers proved him wrong when they launched the campaign to regulate war which culminated with the adoption of the Hague Regulations, Geneva Conventions, and Additional Protocols. We are now being indoctrinated into thinking that when the spies connive the laws fall mute. It didn’t make sense at the time of Cicero; it certainly should not make sense to us now.

We should reject the forces of intellectual stagnation and speak up against what Íñaki Navarrete aptly called the “Politics of Silence.”\(^{311}\) 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.

\(^{311}\) See Navarrete, *supra* note 62, at 17.