JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOL. 14 • NO. 1 • 2022 – 2023

A META-CRITIQUE OF FRONTIER SCHOLARSHIPS ON THE LAWS OF PEACETIME ESPIONAGE: TOWARDS A SYSTEMIC FRAMEWORK FOR *LEX SPECIALIS*

Yang Liu[*]

[*]Yang Liu, J.D. & L.L.M. in National Security Law candidate at Georgetown University Law Center. Special thanks to Professors James W. Zirkle for helpful comments and guidance on this project since its early stages in the *Strategic Intelligence and Public Policy* Seminar.

CONTENTS

I. Introduction 38
II. Three Traditional Approaches 42
1. States Practices 42
2. Self-defense 44
3. International Order 46
b. Espionage is Neither Legal nor Illegal but Per Se Permissible 48
1. Spies Are Not State Agents Under International Law 48
2. The Lotus Principle 49
3. International Cooperation 51
c. Espionage is *Per Se* Illegal 52
1. Espionage Violates Customary International Law 52
2. Espionage Violates Specific Treaties 54
3. Problems of This Approach 55
III. Frontier Theories and the Piecemeal Approach to Espionage 58
a. Craig Forcese's Method-based Approach 59
1. Summary of arguments 59
2. Analysis and Critique 61
b. Ashley S. Deeks's Harm-Based Approach 64
1. Summary of Arguments 64
2. Critique and the Need for an Ontological Turn 66
c. Asaf Lubin's Purpose-Based Approach 68
1. Summary of Arguments 68
2. Four Problems of Lubin's Approach 70
IV. A Dialectical Concept of Just Cause for Espionage that Explores Unknown Unknowns . 73
a. The Liberal World Order and a State's Duty to Have a Transparent Deliberation Process 74
b. The Historical Dimension of the Just Cause to Explore Unknown Unknowns 76
V. A Just Intelligence Framework for the *Lex Specialis* of Peacetime Espionage 77
a. From the Just War Tradition to the Just Intelligence Theory 77
b. Jus ad Explorationem 81
1. 1. Just Cause 81
2. Just Intention 82
3. Correct Authority 82

4. Macro-Proportionality 83
5. Other Factors 83
c. Jus in Exploratione 84
1. Discrimination 84
2. Micro-Proportionality 85
3. No Means or Methods *Mala in Se* 85
d. Jus post Explorationem 86
VI. Conclusion 86

I. Introduction

Espionage is often described as the world's second-oldest profession,[1] which is "as honorable as" the world's oldest profession, prostitution.[2] Sun Tzu's *The Art of War*, written in around the 5th century BCE, is one of the earliest written books discussing this profession.[3] In his book, Sun Tzu connected espionage with warfare and provided arguably the first systematic explanation of the different types of spies and the ways to effectively employ them to achieve one's military goals.[4] In early western civilization, espionage was also constantly discussed in the context of warfare. For example, the Bible recorded two instances where spies were employed: Moses sent spies to Canaan to investigate whether it is plausible to attack and win warfare against them,[5] and Joshua sent spies to Jericho to explore the weakness of their military and national defense.[6] Relying upon the stories of Moses and Joshua, Hugo Grotius, arguably the "father of international law,"[7] found wartime espionage to be *per se* legal under international law.[8] This view has been adopted by later scholars and international treaties. For example, the *Declaration of Brussels* of 1874,[9] the 1899 Hague agreements,[10] and the 1907 Hague rules[11] all considered espionage as a lawful means of warfare.[12]

---

[1] *E.g.*, William C. Plouffe Jr., *Just War Theory as a Basis for Just Intelligence Theory: Necessary Evil or Sub-Rosa Colored Self-Deception?*, 2 INT'L J. OF INTEL. ETHICS 77 (2011) [https://perma.cc/Q9BV-76P5].
[2] *See id.* citing Michael J. Barrett, *Honorable Espionage*, 2 J. DEF. & DIPL., 17, 13–14 (1984).
[3] SUN TZU, THE ART OF WAR 89-93 (Lionel Giles trans., 2014) [https://perma.cc/BSW6-6X7V].
[4] *Id.*
[5] Numbers 13.
[6] Joshua 2.
[7] HAMILTON VREELAND, HUGO GROTIUS, THE FATHER OF THE MODERN SCIENCE OF INTERNATIONAL LAW (1917).
[8] *See* HUGO GROTIUS, THE RIGHTS OF WAR AND PEACE 331 (A.C. Campbell, A.M., trans. 1901).
[9] Project of an International Declaration Concerning the Laws and Customs of War, art. 14, Aug. 27, 1874, 148 Consol. T.S. 133.
[10] Convention for the Pacific Settlement of International Disputes, July 29, 1899, 32 Stat. 1799.
[11] Convention (IV) Respecting the Laws and Customs of War on Land, art. 24, Oct. 18, 1907, 36 STAT. 2277.
[12] *See generally*, Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 332–37 (1996).

In contrast, the legal status of peacetime espionage under international law is ambiguous. On the one hand, most states engaged in, are engaging in and will keep engaging in espionage activities because espionage can serve vital national security interests—as W. Hays Parks puts it:

> [N]ations collect intelligence to deter or minimize the likelihood of surprise attack; to facilitate diplomatic, economic, and military action, in defense of a nation in the event of hostilities; and in times of "neither peace nor war," to deter or defend against actions by individuals, groups, or a nation that would constitute a threat to international peace and security (such as acts of terrorism).

On the other hand, all states regard foreign espionage activities as a threat to their national security and have domestic laws illegalizing and prohibiting other states from conducting intelligence activities within their territories. Thus, scholars often describe the legality of espionage as a "paradox."[14] As W. Hays Parks summarizes:

> "[D]omestic laws are promulgated in such a way to deny foreign intelligence collection efforts within a nation's territory without inhibiting that nation's efforts to collect intelligence about other nations. No serious proposal has ever 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."

Admittedly, regulating espionage under international law is challenging. As summarized by Ashley Deeks, there are at least five

---

[13] W. Hays Parks, *The International Law of Intelligence Collection*, *in* NAT'L. SEC. L., 433–34 (John Norton Moore & Robert F. Turner eds., 1999).
[14] *See* Demarest, *supra* note 12 (citing Maximilian Koessler, *The International Law on the Punishment of Belligerent Spies: A Legal Paradox*, 1958 CRIM. L. REV. 21); *see also* Myres S. McDougal, et al., *The Intelligence Function and World Public Order*, 46 TEMPLE L. Q. 365, 394–95 (1973).
[15] Parks, *supra* note 13, at 433–34.

obstacles.[16] First, intelligence activities "implicate a state's core national security interests."[17] Second, espionage activities are often hard to detect, so without reliable verification and safeguards, states are unwilling to be bound by agreements limiting espionage activities.[18] Third, even if a state wants to reach such an agreement, meaningful negotiation will be challenging as it might reveal its intelligence capacities.[19] Fourth, states have different espionage capacities, and states with a higher level of expertise often resist excessive regulations.[20] Fifth, there used to be little public pressure to regulate espionage because in the past espionage can seldomly affected average citizens directly.[21] For these reasons, it is understandable why international law scholars did not pay a lot of attention to espionage and did not really solve the paradox - as Radsan once pessimistically claimed: "[i]nternational law does not change the reality of espionage."[22]

However, from a normative perspective, the legal paradox of espionage must be resolved. The current ambiguous legal status of espionage is problematic because it fails to deal with and might even exacerbate what some scholars describe as the "liberal dilemma" of espionage - "[l]iberal states are dedicated to the protection of human rights but protecting the rights of their citizens may entail infringing upon or violating the rights of foreign citizens."[23]

Following the disclosure of the vital role espionage activities played in the U.S.-led coalition's decision to use force to overthrow the Iraqi government of Saddam Hussein by the U.S. Joint Congressional Inquiry,[24]

---

[16] Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 313–15 (2015) [https://perma.cc/3URN-E7BQ].
[17] *Id.* at 313–14.
[18] *Id.* at 314.
[19] *See id.* at 314–15.
[20] *Id.* at 315.
[21] *Id.*
[22] A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 623 (2007).
[23] Michael Skerker, *The rights of foreign intelligence targets* 89, *in* NAT'L SEC. INTEL. AND ETHICS (Seumas Miller, Mitt Regan & Patrick F. Walsh ed., 2022).
[24] *See* H. Permanent Select Comm. on Intelligence & S. Select Comm. on Intelligence, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, H.R. Rep. No. 107–792, S. Rep. No. 107–351 (2002).

the Australia Flood Commission report,[25] and the U.K. Hutton Report,[26] the past twenty years have observed a resurge of academic interests in the ethics and laws of espionage. Recently, some scholars have envisioned the need for and the plausibility of the *lex specialis* of peacetime espionage.[27] Considering such a background, my aim in this paper is threefold.

First, this paper will provide an overview of the three traditional approaches to the relationship between espionage and international law (espionage is *per se* legal, *per se* illegal, and neither legal nor illegal but *per se* permissible) and explain why they are no longer acceptable. Second, this paper will introduce recent scholarships advocating for a piecemeal approach to espionage (some but not all kinds of espionage activities are legal). Scholars advocating for this approach have proposed different tests to differentiate illegal espionage from legal espionage. This paper will explain why the approaches adopted by these scholars, although insightful, are neither ideal nor comprehensive. Lastly, this paper will propose a new framework for the *lex specialis* of peacetime espionage by incorporating the just intelligence theory, a frontier theory in intelligence studies. The biggest advantages of this paper's framework are threefold: (1) first, it illustrates why a state can conduct espionage to explore unknown unknowns or without specific causes, and (2) secondly, it preserves the pragmatism value of espionage in promoting transparency and the liberal world order, and (3) lastly, it incorporates the merits of other piecemeal approaches and thus is more comprehensive.

This paper will adopt the U.S. Army's definition of espionage as the conduct of intelligence collection by nation States against other nation States.[28] Sometimes this paper will use the terms espionage and spy interchangeably, but the focus of this paper is not limited to traditional spy activities or HUMANINT, instead, it will address espionage activities in general. However, other intelligence activities such as covert actions or

---

[25] *See* Philip Flood, Report of the Inquiry into Australian Intelligence Agencies (July 20, 2004).
[26] *See* Lord Hutton, Report of the Inquiry into the Circumstances Surrounding the Death of Dr. David Kelly C.M.G., U.K. House of Commons No. HC 247, (Jan. 28, 2004).
[27] *See* Asaf Lubin, *The Liberty to Spy*, 61 HARV. INT'L L.J. 185 (2020).
[28] NAT'L SEC. L. DEP'T, OPERATIONAL LAW HANDBOOK 209 (2020), https://tjaglcspublic.army.mil/documents/27431/37173/Operational+Law+Handbook+2020.pdf/b8630e95-cdf6-4205-a7ca-4cf842ad8dd3?version=1.3.

domestic surveillance for law enforcement purposes are not relevant to this paper's discussion.

II. Three Traditional Approaches

This section will introduce the traditional approaches to espionage. As many scholars have correctly summarized, traditional theories can be divided into three approaches, which regard espionage as, respectively, *per se* legal under international law, *per se* illegal under international law, and neither legal nor illegal but *per se* permissible.[29] While there are still many scholars who advocate for these approaches, with the development of modern espionage technologies, this paper argues that they are no longer acceptable.

a. Espionage is *Per Se* Legal

1. States Practices

To begin with, a group of scholars argues that espionage is *per se* legal under international law because of the widespread state engagements in espionage activities.[30] State practices alone, however, are not sufficient to legitimize espionage, as espionage can still be a constantly practiced illegal activity.[31] Thus, in supporting their arguments, these scholars have brought up some further arguments. And their approaches can be classified into two versions: a soft version and a hard-core version.

Scholars adopting the soft approach would rely on the so-called "clean hand principle."[32] The clean hand doctrine provides that "where two parties have assumed an identical or a reciprocal obligation, one party

---

[29] *See, e.g.*, Todd Emerson Hutchins, *Maritime Espionage and The Legal Consequences of The United States' Potential Ratification Of The United Nations Convention On The Law Of The Sea*, 8 NAT'L SEC. L.J. 1, 11–13 (2021); Lubin, *supra* note 27, at 187; Deeks, *supra* note 16, at 300–13; Radsan, *supra* note 22, at 602; Peyton Cooke, *Bringing the Spies from the Cold: Legal Cosmopolitanism and Intelligence Under the Laws of War*, 44 U.S.F. L. REV. 601, 609–10 (2010); M. E. Bowman, *Intelligence and International Law*, 8 INT'L J. INTEL. & COUNTERINTELLIGENCE 321, 328 (1995).

[30] *See, e.g.*, McDougal, *supra* note 14, at 394–95.

[31] *See, e.g.*, Quincy Wright, Comment, *The Pueblo Seizure: Facts, Law, Policy*, 63 PROC. AM. SOC. INT'L L. 1, 28–30 (1969).

[32] *See, e.g.*, Patrick C. R. Terry, *"Don't Do as I Do" - the Us Response to Russian and Chinese Cyber Espionage and Public International Law*, 19 GER. L.J. 613, 624 (2018).

which is engaged in a continuing nonperformance of that obligation should not be permitted to take advantage of a similar non-performance of that obligation by the other party."[33] Thus, even if espionage is not legal, since basically all states are "guilty" of conducting espionage activities, none of them can take advantage of and condemning another state's espionage activities.[34] Espionage can be said to be *per se* legal under this interpretation in the sense that any remedies or reliefs are *per se* unattainable. This argument, however, is weak. First, the clean hand doctrine is a "highly contentious doctrine."[35] The invocation of it in disputes between states has been severely criticized by many scholars and practitioners for "sacrificing the interests of justice at the altar of power politics."[36] Second, the clean-hand doctrine can only give rise to a court right – it cannot render any state's espionage activities legal but can only possibly preclude one state from suing another state for its espionage activities.[37] Thus, relying on the clean-doctrine is problematic because it does not address issues such as whether and when a state may conduct countermeasures against another state for its espionage activities. Besides, considering that the courts have constantly been reluctant to strictly interpret the clean-hand principle at the cost of justice and the integrity of the courts, its practical value as a court right is also suspicious.[38]

Scholars adopting the hard-core approach would argue that the prevalence of state practice has given espionage the status of customary international law.[39] More precisely, espionage can be viewed as a customary international law "exception" to other international law rules

---

[33] Diversion of Water from the River Meuse (Neth. v. Belg.), Judgement, 1937 P.C.I.J. (ser. A/B) No. 70, at 77 (June 28) (separate opinion by Hudson, J.).
[34] *See* Terry, *supra* note 33, at 624 (2018).
[35] Patrick C. R. Terry, *"The Riddle of The Sands" - Peacetime Espionage and Public International Law*, 51 GEO. J. INT'L L. 377, 412 (2020) (citing Int'l Law Comm'n, Second Rep. on State Responsibility, ¶¶ 332–36, U.N. Doc. A/CN.4/498 (1999)).
[36] Edward Gordon, *Discretion to Decline to Exercise Jurisdiction*, 81 AM. J. INT'L L. 129, 135 (1987).
[37] *See* James Crawford (Special Rapporteur on State Responsibility), Second Rep. on State Responsibility, ¶¶ 333-35, U.N. Doc. A/CN.4/498 (1999).
[38] *See Equity - Maxims - Clean-Hands Doctrine Held Inapplicable Although Fiduciary Duty Violated*, 60 HARV. L. REV. 980, 981 (1947).
[39] *See, e.g.*, Jeffrey H. Smith, *Keynote Address*, 28 MICH. J. INT'L L. 543, 544 (2007) ("[B]ecause espionage is such a fixture in international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law.").

and principles like sovereignty and nonintervention.[40] To be sure, this argument is not totally unreasonable. Customary international law can be established by the general practices of states and *opinion juris* (the subjective intention of states to be bound by such practices).[41] The requirement of general practices of states can be easily satisfied because few, if any, states are not engaging in espionage activities. There have already been several instances where government officials publicly recognized the legality of espionage, including former U.S. President Obama's 2014 remarks on signal intelligence.[42] Besides, these scholars cite the fact that some states have bilateral/multilateral treaties limiting espionage as an indication that these states regard espionage as *per se* legal in the absence of such specific treaties.[43] Even so, it is highly suspicious that *opinion juris* can be established by these sporadic statements, and it seems that most international law scholars have refused to find a customary international law exception to espionage.[44]

2. Self-defense

Another group of scholars would instead legalize espionage by referring to states' inherent right to self-defense,[45] which is both customary law[46] and codified in Article 51 of the U.N. Charter.[47] This approach was seen as early as Thomas Hobbes's theory, which regards espionage as a necessary component of all sovereigns' absolute "natural right" to self-defense.[48] However, the scope of this self-defense right in modern society, especially the right to anticipatory self-defense, has been less clear and

---

[40] *Id.*
[41] *See* Statute of the International Court of Justice, art. 38(1)(b), June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993.
[42] *See* President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *cited by* Deeks, *supra* note 17, at 609.
[43] *See, e.g.*, Deeks, *supra* note 17, at 303.
[44] *See, e.g.*, Iñaki Navarrete & Russell Buchan, *Out of The Legal Wilderness: Peacetime Espionage, International Law and The Existence of Customary Exceptions*, 51 CORNELL INT'L L.J. 897, 897 (2019).
[45] *See, e.g.*, Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 223–26 (1999).
[46] *See, e.g.*, Christopher M. Petras, *"Space Force Alpha": Military Use of International Space Station and the Concept of "Peaceful Purposes"*, 53 A.F. L. REV. 135, 176 (2002).
[47] *See* U.N. Charter art. 51.
[48] *See* THOMAS HOBBES, DE CIVE 62 (1642).

subject to intense academic debates.[49] For most international law scholars, there must exist an "imminent" threat of an armed attack for a state to successfully claim a right to anticipatory self-defense,[50] or such threat must not be "remote or constructive" but "fairly inferable from the preparations and intentions of the other party."[51] Thus, opponents correctly point out that the modern self-defense theory does not provide a justification for peacetime espionage activities, since they normally occur "well in advance" of an armed attack.[52]

In response, some scholars contend that espionage activities are "necessary to give substance and effect to the right of self-defense."[53] Considering the characteristics and destructiveness of modern weapons, a state can hardly exercise its self-defense right without effective intelligence gathering, as it would be too late to wait for the enemy to complete its first strike.[54] Thus, these scholars argue that even if the right to self-defense does not directly justify espionage, it presupposes it. And espionage activities can therefore be regarded as legal if they are conducted against states that "present clear, articulable threats based on their past behavior, capabilities, and expressions of intent."[55]

However, while self-defense can provide some justification for some specific kinds of espionage, it is unlikely to make espionage *per se* legal under international law. First, while self-defense can be invoked when conducting espionage against hostile or enemy states, it does not explain espionage between allies.[56] In practice, however, spying on allies is pretty "normal."[57] Some states conduct "economic espionage" to steal other

---

[49] *See generally*, Byard Q. Clemmons & Gary D. Brown, *Rethinking International Self-Defense: the United Nations' Emerging Role*, 45 NAVAL L. REV. 217 (1998).
[50] *See, e.g.*, Niaz A. Shah, *Self-Defense, Anticipatory Self-Defense and Pre-emption: International Law's Response to Terrorism*, 12 J. CONFLICT & SEC. L. 95, 99 (2007).
[51] *See* THEODORE D. WOOLSEY, INTRODUCTION TO THE STUDY OF INTERNATIONAL LAW (3d. ed., 1873).
[52] *See, e.g.*, Terry, *supra* note 33, at 624 (citing Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* 3 ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 21 (Quincy Wright *et al* eds, Leopold Classic Library 1962)).
[53] *See* Scott, *supra* at note 46, at 224.
[54] *Id.*
[55] *See id.* at 225.
[56] *See* Deeks, *supra* note 17, at 610 n.23.
[57] *See, e.g.*, Elisabeth Braw, *Spying on Allies is Normal. Also Smart.*, POLITICO (Jun. 4, 2021, 4:06 AM), https://www.politico.eu/article/spying-allies-normal-us-denmark/, [https://perma.cc/3YBT-F5JQ].

states' trade secrets and intellectual properties but the right to self-defense certainly cannot provide a justification for such activities.[58]

3. International Order

Lastly, some scholars argue that espionage should be *per se* legal because it is an indispensable component of the current international system. These scholars raise two kinds of arguments.

First, espionage is essential for international order because it can protect international stability and prevent wars.[59] On one hand, they argue that by conducting espionage activities, a state can preemptively learn of potential threats so that it can "take precautionary measures to prevent war."[60] On the other hand, these scholars adopt the view that wars are the results of bargaining failures.[61] They argue that war is always more costly than negotiations, thus, the most important reason that war can occur is the lack or imbalance of information between states.[62] Since espionage would allow states to gain more information about another state's strengths, these scholars argue that "more aggressive intelligence gathering can reduce the chances of [a] conflict."[63]

However, it is unrealistic to expect a state to have complete information about another state. It is one thing to argue that wars can be prevented when all states have complete information about each other. It is another thing to argue that where there is always incomplete and imbalanced information, more information, although incomplete, can always reduce the likelihood of armed conflicts. In any case, notwithstanding any of this argument's theoretical attractiveness, it is simply not supported by history. For example, the 2003 Iraq War is often

---

[58] *See, e.g.*, National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (2018), [https://perma.cc/X3MT-P7T3].
[59] *See, e.g.*, Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 633–35 (2007).
[60] *See id.* at 633.
[61] *See id.* at 634 (citing John Yoo, *Force Rules: U.N. Reform and Intervention*, 6 CHI. J. INT'L L. 641 (2006); Jide Nzelibe & John Yoo, *Rational War and Constitutional Design*, 115 YALE L.J. 2512 (2006)).
[62] *See* Sulmasy, *supra* note 60, at 635–36.
[63] *See id.* at 636.

viewed as a result of, or at least was promoted by an intelligence failure.[64] And while a majority of western countries were able to detect Putin's intention to invade Ukraine, such intelligence was limited to helping Ukraine better prepare for defending against Russian invasion, but could not aid in the prevention of warfare.[65]

The second argument is that many international institutions require the input of information gathered by states through espionage activities to fulfill their obligations.[66] For example, intelligence procured by states is needed by the U.N. to assist its decision-making,[67] by the IAEA to monitor states' nuclear activities,[68] by the WHO to investigate epidemics,[69] and by international criminal tribunals to prosecute war crimes.[70] Thus, as summarized by Asaf Lubin:

From disarmament obligations to counter-terrorism efforts, and from running effective sanctions regimes to providing assistance in disaster relief and humanitarian crises, there isn't an area of work within the broader umbrella of "collective security" that doesn't require such information [collected by states through espionage].[71]

Indeed, like self-defense, international security constitutes a valid and core reason that some types of espionage activities can be justified. On the flip side, just like the self-defense argument discussed above, international security alone cannot render espionage *per se* legal under international law. Because, for example, it also fails to address espionage

---

[64] *See, e.g.*, *MI6 ran 'dubious' Iraq campaign*, BBC NEWS (Nov. 21, 2003, 9:00 PM), http://news.bbc.co.uk/2/hi/uk_news/3227506.stm[perma.cc/A8YH-5XVR].
[65] *See* Neveen Shaaban Abdalla et al., *Intelligence and The War In Ukraine: Part 1,* WAR ON THE ROCKS (May 11, 2022), https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/ [perma.cc/HEP2-ZKN7].
[66] *See* Hutchins, *supra* note 30, at 15–16; *see also* Lubin, *supra* note 28, at 217–220.
[67] *See, e.g.*, Kees Garos, The All Source Information Fusion Unit: A New Phenomenon in UN Intelligence (Apr. 30, 2015) (M.S.S. thesis, Breda University), https://www.stichtingargus.nl/bvd/publicaties/garos.pdf.
[68] *See* OFFICE OF TECH. ASSESSMENT, NUCLEAR SAFEGUARDS AND THE INTERNATIONAL ATOMIC ENERGY AGENCY 5 (1995).
[69] *See generally* World Health Org., WHO Report on Global Surveillance of Epidemic-prone Infectious Diseases, U.N. Doc. WHO/CDS/CSR/ISR/2000.1 (2000).
[70] *See, e.g.*, MARGARET MIKYUNG LEE ET AL., BOSNIA WAR CRIMES: THE INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA AND U.S. POLICY 24 (1998).
[71] Lubin, *supra* note 28, at 218.

activities that cannot promote international security, like economic espionage.

Thus, it seems improper to regard espionage as *per se* legal under international law. Although scholars advocating for such an interpretation have provided some insights into the value of espionage activities, they have failed to provide sufficient reasons why no espionage activities are illegal.

b. Espionage is Neither Legal nor Illegal but Per Se Permissible

The second traditional approach regards espionage as neither legal nor illegal but *per se* permissible.[72] More precisely, scholars advocating for this approach argue that international law has nothing to do with espionage, which "as a legal field, is devoid of meaning"[73] because, *inter alia,* whereas international law is premised upon peaceful resolution of conflicts, espionage is rooted in "treachery and deceit."[74] From a practical perspective, this approach is like the first approach in that it would give states almost an unfettered right to conduct espionage activities. In fact, the line between these two approaches can sometimes be blurred, and many arguments discussed in the previous section are also often raised by this group of scholars. For example, the prevalence of state espionage activities is often cited as a reason why spies should be permissible even if not *per se* legal under international law. But what sets this group of scholars apart is their view that international law has and/or should have gaps, and espionage belongs to a gap thereof.[75]

1. Spies Are Not State Agents Under International Law

The famous German jurist Lassa Francis Lawrence Oppenheim has made the argument that spies have "no recognized position whatever according to international law."[76] Thus, on the one hand, spies can be

---

[72] *See, e.g.*, Radsan, *supra* note 23; Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1094 (2004); L. OPPENHEIM, INTERNATIONAL LAW § 455, (Hersh Lauterpacht ed., 1955).
[73] *See* Lubin, *supra* note 28, at 196.
[74] *See* Radsan, *supra* note 23, at 596.
[75] *Id*.; Sulmasy, *supra* note 60, at 626 ("The very notion that international law is currently capable of regulating [peacetime] intelligence gathering is dubious.").
[76] Oppenheim, *supra* note 73, at 862.

punished or expelled, and they cannot excuse themselves by claiming that they are only executing the orders of their governments because they do not enjoy the status of agents of states.[77] On the other hand, the activities of spies would not be imputed to states employing them, and therefore it is permissible for a state to conduct espionage activities.[78]

Oppenheim's argument has not been echoed by many scholars for good reason. First, Oppenheim seems to regard international law as simply an instrument managing the relationship between sovereigns. With the development of human rights and humanitarian laws, such jurisprudence of international law is no longer accepted. Besides, because of his jurisprudence, Oppenheim differentiates a spy from an official diplomat who is engaging in espionage activities.[79] The latter is not only permitted to espionage but also is legally protected from being punished for their activities.[80] Considering that many modern espionage activities operate remotely through official state institutions, the practical value of Oppenheim's approach is no longer significant.

2. The Lotus Principle

Most of today's scholars argue that espionage is neither legal nor illegal but *per se* permissible under the so-called "Lotus principle,"[81] which is arguably one of the "landmarks of twentieth-century jurisprudence."[82] The Lotus court held that "[r]estrictions on the independence of States cannot . . . be presumed."[83] Thus, according to the Lotus principle, all states are free to do whatever is not specifically prohibited by international law.[84] Relying upon this principle, these scholars argue that espionage is

---

[77] *See id.*
[78] *See id.*
[79] *See id.*
[80] *See id.*
[81] *See* S.S. Lotus (Fr. V. Turk.), Judgment [1927] P.C.I.J. (ser. A) No. 10 at 64 (Sept. 7) [hereinafter Lotus].
[82] Hugh Handeyside, *The Lotus Principle In ICJ Jurisprudence: Was The Ship Ever Afloat?*, 29 MICH. J. INT'L L. 71, 71 (2007) (quoting Louis Henkin, *International Law: Politics, Values and Functions*, 216 RECUEIL DES COURS 9, 278 (1989 IV)).
[83] Lotus, 1927 P.C.I.J. (ser. A) No. 10, at 18.
[84] *See, e.g.*, Tawia Ansah, *War: Rhetoric & Norm-Creation in Response to Terror*, 43 VA. J. INT'L L. 797, 850 n.180 (2003).

permissible because there are no specific international law prohibitions on espionage.[85]

However, this argument is unpersuasive. First, it is likely that this view misinterprets or misapplies the Lotus principle. The majority in Lotus not only cited existing international law rules but also customary international law.[86] Whereas there are no specific rules prohibiting espionage, it is a fundamental customary law that a state's sovereignty should be respected.[87] Since at least some kinds of espionage activities will unavoidably infringe on another state's sovereignty, the Lotus principle does not support the view that espionage is *per se* permissible. To be sure, one might reply that whereas specific espionage activities can be impermissible, espionage can nevertheless be *per se* permissible. Put another way, it might be argued that when a state finds a particular espionage activity to be illegal under international law, the reason is unrelated to the fact that this activity is an espionage activity; instead, the reason is that this activity, regardless of whether it is an espionage activity, violates existing rules or customary law. It is not clear whether scholars advocating for the view that espionage is *per se* permissible would be interested in making such a concession because doing so would sacrifice one of the biggest advantages of this approach – a state's unfettered liberty to espionage under international law. But if such a concession is made, from a practical perspective, this approach would be similar to, if not identical to, the first piecemeal approach, which will be addressed in further detail in Part III.A.

Second, relying on the Lotus principle is also problematic because the Lotus principle is no longer regarded as a commonly agreed principle of international law.[88] One severe problem lies in the principle's "vagueness and generality,"[89] which renders it hard to be applied.[90] More critically, the majority in Lotus failed to differentiate "rules" and "principles" and used these two terms interchangeably.[91] When Lotus was

[85] *See, e.g.*, Gary D. Brown, *The Fourteenth Annual Sommerfeld Lecture: The Wrong Questions About Cyberspace*, 217 MIL. L. REV. 214, 223 (2013).
[86] *See* Lotus, 1927 P.C.I.J. (ser. A) No. 10, at 30.
[87] *See* JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 448 (8th ed. 2012).
[88] *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 301 (6th ed. 2003).
[89] *Id*.
[90] *See* Handeyside, *supra* note 83, at 71 (discussing several different interpretations of the Lotus principle).
[91] *See id.* at 77.

decided in 1927, the jurisprudence of international law was dominated by "idealistic" positivism. Hence, the majority's equating of principles with rules did not cause too much confusion and criticism at that time.[92] However, since the 1960s, a policy-oriented contextualist approach has been developed and gained a lot of support from the community of international law scholars.[93] With the rise of contextualist jurisprudence such as the New Haven School of International Law, it is no longer proper to treat "principles" as "rules."[94] Instead, when there are no specific rules regarding a particular activity, many scholars today would refer to principles to fill the gap and without rigidly following the Lotus principle or easily accepting the incompleteness of international law. Thus, the Lotus principle can no longer serve as a solid intellectual footing in discussing the legality of espionage.[95]

3. International Cooperation

Besides the previous two positive arguments, there is also a normative argument on why international law should have gaps and why espionage should be an extralegal construct. Building upon the functionalism theory of international relations,[96] Christopher D. Baker argues that "international law neither endorses nor prohibits espionage, but rather preserves the practice as a tool by which to facilitate international cooperation."[97] According to Baker, espionage is a functional tool without which states would be less willing to adopt international cooperation, especially security cooperation.[98] Baker emphasized two functions of espionage. First, espionage can facilitate cooperative negotiations by

---

[92] *See* Josef Kunz, *The Swing of the Pendulum: From Overestimation to Underestimation of International Law*, 44 AM. J. INT'L L. 135, 136–37 (1950).
[93] *See, e.g.*, Richard A. Falk, *On Treaty Interpretation and the New Haven Approach*, 8 VA. J. INT'L L. 330 (1968).
[94] *See generally* Eisuke Suzuki, *The New Haven School of International Law: An Invitation to a Policy-Oriented Jurisprudence*, 1 YALE J. WORLD PUB. ORD. 1 (1974).
[95] *See* Falk, *supra* note 94; *see also* Blake D. Mora, *Lessons From Thomas More's Dilemma of Conscience: Reconciling the Clash Between a Lawyer's Beliefs and Professional Expectations*, 78 ST. JOHN'S L. REV. 965, 986–87 (2004).
[96] For a more in-depth explanation and examination of the functionalism approach to international relations, see FUNCTIONALISM: THEORY AND PRACTICE IN INTERNATIONAL RELATIONS 1 (AJR Groom & Paul Taylor eds., 1975); NEW PERSPECTIVES ON INTERNATIONAL FUNCTIONALISM 1, 6 (Lucian M. Ashworth & David Long eds., 1999).
[97] *See* Baker, *supra* note 73, at 1092.
[98] *See id.* at 1102–1111.

"enabling states to better understand their neighbors' security needs and concerns."[99] Second, espionage can facilitate cooperative compliance by enabling "substantive verification" of the other party's compliance with its agreed-upon obligations.[100]

Baker's arguments share many similarities with the previously discussed argument that espionage should be legal because it can help maintain international security and stability, and some scholars seem to equate these two approaches.[101] Indeed, many counterarguments are valid to both approaches. For example, one can equally bring up instances of intelligence failures to contend that his theory is not supported by history and just as one can also argue that this approach fails to account for economic espionage. In any case, the possible function of espionage does not render all espionage activities to be *per se* permissible.

However, what differentiates Baker's approach is that his focus is not merely on the protection of the current international order but also the shaping of new norms. While espionage does not guarantee international cooperation, it does have an important pragmatical function and can sometimes promote international cooperation and the development of the international order. As a result, Baker's approach posed a pragmatism challenge to scholars who view international law as a proper instrument to regulate espionage: it seems that such regulation, even if practical, will only be desirable if it either does not jeopardize the progressive function of espionage or provides an equally or more important pragmatism justification. I will address this challenge and discuss the pragmatism justification for the *lex specialis* of peacetime espionage in Part IV *infra*.

c. Espionage is *Per Se* Illegal

1. Espionage Violates Customary International Law

Scholars advocating for the view that espionage is *per se* illegal under international law often rely on customary international law. To begin with, a minority of them might argue that the prohibition of espionage is by itself a customary international law.[102] On the one hand, many states have

[99] *See id.* at 1105–1108.
[100] *See id.* at 1108–11.
[101] *See, e.g.*, Radsan, *supra* note 23, at 605–07.
[102] *See, eg.*, Aaron Shull, *Cyber Espionage and International Law*, GIGANET: GLOBAL INTERNET GOVERNANCE ACAD. NETWORK, ANNUAL SYMPOSIUM 2013 (2013).

publicly stated that espionage is unacceptable under international law.[103] On the other hand, almost all states have criminalized espionage under domestic law for a long time.[104] However, considering most states, including those that regard espionage as unlawful under international law, have never refrained from engaging in espionage activities, this argument is very weak.[105]

A stronger argument is that espionage violates the long-established customary international law principle of sovereignty, non-intervention, and territorial integrity.[106] These principles are broad, and their exact scopes are constantly under debate. For example, whereas the U.K. views sovereignty as simply a principle, the Netherlands argues that sovereignty is a concrete rule that can be independently violated.[107] As a result, scholars relying on such principles may make arguments that are not identical to each other. But overall, most of their arguments can be summarized: espionage is *per*

---

[103] *See, e.g.*, *China demands halt to 'unscrupulous' US cyber-spying*, THE GUARDIAN (May 27, 2014, 4:16 AM), https://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying [https://perma.cc/2XDQ-DA63]; Maria Lopez Conde, *Rousseff Denounces U.S. Espionage*, RIOTIMES (Sept. 24, 2013), http://riotimesonline.com/brazil-news/front-page/rousseff-denounces-u-s-espionage [https://perma.cc/CD4L-RUFM]; Carla Stea, *Latin America Condemns US Espionage at United Nations Security Council*, GLOB. RSCH. (Aug. 17, 2013), https://www.globalresearch.ca/latin-america-condemns-us-espionage-at-united-nations-security-council/5346120 [https://perma.cc/8MCE-5BTV].

[104] *See, e.g.*, Richard A. Falk, *Space Espionage and World Order: A Consideration of the Samos-Midas-Program*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 45, 80–81 (Roland J. Stanger ed., 1962).

[105] *See, e.g.*, Pete Williams, *FBI Director Wray says scale of Chinese spying in the U.S. 'blew me away'*, NBC NEWS (Feb. 1, 2022, 6:39 PM), https://www.nbcnews.com/politics/politics-news/fbi-director-wray-says-scale-chinese-spying-us-blew-away-rcna14369 [https://perma.cc/77B8-AVKU]; Amar Toor, *Brazil admits to spying on US diplomats after blasting NSA surveillance*, THE VERGE (Nov. 5, 2013, 5:33 AM), https://www.theverge.com/2013/11/5/5068024/brazil-admits-to-spying-on-us-russia-iran-diplomatic-targets-after-nsa-criticism [https://perma.cc/A9R7-2JRV].

[106] *See, e.g.*, RICHARD J. ALDRICH & RORY CORMAC, THE BLACK DOOR: SPIES, SECRET INTELLIGENCE AND BRITISH PRIME MINISTERS 205 (2016); JOHN KISH, INTERNATIONAL LAW AND ESPIONAGE 88 (David Turns ed., 1995); McDougal, Lasswell & Reisman, *supra* note 15, at 394; Wright, *supra* note 32.

[107] *See, e.g.*, Michael Schmitt, *The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis*, JUST SEC. (Oct. 14, 2019), https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/ [https://perma.cc/L4EU-YT3Q].

se illegal under international law because "a state spying on foreign soil extends its governmental functions and activities beyond its own and onto another state's territory without respecting that state's jurisdiction."[108]

2. Espionage Violates Specific Treaties

Besides customary international law, many scholars would also bring up specific treaties. This section will briefly discuss four treaties that are most frequently cited.

The first treaty is the International Covenant on Civil and Political Rights (ICCPR), which recognizes privacy as a fundamental human right.[109] Specifically, article 17 of ICCPR provides that everyone has the right to be protected by law against "arbitrary or unlawful interference with his privacy, family, home or correspondence."[110] The UN Human Rights Committee has expressed the view that article 17 applies to foreign surveillance.[111] However, article 17 may not implicate espionage. Under the U.S.'s interpretation, ICCPR only applies to activities within a state's own territory; and even under the European Convention on Human Rights' broader approach, the application of ICCPR is limited to a state's territory and persons subject to its jurisdiction.[112]

Besides, two treaties implicate espionage activities conducted by a state's diplomats — the Vienna Convention on Diplomatic Relation (VCDR)[113] and the Vienna Convention on Consular Relations (VCCR).[114] Specifically, article 41(1) of the VCDR and article 55(1) of the VCCR requires diplomats to "respect the laws and regulations of the receiving State" and "not to interfere in the internal affairs of [the receiving] State."[115] Since espionage is generally prohibited by the receiving state's

---

[108] *See* Terry, *supra* note 33, at 614–16.
[109] *See* International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 [https://perma.cc/QF7E-7V9D].
[110] *See id.*
[111] *See* Hum. Rts. Comm., Concluding Observations on the Fourth Periodic Rep. of the United States of America, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014).
[112] *See* Deeks, *supra* note 17, at 306–07.
[113] *See* Vienna Convention on Diplomatic Relations, art. 41, Apr. 18, 1961, 500 U.N.T.S. 95 [hereinafter VCDR].
[114] *See* Vienna Convention on Consular Relations, art. 55, Apr. 24, 1963, 596 U.N.T.S. 261 [hereinafter VCCR].
[115] VCDR, *supra* note 114, art. 41(1); VCCR, *supra* note 115, art. 55(1).

domestic laws, the VCDR and VCCR can be interpreted as prohibiting espionage by diplomats.[116] However, such an interpretation is, or at least was, rejected by the DOJ because of the prevalence of employing diplomats to collect foreign intelligence.[117]

Another relevant treaty is the United Nations Convention on the Law of the Sea (LOSC), which implicates maritime espionage.[118] Under article 19 of LOSC, a state has a right to "innocent passage" in another state's territorial sea.[119] Most espionage activities, however, are not innocent according to article 19(2)(c), which explicitly excludes activities "aimed at collecting information to the prejudice of the defence or security of the coastal State."[120] Besides, the catch-all phrase of article 19(2)(l) excludes from the coverage of innocent passage all activities "not having a direct bearing on passage."[121] Thus, some scholars argue that LOSC prohibits all kinds of espionage at another state's territorial sea.[122] However, some other scholars counter that article 19 only confers an affirmative right and does not render all activities that are not innocent passage illegal – espionage might not be prohibited but simply "unprivileged" and "unprotected" under LOSC.[123]

3. Problems of This Approach

The proposition that espionage is *per se* illegal was described as the "most convincing" one according to Patrick C. R. Terry.[124] Indeed, from a purely legal perspective, this approach is the most reasonable one among the three traditional approaches under the current international law framework. However, this approach is also highly problematic for at least two reasons.

---

[116] *See* Deeks, *supra* note 17, at 312–13; *see also* Terry, *supra* note 36, at 397–98.
[117] *See* Antonin Scalia, Assistant Attorney Gen., Office of Legal Counsel, Memorandum for the Attorney General on the Vienna Convention (Dec. 24, 1975).
[118] *See* United Nations Convention on the Law of the Sea, art. 19, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter LOSC].
[119] *See id.* at 404.
[120] *Id*.
[121] *Id*. at 404–05.
[122] *See* Hutchins, *supra* note 30, at 25–27; *see also* Terry, *supra* note 36, at 399–400.
[123] *See* James Kraska, *Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters*, 54 COLUM. J. TRANSNAT'L L. 164, 172, 226 (2015).
[124] Terry, *supra* note 36, at 390.

First, this approach does not address modern satellite espionage, cyber espionage, and maritime espionage beyond a state's territorial sea. In his recent article, Terry argued that modern espionage activities are also prohibited under the current international law framework.[125] This paper, however, finds his explanation to be unsatisfactory.

Terry begins his analysis by admitting that these modern espionage activities are different from traditional espionage in that they generally do not require the presence of a spy within another state's territory.[126] Thus, Terry concedes that satellite espionage does not infringe on another state's sovereignty because a state's sovereignty in the airspace is limited in height and does not extend to outer space.[127] The European Court of Human Rights has similarly held that cyber espionage generally does not violate the target state's sovereignty right.[128]

However, Terry nevertheless finds modern espionage to be illegal by arguing that it constitutes an unlawful intervention in another state's affairs.[129] The non-intervention principle is customary international law, and a violation of it can be found by establishing two elements: (1) "coercion by one state of another state" (2) about "matters in which each State is permitted, by the principle of State sovereignty, to decide freely" (internal quotation marks omitted).[130] The key element to our discussion is clearly the "coercion" requirement, as it seems that espionage is not particularly relevant to the common sense understanding of the term "coercion." Terry, however, offers a novel argument. According to Terry, coercion can be found whenever the target state is unable to fully exercise its "freedom to choose in matters related to its sovereignty."[131] Thus, all kinds of espionage are coercive because they will deprive another state's "sovereign right to decide whether to disclose secret information."[132]

---

[125] *See id*. at 402–12.
[126] *See id*. at 402–03.
[127] *See id*. at 405.
[128] *See id*. at 403 (quoting Weber and Saravia v. Germany, 2006-XI Eur. Ct. H.R. 1, 20 (2006)).
[129] *See id*. at 404–12.
[130] HARRIET MOYNIHAN, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION 27 (2019) (citing Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).
[131] Terry, *supra* note 36, at 408.
[132] *See id*.

Putting aside Terry's later concession that there is a need to make space for "permissible interventions,"[133] the issue of this argument is that his approach would effectively eliminate these permissible interventions and render most, if not all, interventions illegal. For example, applying Terry's rationale, one can argue that broadcasting news to another state's citizens might constitute an unlawful intervention because it deprives that state's "sovereignty right" to decide when to tell their citizens the truth. Moreover, one can argue that open-source intelligence collection is also illegal because it violates another state's "sovereign right" to disclose certain information only to its citizens but not to foreigners.

The reasons why this approach can lead to such absurd consequences are twofold: (1) he adopts an overly broad and ambiguous definition of "sovereign right" without providing valid justifications; and, more importantly, (2) he fails to differentiate between *means* of intervention and *motives/consequences* of intervention. In fact, Terry openly asserts that a state's motive of espionage can constitute a separate reason for finding a violation of the non-intervention principle.[134] However, a more reasonable interpretation of the non-intervention principle seems to be that the motives/consequences of intervention can only satisfy that second element of state sovereignty, and the coercion requirement must be separately met by proving that the means of intervention involves a sufficient degree of pressure.[135] Terry's argument fails because he does not prove that cyber or satellite espionage can exert a high degree of pressure on the target state's policy decision-making.

Terry also brings up the ICJ's decision in Timor-Leste v. Australia[136] and argues that espionage violates the "principle of sovereign equality."[137] However, in the Timor-Leste case, the ICJ ruled against Australia based on its "bad faith" and "violation of attorney client-confidentiality" during an international arbitration proceeding that was

---

[133] *See id*.
[134] *See id*. at 408–09.
[135] *See* MOYNIHAN, *supra* note 131, at 27–29.
[136] *See* Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Austl.), Provisional Measure, 2014 I.C.J. 147 (Mar. 3).
[137] *See* Terry, *supra* note 36, at 410–12.

supposed to be peaceful.[138] The ICJ's holding neither directly relates to espionage nor extends to situations other than international arbitrations.[139]

Besides the failure to address modern espionage, the argument that espionage is *per se* illegal is also problematic from a pragmatical perspective. Generally, the two most important functions of international law are its legitimate function[140] and its expressive function.[141] Regarding espionage as *per se* illegal cannot be justified by international law's legitimate function because it is unlikely that espionage will be prosecuted in an international court. It is unrealistic to expect that international organizations like the ICJ can stop a state from espionage or prosecute it for engaging in peacetime espionage. As for individual spies, even if a court like the ICC is willing to have jurisdiction over them, a state will usually be more willing to deal with espionage through domestic laws and political means. Additionally, the expressive function cannot be achieved by regarding espionage as *per se* illegal because a requirement for a constructive international dialogue on espionage is the existence of a way to differentiate legal and illegal, or at least less comprehensible and more comprehensible, ways of conducting espionage.

III. Frontier Theories and the Piecemeal Approach to Espionage

Many scholars have realized the restrictions and problems of the traditional approaches. These scholars argue that a *per se* approach to espionage is no longer workable, and that instead, the correct approach is to treat certain espionage activities as lawful and to treat others as unlawful.[142] This section will introduce three different approaches adopted by these

---

[138] *See* Hutchins, *supra* note 30, at 15.
[139] *See id*.
[140] *See, e.g.*, Darien Pun, *Rethinking Espionage in the Modern Era*, 18 CHI. J. INT'L L. 353, 371 (2017); *see also, e.g.*, Harold Hongju Koh, *Why Do Nations Obey International Law?*, 106 YALE L.J. 2599, 2601–02 (1997).
[141] *See, e.g.*, Pun, *supra* note 141, at 370–371; Richard H. McAdams, *An Attitudinal Theory of Expressive Law*, 79 OR. L. REV. 339, 340 (2000); Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2032–33 (1996).
[142] *See* Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SEC. L. & POL'Y 179, 195–96 (2011); *see also, e.g.*, Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 685 (2016); Asaf Lubin, *The Liberty to Spy*, 61 HARV. INT'L L.J. 185, 242–43 (2020).

scholars. It will argue that whereas these scholars provide some valuable insights, their proposed approaches are neither ideal nor comprehensive.

a. Craig Forcese's Method-based Approach

1. Summary of arguments

Forcese begins his arguments by noting that there are, broadly speaking, three ways of collecting foreign intelligence: (1) territorial or purely domestic spying, (2) extraterritorial or purely foreign spying, and (2) transnational spying, which means spying that "straddles state borders."[143]

With respect to territorial spying, Forcese finds two relevant sources of international law— international human rights law and international immunities law.[144] In discussing the limits on spying imposed by international human rights law, he further differentiates two methods of domestic spying: interrogation and surveillance.[145] For interrogation, he notes that the ICCPR and the Convention Against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment ("Torture Convention") require the "humane treatment of detainees" and prohibit interrogation that constitutes either torture or "cruel, inhuman, and degrading treatment.[146] For surveillance, he argues that Article 2 of the ICCPR prohibits discriminatory treatment in conducting surveillance,[147] and Article 17 of the ICCPR prohibits "arbitrary or unlawful" surveillance of activities that "take place in [one's] home or place of work."[148] Forcese also invokes soft laws including the U.N. Guidelines for the Regulation of Computerized Personal Data Files[149] and the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[150] These standards provide further protection of personal data, but since they contain "national security" exceptions, it is unlikely that they will be particularly relevant to

---

[143] *See* Forcese, *supra* note 143, at 183–84. Note that Forcese's definition of the term "spy" is very broad — he basically equates "spy" with "intelligence collection." *See id*. at 181–83.
[144] *See id*. at 185–86.
[145] *See id*. at 186.
[146] *See id*. at 186–193.
[147] *See id*. at 193.
[148] *Id*. at 194–95.
[149] *Id*. at 195.
[150] *Id*.

our discussions.[151] In addition to international human rights law, Forcese also notices that the VCDR protects diplomats[152], the diplomatic premises[153], official correspondence[154], and personal correspondence ad premises of diplomats.[155] Thus, he argues that spying on diplomats is generally prohibited.[156]

With respect to extraterritorial spying, Forcese also finds two relevant sources of international law: international human rights law and the customary principle of sovereignty.[157] In discussing human rights law, he still focuses on the ICCPR and the Torture Convention, and their extraterritorial applicability.[158] He concludes that these two treaties still provide some constraints on extraterritorial spying because the Torture convention can "extend to territories over which it has factual control" and the ICCPR can be applied to extraterritorial HUMANINT.[159]

In discussing the sovereignty principle, Forcese differentiates between two methods of espionage: espionage by diplomats and espionage by other agents.[160] Article 41 of the VCDR requires diplomats to respect the laws and regulations of the receiving state.[161] However, unlike the traditional prohibitive approach, he highlights article 3 of the VCDR, describing the "function of a diplomatic mission" as, inter alia, "[a]scertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State."[162] Forcese interprets the VCDR in a holistic way, arguing that even if a state has domestic laws per se prohibiting espionage, such laws are not compatible with the fundamental principles of the VCDR. Thus, not all violations of domestic laws of the receiving state automatically violate article 17.[163]

---

[151] *Id*.
[152] *Id*. at 196.
[153] *Id*.
[154] *Id*.
[155] *Id*.
[156] *Id*. at 197.
[157] *Id*.
[158] *Id*. at 205–07.
[159] *Id*. at 207.
[160] *See id*. at 199–205.
[161] *Id*. at 199.
[162] *Id*.
[163] *See id*. at 200.

Forcese argues instead that the key is the "means" of espionage.[164] He lists some examples of unlawful means of espionage such as "[b]reaking into a residence to plant a listening device."[165] Beyond these sporadic examples, however, Forcese fails to propose a workable standard in distinguishing between lawful and unlawful means of espionage. Forcese then discusses espionage by non-diplomats and reaches a precise, yet not very valuable conclusion— "there is no clear answer."[166]

Lastly, he discusses transnational spying.[167] The way by which Forcese addresses transnational spying seems to be quite straightforward—some transnational spying should be treated the same way as extraterritorial spying, and others will be treated like domestic spying.[168] Although his discussion here is not in-depth, Forcese seems to draw a line between two methods of transnational espionage—passive espionage and active espionage.[169] Passive espionage refers to the collection of signals that originated in other states but are intercepted in one's own territory.[170] Forcese argues that such passive espionage should not be treated like extraterritorial spying because it does not infringe on the target state's sovereignty.[171]

2. Analysis and Critique

This paper describes Forcese's approach as a "method-based approach" because, according to him, the primary, if not the only, distinction between lawful espionage and unlawful espionage is through the means by which information is collected.[172] His framework has two layers. The first layer focuses on the territoriality of a method of espionage. The second layer focuses on other aspects such as who is collecting the intelligence, against whom, and through what means. However, whereas Forcese arguably provides a new *analytical* framework, his approach does

[164] *Id.*
[165] *Id.*
[166] *Id.* at 204–05.
[167] *Id.* at 207–09.
[168] *See id.* at 207–08.
[169] *See id.* at 208.
[170] *Id.*
[171] *Id.*
[172] *See id.* at 180–81.

not exceed the well-established *substantial* framework of international law, as he only relies on the existing rules, treaties, and principles and does not provide any critical evaluation of them. In fact, other scholars have adopted similar approaches. For example, the Tallinn Manual 2.0 also emphasizes the territoriality and methods of cyber espionage while not intending to transcend the existing grammar of international law.[173]

On a higher level, we can view this approach as sharing a critical similarity with Terry's approach—they both recognize the challenges brought by modern espionage to international law, intend to deal with such challenges, and believe that such challenges can be overcome by interpreting the existing laws in a novel way. The only difference is that whereas Terry provides a novel interpretation of specific rules and principles like the non-intervention principle, Forcese's focus is on a different way to apply the existing international law to espionage.

Thus, it is no surprise that scholars adopting such a method-based approach, including Forcese, reject the need for a *lex specialis* of peacetime espionage.[174] However, as Asaf Lubin correctly points out, it is not true that we only need a new analytical framework or a different way of applying the existing international law to effectively deal with challenges brought by modern espionage.[175] In his paper, Lubin provides the first comprehensive analysis and critique of the method-based approach.[176] He offers four reasons why the method-based approach is incorrect or at least not comprehensive enough, and this paper recognizes two of them as strong arguments but finds the other two to be invalid.

The first incorrect argument is that the method-based approach "ignores widespread state practice of interstate territorial and diplomatic spying as well as the crucial functions that such intelligence operations play in our contemporary legal order."[177] Lubin regards this to be the "[m]ost significant" problem of this approach.[178] Lubin makes such a critique because he characterizes the method-based approach as if it would legalize

---

[173] *See* David A. Wallace, et al., *Peeling Back the Onion of Cyber Espionage After Tallinn 2.0*, 78 MD. L. REV. 205 (2019).
[174] *See* Lubin, *supra* note 28, at 198.
[175] *See id.* at 197–206.
[176] *Id.*
[177] *Id.* at 199.
[178] *Id*.

all remote espionage and illegalize all territorial espionage.[179] However, this characterization, at least as it applies to Forcese's approach, is not precise. As discussed in the section above, Forcese offers a creative and reasonable argument rebutting the view that the VCDR per se prohibits diplomats from spying.

The second problematic argument is that the method-based approach can "entrench regional and global social structures and enforce[e] a specific constellation of power and knowledge dynamics."[180] Lubin's view is that territoriality should play no role in determining the legality of espionage activities because treating remote espionage as more permissive will jeopardize those third-world countries without a capacity to conduct remote espionage.[181]

However, third-world countries have fewer resources to conduct espionage, so it is unclear what these countries can gain from an international law that is equally lenient to territorial espionage and remote espionage. While this paper rejects the pure realpolitik approach, it also rejects what Lubin describes as the "Third World Approaches to International Law."[182] It is too unrealistic to be relied upon.

Lubin correctly points out that the method-based approach's overemphasis on territoriality is not ideal.[183] Most critically, relying on territoriality cannot overcome the challenges of modern espionage to international law. As discussed above, Forcese's analysis fails to offer many insights into the legality of cyber and satellite espionage. Forcese's dualistic approach to transnational espionage, to treat it as either territorial espionage or exterritorial espionage, is too difficult to apply. At the same time, his failure to give a clear answer to the legality of espionage by non-state actors is disappointing considering that "intelligence outsourcing" has increasingly become one of the biggest international law challenges.[184]

---

[179] *See id.* at 205–06.
[180] *Id.* at 203.
[181] *See id.* at 203–04.
[182] *See id.* at 203.
[183] *See id.* at 204–06.
[184] *See, e.g.*, Joshua R. Storm, *Outsourcing Intelligence Analysis: Legal and Policy Risks*, 9 J. NAT'L SEC. L. & POL'Y 669, 672 (2018).

Besides, as Lubin keenly observes, the method-based approach does not address the whole "intelligence cycle" because it only specifies how a state can legally conduct its espionage activities.[185] This approach fails to address issues like, "when is it lawful to spy?"[186] Hence, while Forcese provides some insight into how to regulate the ways by which espionage activities are conducted, his method-based approach is incomplete.

b. Ashley S. Deeks's Harm-Based Approach

1. Summary of Arguments

Deeks begins her arguments by detailing two opposing narratives of the relationship between international law and intelligence.[187] On one side, the realpolitik approach views international law as inapplicable to intelligence activities.[188] On the other end, formalists take the view that international law "represents commitments assumed by a state" and therefore applies to all state activities including intelligence activities.[189]

Deeks rebuts the realpolitik approach and identifies nine reasons why international law should play a role in regulating espionage.[190] The first five reasons are related to the instrumental values of international law.[191] Specifically, applying international law to espionage can (1) provide further deterrence, (2) supplement domestic laws, (3) provide remedies for minorities who are not adequately protected by their state's domestic laws, (4) serve an expressive function, and (5) provide additional remedies through international institutions.[192] The remaining four reasons concern the practical needs of regulating espionage through international law: (1) there will be more public pressure because of the increase in public access to information about intelligence activities; (2) the expansion of missions of intelligence agencies has led to more interactions between intelligence agencies and non-government actors; (3) the intelligence culture is changing and requires intelligence agencies to be more law-bidding; and (4) international law has played an increasingly important role in protecting

---

[185] *See* Lubin, *supra* note 28, at 203.
[186] *Id.*
[187] *See* Deeks, *supra* note 17, at 606–14.
[188] *See id.* at 606–07.
[189] *Id.* at 601.
[190] *See id.* at 613–31.
[191] *See id.* at 613–14.
[192] *Id.*

individual rights, which will unavoidably influence the intelligence agencies.[193]

Deeks, however, also rejects the formalism approach, or more precisely, the three traditional approaches discussed in Part II.[194] Instead, she advocates for a "sliding scale" approach that accepts "*gradations of interpretation* of international law."[195] She argues that international law that focuses on "protecting individuals" should be interpreted strictly, whereas international law that protects states and "regulates state-to-state activity" should be interpreted liberally.[196] To justify this approach, Deeks offers both practical and theoretical justifications.

With respect to the practical justifications, Deeks compares the "pressure" to respect individual rights with that to respecting state rights.[197] She notices that the former is particularly strong because (1) many states and international organizations will publicly accuse human rights violations by intelligence agencies, (2) human rights groups will litigate against intelligence agencies violating human rights laws, (3) the U.N. will also pressure states to refrain from conducting intelligence activities in a way inconsistent with human rights treaties, and (4) there is a strong peer pressure within intelligence communities to respect human rights.[198] In contrast, Deeks argues that the pressure to protect state rights is weaker primarily because of the "lack of consensus" about whether, which, and how these rules govern intelligence activities.[199]

Deeks then provides two theoretical justifications.[200] First, she brings up the "principle of tacit consent" and argues that whereas a state can be regarded as having tacitly consented to other states' espionage activities because of its own espionage activities, such consent cannot be extended to individuals.[201] Second, Deeks highlights the fact that "intelligence activities pose increased risks of harm to non-state actors."[202]

---

[193] *Id.* at 614–31.
[194] *See id.* at 607–12, 667–68.
[195] *Id.* at 669.
[196] *Id.* at 604.
[197] *Id.* at 631–45.
[198] *Id.* at 631–41.
[199] *Id.* at 632.
[200] *See id.* at 645–50.
[201] *Id.* at 646.
[202] *Id.* at 648.

Interpreting international laws that protect individual rights more strictly, she explains, can help reduce unintended harm to non-state actors *ex-ante*.[203]

2. Critique and the Need for an Ontological Turn

It is worth noting that the methodology of Deeks's approach has departed from the four approaches discussed above. While those approaches take the current international law framework as given, in proposing a novel way to interpret different legal rules and principles within it, Deeks has tried to innovate that framework. If successful, this would unavoidably influence the way the current international legal system operates.

However, this paper finds the starting point of Deeks's paper, that is, the inquiry into the relationship between international law and espionage activities, to be problematic. This starting point restricts her paper to the discussion of the interpretation of international law instead of the exploration of what a *lex ferenda* of peacetime espionage would look like. Put another way, to apply H.L.A. Hart's terminologies, Deeks only focuses on proposing a new rule of recognition, or *secondary* law, rather than a new *primary* international law.[204]

Deeks does not explain why proposing a new secondary *lex specialis* that specifies how to apply international law to peacetime espionage activities in a different way should be preferred over directly advocating for a new primary *lex specialis* of peacetime espionage. However, it seems that all reasons Deeks brought up to justify her approach are equally applicable to the proposition that we need a new primary international law of peacetime espionage. Deeks argues that her approach can (1) render states to "act more carefully and cautiously when undertaking nontraditional intelligence activities," (2) "alter state incentives ex ante," (3) "increase the quantity of verbal state practice related to intelligence," (4) alter states' intelligence operations, and (5) help develop a new international norm.[205] All of these reasons are valid, however, none of them are specific to secondary laws. A new *lex specialis*

---

[203] *Id.* at 648–49.
[204] *See* H.L.A. HART, THE CONCEPT OF LAW 79–81 (1961).
[205] Deeks, *supra* note 17, at 683–85.

of peacetime espionage can have similar, if not stronger, functions to achieve these policy goals.

On the other hand, relying on secondary laws can cause two problems. First, while there has been some consensus among the international community on how to develop a new customary international law, it is unclear whether a similar consensus can be reached on the development of a customary way of interpreting international law. Currently, the authoritative way of interpreting international law is written in a treaty (Articles 31 and 32 of the Vienna Convention on the Law of Treaties) instead of being developed through state practices.[206] Besides, developing a new customary secondary law will clearly face many tough issues – for example, shall we refer to the executive branch's interpretation or the juridical branch's interpretation? Can a customary secondary law bind a state's domestic courts? How do we deal with the separation of power concerns?

Second, as legal formalists correctly noticed, while Deeks's aim is to reconcile the intelligence community's practical needs with the fundamental principles of international law, her approach fails because, by arguing that the contents of international law should be subject to political needs, it "does not operate to give international law primacy in any instance."[207] Legal formalists, however, contend that we need neither a new secondary law nor a new primary law but only a new analytical framework.[208] As Forcese reasons, international law "colors state discourse without governing the outcomes of state decisions, at least for matters of high politics."[209] Thus, he continues, international law "approximates a grammar of international relations" and "does bind" how things can be said.[210] However, as we have illustrated through the discussion of the first four approaches, using the current "grammar" that is composed of concepts such as sovereignty cannot solve the dilemma of modern espionage –

---

[206] *See* Vienna Convention on the Law of Treaties, arts. 31-32, May 23, 1969, 1155 U.N.T.S. 331.
[207] Craig Forcese, *Pragmatism and Principle: Intelligence Agencies and International Law*, 102 VA. L. REV. ONLINE 67, 82 (2016).
[208] *See id.* at 81; *see also* Terry, *supra* note 36, at 385–86 (arguing that "international law already regulates most activities commonly associated with espionage, making a distinct body of rules on "espionage" almost superfluous").
[209] Forcese, *supra* note 208, at 82.
[210] *Id.* at 82–83.

intelligence agencies will be in a dilemma themselves: that it must either violate international law or be unable to function properly. Thus, this paper argues that what we need is a new set of "grammar" that applies specifically to peacetime espionage, or a set of new and more relaxed *lex specialis* because, as Deeks highlights, it is undeniable that "there *is* something unique about intelligence activity."[211]

If we reexamine Deeks's approach considering such needs, we must recognize the merits of her harm-based approach. In fact, a recent German case has illustrated that some states have adopted a strict interpretation of human rights laws to restrict espionage activities.[212] What this paper will do then is twist Deeks's approach for an ontological turn – it will incorporate her observations into the proposed systematic framework for the new *lex specialis* of espionage. As will be discussed in Part V, the harm-based approach, as well as Deeks's tacit consent argument, have a direct implication in our discussion about the principle of macro-proportionality, micro-proportionality, and discrimination. Most critically, Deeks's approach highlights the need to consider both the quantity and the *quality* of harm in proportionality analysis, which, according to the author's knowledge, has not been proposed by ethicians in the development of the just intelligence theory.

c. Asaf Lubin's Purpose-Based Approach

1. Summary of Arguments

Lubin's paper for the first time systematically introduced and examined the *lex specialis* of peacetime espionage.[213] Lubin first considers what a framework for such a *lex specialis* would look like.[214] After highlighting the *Zakharov v. Russia* case decided by the European Court of Human Rights[215] and some 1980s philosophical literature discussing the

---

[211] Deeks, *supra* note 17, at 602.
[212] *See* Katrin Kappler, *Consequences of The German Constitutional Court's Ruling on Germany's Foreign Intelligence Service: The Importance of Human Rights in The Cooperation of Intelligence Services*, 23 GER. L.J. 173 (2022).
[213] *See* Lubin, *supra* note 28, at 206–11.
[214] *Id.* at 210.
[215] Roman Zakharov v. Russia, 2015-VIII Eur. Ct. H.R. 58–59.

plausibility of applying the just war tradition to espionage,[216] Lubin provides a framework that divides espionage activities into three stages with three different paradigms – he uses the term *jus ad explorationem* to describe a state's right to launch an espionage operation, *jus in exploratione* to describe a state's obligations when conducting an espionage operation, and *jus post explorationem* to describe a state's duties after its espionage operations.[217] Lubin then explains that his paper will only focus on *jus ad explorationem*.[218]

For a comprehensive discussion of *jus ad explorationem*, one clearly has to answer at least two questions. First, one must explain why espionage can *ever* be legal. Then, one must explain *when and under what circumstances* a particular espionage activity is or should be legal under international law. Lubin provides answers to both questions.

As for the first issue, Lubin invokes the rights theory of Hohfeld and argues that there exists a "liberty right" to spy.[219] According to Hohfeld, legal interests are incorporeal, and they exist and must be analyzed in abstract legal relations.[220] Hohfeld identifies two primary rights: claim rights and liberty rights.[221] A claim right exists when the person against whom the right-holder has a claim is under a duty to respect the latter's claim, so "[w]hen a right is invaded, a duty is violated."[222] A liberty right, in contrast, is, strictly speaking, not a right but a "privilege" and exists when the privilege-holder has no duty to respect certain claims of another person.[223] Relying on such a dichotomy, Lubin argues that while a state does not have a claim right to spy, it can have the discretion (liberty right) to do so; and while the target state cannot get legal remedy, it can

---

[216] *See, e.g.*, James A. Barry, *Managing Covert Political Action: Guideposts from Just War Theory*, 36 STUD. INTEL. 19, 19 (1992); William E. Colby, *Public Policy, Secret Action*, 3 ETHICS & INT'L AFF. 61, 63 (1989).
[217] Lubin, *supra* note 28, at 206–11.
[218] *Id.* at 211.
[219] *Id.* at 225–29.
[220] FUNDAMENTAL LEGAL CONCEPTIONS AS APPLIED IN JUDICIAL REASONING BY WELSEY NEWCOMB HOHFELD 8 (David Campbell & Philip Thomas ed., 2001).
[221] *Id.* at 12–21.
[222] *See id*. at 13.
[223] *See id.* at 12–21.

choose to adopt counter-espionage operations because it does not have a duty to protect the other party's liberty right.[224]

As for the second issue, Lubin first argues that the right to spy, as a liberty right, is "only a derivative of harder claim-rights."[225] Lubin seems to identify five sources of such "harder claim-rights"—(1) survival and self-determination, (2) self or collective self-defense, (3) collective monitoring of international obligations, (4) protect the integrity of international human rights laws, and (5) the principle of precautious under the laws of armed conflict.[226] However, it seems that Lubin's application of Hohfeld's rights theory is problematic because the last three sources should be better classified as a state's "duty" instead of "right." Although Lubin introduces five sources from which the right to liberty derives, he does not use all of them in his framework. Under Lubin's framework, the difference between the legal and illegal exercise of one's liberty right to spy depends on what he calls "just causes."[227] However, he only identifies two just causes: (1) national security and (2) international stability and cooperation.[228] Moreover, he specifies four situations when a state's espionage activities can be regarded as illegal: (1) spying to advance personal interests, (2) spying to commit internationally wrongful acts, (3) spying to advance corporate interests, and (4) spying to exploit post-colonial relations.[229]

2. Four Problems of Lubin's Approach

Although Lubin correctly notices the need for a *lex specialis* of peacetime espionage, his framework has four fundamental problems.

First, from a jurisprudential perspective, it is confusing, if not unreasonable, to invoke Hohfeld's theory. To be sure, Hohfeld is a great jurist and provides important insights into different types of rights. However, since Hohfeld's rights theory is largely a positive one, relying on it cannot really give us insight into the normative question of why and when espionage can be justified. Thus, Lubin's framework contains an "is-

[224] *See* Lubin, *supra* note 28, at 226–27.
[225] *See id.* at 231.
[226] *See id.* at 211–25.
[227] *See id.* at 231.
[228] *See id.* at 231–36.
[229] *See id.* at 236–42.

ought fallacy": he incorrectly mixes up a positive description of a state's liberty right to espionage with a normative argument that a state should have a liberty right to espionage.[230] A possible reply is that while Hohfeld's theory does not provide a normative justification, Lubin's paper has made a normative argument to supplement it. That is, as discussed above, the argument that a liberty right can be derived from a claim right under international law. Thus, he may argue that the normative justification for a state's liberty right to espionage is derived from the normative justification for its claim right from which the liberty right derives, and since the latter, like a state's right to self-defense, is well-established and well-justified under international law, the former can also be normatively justified. However, this argument is also problematic because it does not explain the relationship between a state's derivative rights of its claim rights with another state's claim rights. Put another way, considering that many espionage activities can infringe on another state's claim rights like sovereignty, Lubin has to explain why the former's liberty right to spy, which is a derivative right of its claim rights like self-defense, should prevail over the latter's claim right to sovereignty. One might reply that the reason can be reduced to the original relationship between the two states' claim rights, thus since the right to self-defense can sometimes prevail over another's right to sovereignty, the former's derivatives can also prevail. However, even assuming this argument is valid, it fails to give us any hints on solving the paradox of espionage but only sends us back to the very starting point. What Hohfeld's right-privilege or claim-liberty distinction provides, then, is simply such a not very valuable conclusion – the target state has no "duty" to respect and protect another state's espionage activities against it.

Since Lubin mistakenly believes that he has explained why a state has a liberty right to espionage, his latter discussion only focuses on the scope of such a right.[231] This leads to the second problem of his framework – it does not explain why a state can conduct espionage activities to explore unknown unknowns. Because a state's right to spy cannot be normatively presumed according to Hohfeld's rights theory, under Lubin's framework, a state can only conduct espionage activities when it has at least one of the two "just causes" – self-defense and international stability. However, a

[230] *See generally* DAVID HUME, A TREATISE OF HUMAN NATURE (1738) (discussing the is-ought fallacy).
[231] *See* Lubin, *supra* note 28, at 229–42.[231]

state certainly does not and cannot wait until it discovers another state's hostile intents to collect that state's information. That would lead to a catch-22 dilemma – a state must have a specific cause to do espionage, but such a cause often must be acquired through espionage.

Thirdly, although this paper agrees with Lubin that the just war tradition provides a workable framework for analyzing espionage, Lubin's theory does not really capture the essence of it. It seems that Lubin does not notice the recent development of the just intelligence theory, and he therefore adopts a very simple view of the applicability of the just war tradition to espionage. Specifically, Lubin only notices the structural characteristics of the just war framework, that is, to analyze war from *jus ad bellum*, *jus in bello*, and *jus post bellum*.[232] Such a trichotomy structure is of course valuable; however, the value of the just war tradition is not limited to this. As will be discussed in Part V, the just war theory not only tells us that we should analyze espionage through *jus ad explorationem*, *jus in exploratione*, and *jus post explorationem*, but it also provides us with insights into the necessary components or factors of *jus ad explorationem* and *jus in exploratione*.

Lastly, because of the oversimplified view of the just war tradition, it seems that Lubin equates *jus ad explorationem* with "just cause." However, just cause cannot by itself justify the use of force under the just war theory, and there are other requirements such as just intention, macro-proportionality, correct authority, etc. Similarly, it is not correct to conclude that a state can conduct espionage activities simply because it has a just cause. Furthermore, it seems that Lubin does not realize the difference between "cause" and "intention"—while he uses the term "just cause," his discussion is more properly labeled as "just intention." That is also why I did not describe Lubin's approach as cause-based but rather purpose-based. A major difference between cause and intention is that while the former is exogenous, the latter is endogenous. For example, when a state says "we decide to attack State X because it did Y, which constitutes an imminent national security threat to us," it provides a cause—State X's action of Y; but when it says "we decide to attack State X because we believe that doing so can further our national security interests," it does not provide a cause but only an intention, which illustrates the reason why it decides to launch an attack. Therefore, whereas Lubin claims that factors

[232] *Id*. at 206.

like whether a state conducts espionage activities to advance corporate interests as part of his "just cause" analysis, these factors are more properly analyzed through the lens of "just intention," which is not included in Lubin's *jus ad explorationem* framework.

IV. A Dialectical Concept of Just Cause for Espionage that Explores Unknown Unknowns

So far, this paper has examined traditional approaches to espionage and explained why they are no longer acceptable. It also discussed recent scholars' efforts to propose new approaches. To begin with, Forcese argues that the current international law framework works, and what we need is simply a new analytical method to evaluate the legality of modern espionage under the existing legal framework.[233] Then, Deeks notices the problems of Forcese's formalism approach, and she argues that we should adopt a new secondary *lex specialis* so that even if we still apply the existing international law concepts, their meaning and strength will differ when applying to espionage.[234] Lastly, Lubin correctly argues that the best way to solve the paradox of modern espionage is to develop a new primary *lex specialis* of peacetime espionage.[235] However, Lubin fails to provide a systematic framework.

To develop such a framework, considering the problems this paper has identified above, we must deal with three primary obstacles. First, such a framework must explain why a state can legally conduct espionage activities to explore unknown unknowns. Second, it must have enough pragmatism justifications. Third, it must be systematic and comprehensive and able to absorb the merits of the different piecemeal approaches.

This section will provide a solution to the first two challenges by developing a dialectical concept of just cause for peacetime espionage. Additionally, the next section will argue that the just intelligence theory can provide us with significant insights into the development of a workable systematic framework.

---

[233] *See* Forcese, *supra* note 143, at 180–85.
[234] *See* Deeks, *supra* note 17, at 300–05.
[235] *See* Lubin, *supra* note 28, at 242.

a. The Liberal World Order and a State's Duty to Have a Transparent Deliberation Process

First, we must deal with the issues that Lubin fails to answer: why is espionage ever justifiable? More importantly, why is espionage that explores unknown unknowns ever justifiable?

Scholars advocating for traditional approaches have argued that espionage can be justified because it has an instrumental value such as protecting national security and verifying others' compliance with treaties.[236] This paper recognizes this claim as a workable starting point and agrees that we should focus on the pragmatical value of espionage. However, the instrumental value these scholars identified fails to address espionage activities that are purported to explore unknown unknowns because a specific cause is often lacking when states make the decision to engage in such espionage activities. Thus, these arguments fail to provide a satisfying answer.

This paper finds that a paper written by Raphael Bitton about the instrumental value of espionage can provide a hint to solving this problem.[237] Therefore, I will first offer a brief overview of her key arguments. Noticing international law is essentially about the order of the international community, Bitton begins her paper with an analysis of the structure of the international community.[238] She observes that the key feature of the international community is that its proper function requires international cooperation, but such cooperation will not be possible unless states are "transparent about their strategic intentions to some degree."[239] The reason lies in another feature of the international community—proximity, or the offensive military capacity one state has against another.[240] Proximities are common because, with the development of modern technologies, even weaker states now possess the capacity to launch a "surprise attack."[241]According to Bitton, such strategic surprises

---

[236] *See, e.g., id.* at 188.
[237] *See* Raphael Bitton, *The Legitimacy of Spying Among Nations*, 29 AM. U. INT'L L. REV. 1009 (2014) [https://perma.cc/8X3J-KNNR].
[238] *See id.* at 1021.
[239] *See id.* at 1021–30.
[240] *See id.*
[241] *See id.* at 1023–27.

are the biggest obstacle to international cooperation.[242] To mitigate concerns of a strategic surprise, a state must be able to ascertain other states' strategic intentions.[243] Thus, she concludes that a functional international community requires the existence of an international obligation for a state to be transparent about its strategic intention.[244] She further notices that such an obligation can be fulfilled by a truly liberal state because it cannot hide its strategic intention due to its transparent structure and deliberation process (free elections, free media, etc.)[245]

While Bitton provides vital insights thus far, her later arguments degraded into an intention-based approach. She argues that espionage has an instrumental value as "a non-structural substitute for an international duty of basic transparency."[246] Bitton concludes that "[e]spionage would be permitted for the specific purpose of enforcing transparency and facilitating international trust, cooperation, and stability."[247] However, this approach is problematic because it overemphasizes a state's subjective intention, which is relevant but not always easy to ascertain. Besides, Bitton seems to draw a very bright line between liberal and illiberal states, and she claims that peacetime espionage can only be conducted against non-transparent regimes.[248] However, the fact is that even liberal allies spy on each other because a true liberal or transparent state is a perfect ideal that no existing states have achieved. Thus, it is improper to view a state as either liberal and transparent or illiberal and untransparent because all states are between the two extremes. Lastly, Bitton regards her transparency test as a panacea and does not incorporate other restrictions on the lawfulness of espionage. Hence, her approach fails to be comprehensive because it does not address situations like a state conducting espionage with the intention to collect evidence that another state is violating human rights.

---

[242] *See id.* at 1022–29.
[243] *See id. See id.* at 1026–30.
[244] *See id.* Note that strategic intention is different from tactical intention. For example, in Gulf Wars, Saddam might be unable to know how and when the U.S. would launch an attack, but the U.S.'s strategic intention to use force against him was ascertainable. *See id.* at 1034.
[245] *See id.* at 1031–34.
[246] *See id.* at 1038.
[247] *See id.* at 1049.
[248] *See id.* at 1046–47.

b. The Historical Dimension of the Just Cause to Explore Unknown Unknowns

Although this paper finds Bitton's conclusion not ideal, her observation that a state should have a duty to make its strategic intention transparent serves as a good starting point for our discussion here. This paper argues that the reason why Bitton's arguments degraded into an intention-based test largely lies in her inherent presumption that the instrumental value of espionage can *per se* excuse its unethicality. This presumption, however, is not correct because it is one thing to claim that something has instrumental value, it is another thing to say that I am justified in using this instrument. This is especially the case when the instrument involved, like war or espionage, contains an inherent unethicality. Put another way, despite its pragmatical value, the decision to engage in espionage still needs a just cause.

Some just causes for espionage, like self-defense and international order, have been illustrated in our above discussion, and what we need here is a just cause for exploring unknown unknowns. Relying on Bitton's arguments, this paper argues that such a just cause exists when a state fails to fully fulfill its obligation to maintain a liberal structure and be transparent about its deliberation process and strategic intention. Since no states have fully achieved such an ideal status, as a practical matter, such a just cause provides a basic level of justification for every state to conduct espionage activities against any other states and to explore unknown unknowns.

One possible objection to this paper's approach is that this approach will be like the traditional approaches under which espionage is *per se* legal or permissible because whereas I used the term "just cause," a state does not really need a cause to espionage because no state has fully fulfilled its transparency responsibility. However, such an objection is wrong for two reasons. First, whereas my approach would give all states a right to espionage, such a right is not unlimited. Instead, since the justification for such a right to espionage that does not require a specific cause is the target state's failure to fulfill its transparency duty, the intrusiveness allowed for such espionage will differ depending on the target state's degree of liberalness and transparency. Although this paper highlights the importance of the principle of just cause, as well be discussed below, it is not the only element in deciding the legality of a particular espionage activity – it is just

one factor of *jus ad explorationem*. Therefore, if a state does not have other just causes like national defense or international order, its right to espionage is very limited. In fact, this is also the major difference between Bitton's approach and mine—whereas the former regards the instrumental value of espionage as a justification for its legality, the latter regards the reason why espionage can serve such a value as an excuse for the unethicality of employing it.

Second, the fact that my concept of just cause will be presumed to be met in today's world does not mean that this concept is meaningless. In contrast, this concept of just cause is valuable as a, in Hegel's term,[249] dialectical concept. According to Hegel, dialectics means the process of superseding contradicting and polar elements into a higher reality, which is accomplished by the moving of the world.[250] Thus, there is a historical dimension in Hegel's dialectics – "the past is pregnant, waiting to deliver the future."[251] Applying such rationale here, this paper's concept of just cause clearly contains an inherent contradiction—from a theoretical perspective, just cause requires an exogenous cause, but from a practical perspective, it amounts to granting states a certain level of liberty to do espionage without cause. However, shall we recognize the historical dimension or the temporal dimension, this concept of just cause would be meaningful because its inherent contradiction can or at least might be transcended through the development of liberal democracy and liberal world order. Thus, although Bitton's approach justifies espionage, this paper does not eliminate the possibility that espionage without a specific just cause might be regarded as illegal at some future point. This approach implies the imperfectness of the current world but also contains the potential of a better world order in which states can cooperate with each other because they share a liberal and transparent structure.

V.A Just Intelligence Framework for the *Lex Specialis* of Peacetime Espionage

a. From the Just War Tradition to the Just Intelligence Theory

---

[249] *See Hegel's Dialectics*, STAN. ENCYC. of PHIL. (JUN. 3, 2016), https://plato.stanford.edu/entries/hegel-dialectics/ (Oct. 3, 2022, 3:05 PM) [https://perma.cc/NYW9-BKQ5].

[250] *See id.*

[251] *See, e.g.,* Augusto César Moreira Lima, *A Brazilian Perspective on Jurisprudence: Miguel Reale's Tridimensional Theory of Law*, 10 OR. REV. INT'L L. 77, 123 (2008).

The just war theory has been presented for more than two thousand years and developed by many prestigious philosophers, including Cicero,[252] Augustine,[253] Aquinas,[254] Grotius,[255] and Michael Walzer.[256] It comprises a number of "recurrent issues and themes in the discussion of warfare . . . reflecting a general philosophical orientation towards the subject."[257] The essence of the just war tradition lies in the balance between maintaining peace and stability and granting the public authorities to retain the capacity to use force for national or international security.[258] Recently, philosophers have increasingly recognized the applicability of the just war framework to intelligence activities. As Sir David Omand and Mark Phythian observe, such adoption of the just war theory to intelligence represents "one of the most thoughtful dimensions of Intelligence Studies in recent years."[259]

To begin with, in a 2005 lecture, Michael Quinlan systematically examined the relationship between just war theory and the ethics of intelligence activities.[260] He introduces the concept of *jus ad intelligentiam* and *jus in intelligentia* to analyze, respectively, a state's resort to

---

[252] *See generally* CICERO, De OFFICIIS (44 B.C.E.).
[253] *See generally* ST. AUGUSTINE, THE CITY OF GOD (426).
[254] *See St. Thomas Aquinas Discusses the Three Conditions for a Just War*, ONLINE LIBR. OF L., http://files.libertyfund.org/files/542/Cicero_0265.pdf (last visited OCT. 3, 2022) [https://perma.cc/5G5E-5FWV].
[255] *See Just War Theory*, INTERNET ENCYCLOPEDIA OF PHIL., https://iep.utm.edu/justwar/ (last visited Oct. 19, 2022) [https://perma.cc/QQE6-ANG6].
[256] *See* MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS (1978).
[257] IAN CLARK, WAGING WAR: A PHILOSOPHICAL INTRODUCTION 31 (1988).
[258] *See, e.g.*, BRIAN OREND, MORALITY OF WAR 9 (2006); JAMES TURNER JOHNSON, JUST WAR TRADITION AND THE RESTRAINT OF WAR: A MORAL AND HISTORICAL INQUIRY xxi (1981) [https://perma.cc/FA8F-Z639].
[259] *See* Sir David Omand & Mark Phythian, *Ethics and Intelligence: A Debate*, 26 INT'L J. OF INTEL. AND COUNTERINTELLIGENCE 38, 42 (2013) [https://perma.cc/TN7G-997P].
[260] *See* Michael Quinlan, *Just Intelligence: Prolegomena to an Ethical Theory*, CTR. FOR INTEL. AND INT'L SEC. STUD. ANN. LECTURE (Mar. 15, 2007), https://doi.org/10.1080/02684520701200715;
see generally Brian Auten, *Just Intelligence, Just Surveillance, & The Least Intrusive Standard*, PROVIDENCE (Sep. 23, 2016), https://providencemag.com/2016/09/just-intelligence-just-surveillance-least-intrusive-standard/ [https://perma.cc/XD45-B7MM].

intelligence activities and execution of intelligence activities.[261] Thereafter, the just intelligence theory has been further developed by many scholars.[262]

During its development, some scholars noticed that the concept of intelligence activities is too broad and thus hard to operate.[263] For example, the ethical considerations for covert coup operations will clearly not be identical to that for peacetime espionage. Whereas all intelligence activities can arguably be analyzed under the general just intelligence framework, the exact contents within it should differ. Thus, in 2013, Kevin Macnish coined the concept of *jus ad speculandum* and *jus in speculando* to analyze domestic surveillance.[264] Whereas Macnish's framework also contains elements like just cause and proportionality, it also includes some unique components like the "least intrusive standard" test.[265] Besides, there are also some scholars who, while generally accepting the just intelligence theory, doubt its applicability to mass surveillance and argue that the latter should be justified under a policing framework by consent.[266] Thus, this paper will use Lubin's terminologies (*jus ad explorationem*, *jus in exploratione*, and *jus post explorationem*) because its focus is only on espionage.

Before introducing this paper's framework, I will first rebut an argument that many scholars have made against the just intelligence theory. The argument highlights one key difference between espionage and war – whereas war is an "exceptional state," espionage is a "constant state."[267] If this is true, it also seems to be an argument against the *lex specialis* of peacetime espionage. Besides, some argue that since the just war theory

---

[261] *See* Quinlan, *supra* note 261, at 3.
[262] *See, e.g.*, Sir Omand & Phythian, *supra* note 260; Ross Bellaby, *What's the Harm? The Ethics of Intelligence Collection*, 27 INTEL. AND NAT'L SEC. 93 (2012); Plouffe Jr., *supra* note *1*; Sir David Omand GCB, *Ethical Guidelines in Using Secret Intelligence for Public Security*, 19 CAMBRIDGE REV. OF INT'L AFF. 613 (2006) [https://perma.cc/J6PQ-GZXW]; Angela Gendron, *Just War, Just Intelligence: An Ethical Framework for Foreign Espionage*, 18 INT'L J. OF INTEL. AND COUNTERINTELLIGENCE 398 (2005).
[263] *See* Sir Omand & Phythian, *supra* note 260.
[264] Kevin Macnish, *Just Surveillance? Towards a Normative Theory of Surveillance*, 12 SURVEILLANCE & SOC'Y 142, 147 (2014) [https://perma.cc/VLE3-Y7QU].
[265] *See* Auten, *supra* note 261.
[266] *See* Adam Diderichsen & Kira Vrist Rønn, *Intelligence by consent: on the Inadequacy of Just War Theory as a framework for intelligence ethics*, 32 INTEL. AND NAT'L SEC. 479, 482 (2017) [https://perma.cc/XWG6-TRZU].
[267] *See* Sir Omand & Phythian, *supra* note 260, at 42.

only applies to an exceptional state, the concept of just cause can only comprise self-defense and international security.[268] Since espionage can be not unlawful even without such specific justifications, these scholars argue that it is not proper to analyze espionage and war under similar frameworks.[269]

There are two reasons why this argument fails. First, this argument underestimates the value of the just war tradition. As Quinlan explained, there is a value of the just war framework unrelated to war—it provides a general methodology to analyze state activities that "at least in some respects cannot be conducted effectively without cutting across normal moral expectations, but which is essential for public purposes that seem plainly of compelling moral necessity and rightness."[270] Thus, it is not unreasonable to analyze espionage under a similar framework because notwithstanding the clear difference between war and espionage, both can present this ethical dilemma for a state to balance the need for an activity that derives from the fundamental nature or duty of a sovereign and the unethicality of such an activity.

Second, the objectors seem to presume that the line between exceptional state and constant state is always clear, but this is not true. For example, in today's world, one can equally say that the war against terror is a constant state. Similarly, according to this paper's dialectical approach to just cause for espionage that explores unknown unknowns, one can reasonably argue that we are in an exceptional state where states are not fulfilling their transparency duties, and such an exceptional state will, or at least might, end in the future, just like the war on terror might not be last forever.

The following sections will introduce elements of *jus ad explorationem* and *jus in exploratione* in this paper's framework. Since the intent of this paper is to illustrate the necessary components of a just espionage framework instead to develop a fully comprehensive one, my framework will exclude some factors that are suspicious or controversial even if they are very often invoked by philosophers studying intelligence ethics.

---

[268] *See* Bitton, *supra* 238 at 1017–21.
[269] *Id.* at 1018.
[270] *See* Quinlan, *supra* note 261, at 6.

b. Jus ad Explorationem

1. Just Cause

The first indispensable element of *jus ad explorationem* is the principle of just cause. Just cause has always been one of the most vital factors in the just ear tradition as it interrogates the justification for going to war.[271] According to Thomas Aquinas, a prerequisite for going to war is that "there must be some reason or injury to give cause" so that the target state is "deserve[d]" to be attacked on account of its fault.[272] Originally, Grotius argued that the sole just cause for war is self-defense.[273] But nowadays, a state is also authorized to attack another state to protect international order when there is a U.N. Security Council authorization.[274] Besides, according to some states like the U.K., there is also a right to humanitarian intervention—the right to use force against a state to solve its humanitarian crisis or stop its human rights violations.[275]

These justifications also apply to espionage. However, as aforementioned, they do not justify espionage to explore unknown unknowns. Thus, this paper adopts a structural approach to the just cause principle. On the most basic level, since states' failure to fulfill their transparency duty, all states have a just cause to explore other states' strategic intentions or willingness (and ability) to conduct a surprise attack. This most fundamental cause is a dialectical concept that has a temporal dimension, which means that whereas in a future time, states might lose this causation to do espionage against a specific state, because the latter has a highly developed liberal deliberation process, as of now and at this historical moment, this element gives all states a basic right to espionage on each other without cause.

During such basic level espionage, or because of the occurrence of other incidents, a state might find another state's illegal intents or problematic behaviors, which will give the former one or several higher-

---

[271] *See* Orend, *supra* note 259, at 9.
[272] THOMAS AQUINAS, SUMMA THEOLOGICA 1360 (Fathers of the English Dominican Province, trans. 1911) (1947).
[273] *See* Grotius, *supra* note 9.
[274] *See* U.N. Charter art. 51.
[275] *See* Edward Newman, *Exploring the UK's Doctrine of Humanitarian Intervention*, 4 INT'L PEACEKEEPING 632, 642 (2021) [https://perma.cc/5KGM-N9J8].

level just causes for conducting more intrusive espionage activities. Such just causes shall at least include self-defense, protecting international order, protecting human rights, and assessing another state's compliance with its treaty or other international obligations.

Note that the different elements of *jus ad explorationem* are not totally independent of each other, so the type and degree of just cause are relevant to other elements. For example, when a state only has a basic level cause to explore unknown unknowns, it will have a higher burden of proof and a possible higher burden to meet such as the macro-proportionality requirement.[276]

2. Just Intention

The second indispensable element of *jus ad explorationem* is just intention. Unlike just cause, just intention is a subjective element, which illustrates that for a war/espionage to be justified, it is "not sufficient that things turn out for the best."[277] Just intention requires a state to, at least, in Aquinas's words, an intention to promote good and to avoid evil.[278] Thus, the four improper intentions identified by Lubin's paper are also illegal under this paper's framework.[279] Besides, it is commonly agreed that there must be a close nexus between just intention and just cause so that a state cannot rely on sham causations. For example, if a state claims that it will conduct espionage activities because of the target's state's violation of human rights, its espionage will be illegal if people later find out that the real intention was to steal the target state's trade secrets.[280]

3. Correct Authority

The third indispensable element of *jus ad explorationem* is correct authority. As explained by Aquinas, "the ruler for whom the war is to be fought must have the authority to do so and a private person does not have the right to make war."[281] The reason for this requirement is that war is inherently immoral, and the just war tradition holds that the right to resort

---

[276] *See, e.g.*, Bellaby, *supra* note 263, at 110.
[277] *See* DOUGLAS P. LACKEY, THE ETHICS OF WAR AND PEACE 32 (1989).
[278] *See* AQUINAS, *supra* note 273, at 1359–60.
[279] *See* Lubin, *supra* note 28, at 36-42.
[280] *See, e.g.*, Macnish, *supra* note 265, at 148.
[281] *See* AQUINAS, *supra* note 273, at 1360.

to such necessary evil is limited to states or sovereigns. As applied to intelligence activities, however, it is improper to read this element as a *per se* ban on private espionage. On the one end, if a private actor collects intelligence in a way that does not otherwise violate international law (e.g., open-source intelligence collection), there is no need to resort to the *lex specialis* of espionage, and its action is not illegal. On the other end, even if the *lex specialis* of espionage is triggered, a state is still authorized to outsource intelligence to private actors if such authorization does not involve inherent sovereign functions (e.g., not giving the private actor improperly broad discretion).

4. Macro-Proportionality

The last indispensable element of *jus ad explorationem* is macro-proportionality. The principle of proportionality is both a *jus ad explorationem* principle and a *jus in exploratione* principle. The former is commonly referred to as "macro-proportionality" because it requires that a state can only conduct a particular espionage activity if the foreseeable damage is proportionate to the occasioning cause.[282] In calculating the foreseeable damage, this paper agrees with Deeks in that injuries to individual rights should be weighted more heavily as compared to injuries to state rights.

5. Other Factors

There are two other factors that philosophers often invoke, but this paper does not incorporate them because they are highly controversial. The first is the principle of last resort. It is a fundamental principle in the just war tradition, which holds that even if it is sometimes necessary and morally justifiable, but the just cause could be achieved through non-violence means, then the party has a moral duty to prefer these methods.[283] Some philosophers argued that the "last" here does not mean "the final move in a chronological series of actions."[284] Instead, what it demands is that actors "carefully evaluate all the different strategies that might bring

[282] *See, e.g.*, Macnish, *supra* note 265, at 150.
[283] *See* RICHARD BRIAN MILLER, INTERPRETATIONS OF CONFLICT: ETHICS, PACIFISM, AND THE JUST-WAR TRADITION 14 (1991).
[284] ROBERT L. PHILLIPS, WAR AND JUSTICE 14 (1984).

about the desired end, selecting force as it appears to be the only feasible strategy for securing those ends."[285] Thus, they argue that the last resort principle means that a state cannot espionage to collect information that can be acquired through open source or other lawful means. However, unlike warfare, intelligence needs to be corroborated, and it is rarely the case that a state can know whether particular open-source information is reliable without corroborating it with secret information. Thus, I do not think the last resort principle should be included. Another principle is the requirement that a state must have a reasonable prospect of success.[286] This element is problematic for similar reasons—you will not know whether you can get the information you need unless you first try to collect it.

c. Jus in Exploratione

1. Discrimination

The first indispensable element of *jus in exploratione* is the principle of discrimination. Under the just war tradition, a state is prohibited from directly targeting civilians but can legally target combatants.[287] The underlying reason for this principle is like what Deeks described as "tacit consent"[288]—a soldier can be targeted because he has "waived or temporarily suspended his normal protective rights" by joining the army[289]

Applying this principle to espionage activities, a state must make a distinction between people who are working in the intelligence community or holding other sensitive positions and those who are not. At the one end, as Tony Pfaff and Jeffery R. Tiel explained, "consent to participate in the world of national security on all levels of a country's self-defence structure together with the quality of the information possessed" justifies targeting.[290] At the other end, when a person clearly has no connection with

---

[285] ALEX J. BELLAMY, JUST WARS: FROM CICERO TO IRAQ 123 (2006).
[286] *See, e.g.*, Macnish, *supra* note 265 at 150.
[287] Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3.
[288] Deeks, *supra* note 17, at 646–48.
[289] Walzer, *supra* note 257, at 145.
[290] Tony Pfaff & Jeffery R. Tiel, *The ethics of espionage*, 3 J. OF MIL. ETHICS 1, 1–15 (2004).

a state's intelligence agencies and does not possess state secrets, it is likely illegal to surveil him.

2. Micro-Proportionality

Whereas a state cannot directly target civilians, the just war tradition allows some level of collateral injuries to them, provided that the targeting state does not violate the principle of micro-proportionality. The difference between macro-proportionality and micro-proportionality is that the former concerns the legality of a state's decision to conduct espionage activities against a particular state, while the latter concerns the legality of a state's particular espionage activities. A state will violate the principle of micro-proportionality if the foreseeable value of a particular espionage activity is disproportionate to the damages it can foreseeably cause. Thus, a state will likely commit a wrong when it employs intrusive methods of espionage to gain information that is of very low value. Similarly, a mass surveillance program will require a more significant justification than an espionage activity targeting a foreign intelligence officer because the former can foreseeably cause more damage. In calculating damages, this paper also agrees with Deeks that the injuries to individual rights should be weighed more heavily compared to that to state rights.

3. No Means or Methods *Mala in Se*

The last indispensable principle of *jus in exploratione* is the prohibition of means and methods of espionage that are *mala in se*. *Mala in se* is the correspondent of *mala prohibita* - whereas the reason why an action that is *mala prohibita* is illegal lies in the fact that it contradicts a positive law, an action that is *malum in se* is illegal even without human-made laws because it is inherently wrong and thus is forbidden by "superior laws."[291] Under the just war tradition, some activities and methods of warfare like rape[292] and perfidy[293] are recognized as *mala in se* and will under no circumstances be legal. Similarly, under the framework

---

[291] WILLIAM BLACKSTONE, COMMENTARIES 54 (1st ed., 1765) [https://perma.cc/5SD9-TM8K].
[292] *See, e.g.*, George R. Lucas, Jr., *Automated Warfare*, 25 STAN. L. & POL'Y REV. 317, 339 n.24 (2014) [https://perma.cc/83F8-A898].
[293] Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts art. 37, June 8, 1977, 1125 U.N.T.S. 3.

for the *lex specialis* of peacetime espionage, certain means and methods of espionage like using torture to solicit information should also be regarded as inherently illegal.

d. Jus post Explorationem

Jus post explorationem should specify a state's duty after intelligence is collected. This is the most undeveloped part of today's intelligence studies as no philosophers or legal scholars have systematically examined it.[294] It would be beyond this paper's scope to fully discuss this unexplored field but *jus post explorationem* shall at least require "proper oversight from outside the intelligence community."[295] Other considerations might include limiting the retention of data, restricting query of intelligence databases, periodically reviewing espionage activities, etc.

VI. Conclusion

This paper proposed a new approach to analyzing the lawfulness of espionage activities under international law. It began by summarizing the key arguments of the three traditional approaches and explained why these traditional *per se* approaches are no longer acceptable. Then, the paper introduced frontier scholarships that advocate for a piecemeal approach to espionage. This paper identified a thread of the development of their approaches—from proposing a new analytical method to proposing a new secondary law and to proposing a new primary *lex specialis* of peacetime espionage. This paper found that whereas their approaches provided some valuable insights, they are neither ideal nor comprehensive. Thus, this paper proposed a new framework for the *lex specialis* of peacetime espionage. It introduced a dialectical concept of just cause for peacetime espionage that explores unknown unknowns and solved the pragmatism challenge to espionage law. It then applied the just intelligence theory and developed a comprehensive framework that incorporated the merits of recent piecemeal approach scholarships.

---

[294] CÉCILE FABRE, SPYING THROUGH A GLASS DARKLY: THE ETHICS OF ESPIONAGE AND COUNTER-INTELLIGENCE 24 n.24 (2022) (noticing that scholars of just intelligence theory have not focused on *jus post intelligentiam*).

[295] Sir David Omand, *The Dilemmas of Using Secret Intelligence for Public Security* 165, *in* THE NEW PROTECTIVE STATE: GOVERNMENT, INTELLIGENCE AND TERRORISM (Peter Hennessy ed., 2007).