Chicago Journal of International Law

Volume 18 | Number 1 Article 10

7-1-2017

Rethinking Espionage in the Modern Era

Darien Pun

Rethinking Espionage in the Modern Era

Darien Pun*

Abstract

Espionage's permissibility under international law remains largely unsettled; no global regulation exists for this important state activity. This Comment first surveys the longstanding scholarship regarding espionage's legality, and proceeds to highlight the reasons why regulation continues to be absent. Then by examining cyber technology's transformative effects in this field, this Comment argues that this ambiguity is no longer sustainable, as espionage becomes more indistinguishable from low-level warfare, more efficient, more visible, and more involved in information wars. This prompts a need for the international community to set clear guidelines for allowable espionage activities. This Comment suggests that a possible solution, given the barriers prohibiting the development of wide-reaching regulations of cyber espionage, is to begin by incrementally carving out specific activities—starting with those that transcends states' strategic calculus. An example then provided is the broad disallowance of private entities to engage in cyber espionage.

Table of Contents

* J. D. Candidate, 2018, The University of Chicago Law School. I would like to thank Professor Abebe for his patience and guidance throughout the writing process, and the editors of the *Chicago Journal of International Law* for their thoughtful suggestions.

I. INTRODUCTION

Espionage has existed for a long time. In fact, it is often referred to as the "world's second oldest profession."[1] Mentions of spies can be found in the Bible,[2] in ancient Greece,[3] and in ancient China.[4] Espionage continued to persist and evolve, with now over a hundred global intelligence agencies responsible for related activities,[5] operated by countries across the economic development spectrum.[6] For such a widely-used tool though, espionage during peacetime faces no form of international regulation.[7]

The art of spying has a peculiar dual identity. On one hand, states openly acknowledge their own intelligence agencies and deem their activities legitimate and necessary to protect national security. On the other hand, states aggressively denunciate foreign espionage and criminalize any domestic support of foreign espionage. As one commentator puts it, the mentality appears to be: "we and our friends merely gather information; you and your type violate sovereignty."[8] International law struggles with clarity in the face of this strange "doublethink" tension,[9] plagued with seemingly ideological contradictions.[10]

Like many other fields, espionage is being transformed by the "cyber" prefix or descriptor. Cyber space simultaneously makes offensive information gathering more valuable and cyber defense protections more necessary because of the sheer volume of data now available. Cyber intrusions have become a frequent concern and are aimed at a diverse range of targets.[11] According to NATO Secretary

---

1 *See* Paul Reynolds, *The World's Second Oldest Profession*, BBC NEWS (Feb. 26, 2004), https://perma.cc/B9KM-E5E5.

2 *Joshua* 2:1.

3 *See generally* J. A. Richmond, *Spies in Ancient Greece*, 45 GREECE & ROME 1 (1998).

4 *See* SUN TZU, THE ART OF WAR 77–82 (J. Clavell ed., 1981).

5 MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 11 (4th ed. 2009). For a more descriptive account of various intelligence organizations around the world, see GLENN HASTEDT, ESPIONAGE 75–101 (2003).

6 *See* LOWENTHAL, *supra* note 5, at 11; HASTEDT, *supra* note 5, at 97 ("Intelligence organizations and the practice of espionage are not the monopoly of the great world powers. . . . Espionage is practiced by states of all sizes.").

7 *See* Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1072 (2006) ("Despite its relative importance in the conduct of international affairs, there are few treaties that deal with it directly.").

8 *See id.* at 1072.

9 *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR 37 (2008).

10 *See* A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 607–23 (2007) (describing the duality in espionage).

11 *See, for example*, Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites across U.S.*, N.Y. TIMES (Oct. 21, 2016), http://www.nytimes.com/2016/10/22/business/internet-problems-

General, Anders Fogh Rasmussen, there are now more than 100 daily cyber intrusion attempts on NATO headquarters, and over 1,000 daily cyber intrusion attempts on U.S. military and civilian networks.[12] These attacks allegedly originate from over 100 countries,[13] showing that this is a dispersed phenomenon, not restricted to a handful of capable states. The recent hacking of the U.S. Democratic National Committee's (DNC) emails, allegedly by Russian actors, highlights cyber intrusions' creeping invasion into significant public matters.[14] Meanwhile, from an economic standpoint, cyber intrusions are projected to cost the global economy $2.1 trillion by 2019.[15]

Driven by this structural evolution, this Comment argues that states need to establish clearer guidelines for permissible espionage activity, and can do so by carving out narrow activities within espionage to overcome strategic state considerations. Section II first sets out what espionage precisely is, to establish the parameters of this Comment. Section III outlines the existing ambiguity of espionage in existing international law. Section IV then looks at the difficulties of regulating espionage to explain why the ambiguity has persisted. Section V argues the existence of several catalysts and unique problems presented by cyber espionage that will likely encourage reconsideration of its legal ambiguity, mainly the difficulties of identifying the appropriate threat level and response of any intrusion. The Section then reevaluates the traditional views on the legality of espionage given the emergence of cyber technology. Section VI concludes by presenting an exemplary norm states may pursue to limit or attempt to eradicate the consequences of lingering uncertainties by carving out specific activities as impermissible.

---

attack.html?rref=collection%2Ftimestopic%2FCyberwarfare&_r=0 (reporting on intrusions against commercial websites such as Netflix and Airbnb, social media outlets such as Twitter, and mass press outlets such as the New York Times).

12 *See* Siobhan Gorman & Stephen Fidler, *Cyber Attacks Test Pentagon, Allies and Foes*, WALL ST. J. (Sept. 25, 2010), http://www.wsj.com/articles/SB10001424052748703793804575511961264943300.

13 *Id.*

14 *See, for example*, Carol E. Lee et al., *Obama Suggests Russia's Putin Had Role in Election Hacking*, WALL ST. J. (Dec. 16, 2016), https://www.wsj.com/articles/obama-likely-to-field-questions-on-russia-syria-and-donald-trump-1481908017 (describing the recent alleged hack of the U.S. Democratic National Committee by Russian actors).

15 PRESS RELEASE, JUNIPER RESEARCH, *Cybercrime Will Cost Businesses Over $2 Trillion by 2019* (May 12, 2015), https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion. Cyber espionage and cyber-attacks are the two activities often aggregated as cyber intrusion. As a point of early clarification, the division between the two is fine, if even existent. This is further explored in Section V, *infra*.

II. WHAT IS (CYBER) ESPIONAGE?

There has always been difficulty in pinning down the precise contours of what "espionage" entails. The words espionage and spy tend to conjure images from the works of Ian Fleming and Tom Clancy as depicted through various forms of mainstream media. For example, the CIA even highlights this misperception on its own website for children.[16]

By surveying various sources and searching for common themes, this Comment settles on the following definition: the unauthorized intentional collection of information by states.[17] This embodies a few key components: (1) espionage refers to the collection of information; (2) the collection of the information is disallowed by the targeted state; (3) the distinctive use of the term "information" rather than "intelligence"; and (4) it involves only activities affiliated with states.[18] These are addressed in turn. Cyber espionage is then simply the use of cyber technology to achieve the goals of traditional espionage.

First, espionage is a segment of the larger intelligence cycle, which in turn describes the sets of activities designed to produce the information necessary for policymakers' decision-making.[19] This cycle generally involves five steps: tasking,

---

16 *See* CIA, *Who We Are & What We Do: Our Mission*, https://perma.cc/67GL-VG4P (last visited Jan. 23, 2017) ("A lot of people still think that our employees lurk around in trench coats, send coded messages, and use exotic equipment like hidden cameras and secret phones to do their job.").

17 For other definitions of espionage, see 18 U.S.C. § 793 (2016) ("[O]btaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation"); SOVA CENTER FOR INFORMATION AND ANALYSIS, *Duma Adopts Expansion of Criminal Code Articles on Treason, Espionage at First Reading* (Sept. 28, 2012), https://perma.cc/J6NZ-ZBTR [hereinafter "SOVA Center"] ("The transmission, and likewise collection, storage, or abduction in order to transfer to a foreign state, international or foreign organization or their representatives information constituting a state secret, and the transfer or collection by a foreign intelligence service or a person acting on its behalf, of other information for use threatening to the security of the Russian Federation (espionage), if such acts are committed by a foreign national or a stateless person – shall be punished with imprisonment for a term of ten to twenty years"); MI5, WHAT WE DO: ESPIONAGE, https://perma.cc/9DWG-6UZ4 (last visited Jan. 14, 2017) ("[T]he process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems)."); *Espionage*, Black's Law Dictionary (10th ed., 2014) ("The activity of using spies to collect information about what another government or company is doing or plans to do.").

18 Some commentators have included intention as an element to prevent making unwitting participants liable. This Comment's definition excludes it since it is not clear in the cyber context whether unwitting states should be held liable or not to reduce the difficulties of attribution. For an explanation of the debate over the application of neutrality in cyberwarfare, see Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 855–56 (2012).

19 *See* HASTEDT, *supra* note 5, at 52.

collection, processing and evaluating, analysis and production, and feedback.[20] Espionage falls within the second step.

Covert action[21] is a field that requires explicit attention since it tends to be included in espionage.[22] This Comment will bifurcate the two by reserving espionage to collection, and covert action to acting on information in pursuit of national interests. This distinction is imprecise, and becomes even more so in the cyber context.[23] Common forms of espionage would include intercepting correspondence and recording the movement of military assets. The following examples, in contrast, might provide more clarity as to what covert action entails: the destruction of power stations in Nicaragua to undermine the Marxist-oriented *Sandinista* regime, assassination of foreign leaders, and propaganda during the Cold War transmitting anti-communist themes into nations under the purview of the Soviet Union.[24]

Second, espionage only encompasses the collection of information not made publicly available. The gathering of open source information is a separate activity,[25] one that is not subject to any legal concerns.[26] The state is presumptively inviting others to view it.

Third, intelligence is considered a subset of information, [27] tailored to the purposes of national security.[28] Despite debates over the appropriateness of using

---

20 *See id.*

21 *See, for example*, 50 U.S.C. § 3093(e)(1) (2016) ("an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include . . . activities the primary purpose of which is to acquire intelligence").

22 *See, for example*, MI5, *supra* note 17 (including covert action in their definition of espionage).

23 *See* Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1164 (2011) (arguing that the distinction with cyber intrusions is so unclear that it is better to analyze cyberespionage under a covert action framework).

24 *See* LOCH K. JOHNSON, *Preface* to STRATEGIC INTELLIGENCE: UNDERSTANDING THE HIDDEN SIDE OF GOVERNMENT, at xii (Loch K. Johnson ed., 2007).

25 *See* MI5, *supra* note 17 (defining open information gathering as "[t]he gathering of publicly available information is a routine activity of diplomatic staff, military attachés and trade delegations. They use open sources such as the media, conferences, diplomatic events and trade fairs, and through open contact with host government representatives").

26 *See* Chesterman, *supra* note 7, at 1073 (stating that "intelligence analysis that relies on open source information is legally unproblematic"); *id.* at 1074 (indicating that to obtain "secret intelligence" means to get information "*without the consent* of the state that controls the information") (emphasis added); *see also, for example*, SOVA CENTER, *supra* note 17 (referring to the relevant information for espionage as "state secrets"); MI5, *supra* note 17 (defining espionage as "the process of obtaining information that is not normally publicly available"). *But see* 18 U.S.C. § 793 (2016) (referring to "information respecting the national defense" instead of a secrecy determination).

27 *See* LOWENTHAL, *supra* note 5, at 2.

28 *See id.* at 8.

"intelligence" or "information," [29] this Comment does not apply the more restrictive term, and instead focuses on the target state's authorization for accessing the collected information.[30] The definitional difference turns on the classification by the acting state, which, when defining espionage, undercuts the target state's own determination of how important certain information is. To elaborate, insisting on the use of "intelligence" may create situations where states perpetrating espionage insist that the information acquired was not important enough to rise to "intelligence" in the face of condemnation by the victim state. Understandably, this matters mainly in limited situations where two countries disagree and the same information diverges in its classification (that is, State X considers it information but State Y considers it intelligence).

Lastly, the qualification of state activity is essential to remove two important groups of potential participants. First, there are those whose roles involve a clear allowance to legally gather information (for example, news reporters, scholars, and other similar individuals or organizations).[31] This is an extension of the secret and open information distinction. Second, the acts of private individuals and private organizations generally fall under criminal law, and do not implicate the same international law issues.[32]

III. LEGALITY OF TRADITIONAL ESPIONAGE

Espionage has an ambiguous existence in international law. Before exploring this further, the Comment must draw some initial distinctions. The following discussion on the legality of espionage refers to the concept of information collection in the abstract. Although it is unclear in international law whether states in general have a lawful right to spy on other states, the disallowance of certain activities within espionage is clearer. For example, international law is clear on

---

29 For instance, Michael Warner, a former historian for the Central Intelligence Agency (CIA), believes that although information is not wrong *per se*, the term "is too vague to provide real guidance" for those involved in the intelligence community. *See* Michael Warner, *Wanted: A Definition of "Intelligence"*, 46(3) STUD. IN INTELLIGENCE (UNCLASSIFIED EDITION) (2002), https://perma.cc/JEV5-5H8X. Instead, he offers his own definition of intelligence as "secret, state activity to understand or influence foreign entities." *Id.*

30 This Comment uses terms of art such as intelligence agencies and intelligence operations; the distinction made here simply reflects a belief that espionage itself should be defined broadly rather than narrowly.

31 This is important to distinguish overgeneralizing the problem to individuals collecting information online via legal means such as basic online research through publicly accessible databases, or observance of actions that happen in public.

32 This is a descriptive point. Section VI, *infra*, suggests that states should reconsider this approach under normative considerations.

prohibiting the use of torture and cruel, inhuman, or degrading treatment to extract information.[33]

Espionage conducted during wartime and espionage conducted during peacetime have also received different treatments. The Comment will focus on the latter since the former has received direct attention in formal legal instruments throughout history.[34] They generally indicate that espionage is presumably an accepted reality during times of war,[35] and attempts to outline the treatment of spies. Understandably, as one author puts it, the distinction between peacetime and wartime is becoming an "anachronism" since various conflicts in the recent era have gone on without any formal declaration of war.[36] This Comment proceeds on the assumption that a distinction persists.

The status of espionage during times of peace is less certain.[37] There are two main academic views. First, scholarship traditionally describes international law as being silent, without any clear prohibition against espionage.[38] This breaks down into two subsets of opinions: espionage is not illegal, and espionage is neither illegal nor legal. Second, there is a minority view that espionage in fact does violate

---

33 *See* Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SEC. L. & POL'Y 179, 186–93 (2011).

34 *See, for example*, Project of an International Declaration concerning the Laws and Customs of War art. 20, Aug. 27, 1874, [hereinafter Brussels Declaration]; The Hague Convention (IV) Respecting the Laws and Customs of War on Land, Annex arts. 29–30, Oct. 18, 1907, 36 Stat. 2259, 205 Consol. T.S. 263; Geneva Convention Relative to the Protection of Civilian Persons in Time of War art. 5, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter the Geneva Convention]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 45(3) and 46(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]. For a more detailed account of the history of the development of international legal instruments outlining espionage during times of armed conflict, see Lt. Col. Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 330–38 (1996).

35 *See* QUINCY WRIGHT, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, 12 (1962) ("The legitimacy of espionage in time of war arises from the absence of any general obligation of belligerents to respect the territory or government of the enemy state, and from the lack of any specific convention against it.").

36 *See* HASTEDT, *supra* note 5, at 48–49.

37 *See* Commander Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 218 (1999) ("No international convention has ever addressed the legality of peacetime espionage.").

38 *See* Radsan, *supra* note 10, at 603–04 (discussing the views of various scholars who believe that espionage is not illegal); Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 600 (2016) ("Conventional wisdom holds that international law should matter little to a state when it conducts intelligence activities."); *see also* Gary Brown, *Spying and Fighting in Cyberspace: What is Which?*, 8 J. NAT'L SEC. L. & POL'Y 621, 622 (2016) ("States freely engage in espionage and generally accept it from other States, with results limited to punishing spies under domestic law and the expulsion of diplomats.").

international law because it runs contrary to customary international law, the International Covenant on Civil and Political Rights, and the Vienna Convention on Diplomatic Relations.[39]

The traditional view is more readily asserted in the literature, but recent events such as the retaliation by the Obama administration against Russian intelligence operations may be signaling a reorientation.[40] For now though, as Professor Forcese puts it, "the international community seems content with an artful ambiguity on the question" of the international legality underlying espionage.[41]

A. Espionage as a Permissible Activity

There are various arguments advanced to support this view. The common underlying principle justifying the lack of prohibition is mainly the practicality of using espionage as a necessary means of statecraft and protection of national security against foreign intervention or intrusion. The legal versus not legal or illegal view is hard to distinguish since states both condemn and condone the activity.[42]

1. Absence of Impermissibility.

Some scholars believe the absence of explicit international regulation and states' wide engagement in espionage makes the behavior permissible.[43] The lack of explicit historical prohibition of peacetime espionage in international law has

---

39 *See* Deeks, *supra* note 38, at 612 ("A competing narrative has developed . . . Some actors today reject these [legal or not illegal] positions, arguing that international law prohibits espionage and other intrusive intelligence agencies."); Luke Pelican, *Peacetime Cyber-Espionage: A Dangerous but Necessary Game*, 20 COMMLAW CONSPECTUS 363, 369–74 (2012).

40 *See* Carol E. Lee & Paul Sonne, *U.S. Sanctions Russia over Election Hacking; Moscow Threatens to Retaliate*, WALL ST. J. (Dec. 29, 2016), http://www.wsj.com/articles/u-s-punishes-russia-over-election-hacking-with-sanctions-1483039178; *see also* The White House, *Press Release: Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment* (Dec. 29, 2016), https://perma.cc/335H-ECP2.

41 *See* Forcese, *supra* note 33, at 205.

42 *See* Radsan, *supra* note 10, at 604 ("Under international law, if something were truly legal (or at least not illegal), no state should prosecute those who do it.").

43 *See* Deeks, *supra* note 38, at 608 ("[S]tates and scholars have generally agreed about international law's relation to espionage: International law either fails to regulate spying or affirmatively permits it."); *see also, for example*, Nicole Gaouette, *Ex-CIA Chief: Russian Hackers Trying to 'Mess with Our Heads'*, CNN (Oct. 18, 2016), https://perma.cc/YXM4-96QL (quoting Gen. Michael Hayden, a former head of the CIA, as describing a Russian hack of the Democratic National Committee's emails as "honorable state espionage" and as an activity often engaged in by the CIA).

created a customary norm for its permissibility.[44] This receives support from the 1927 *S.S. Lotus* case by the Permanent Court of International Justice, which articulated an often cited principle in international law, essentially holding permissive whatever is not explicitly prohibited.[45]

Meanwhile, when a spy has been allegedly captured and the behavior is publicly denounced, states rarely come forward to acknowledge the act.[46] Some commentators argue this implies an understanding that the behavior is in fact prohibited by international law.[47] The absence of any comments from the perpetrating state, however, may stem from a belief in the fruitlessness of any collateral negotiations over the prisoner.[48] Arguing for legality might be pointless too, because the targeted nation likely has domestic law in place prohibiting the conduct, and the spy is operating in its jurisdiction.[49]

Nevertheless, the winds seem to be shifting. States, humanitarian organizations, and commercial entities have recently become more hostile towards espionage activities.[50] The Edward Snowden leaks led to wide condemnation of mass surveillance and cyber espionage from victim states.[51] Russian spies had been expelled from the U.S. after condemnation of their intelligence activities during

---

44 *See* Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1094 (2004) ("As a result of its historical acceptance, espionage's legal validity may be grounded in the recognition that 'custom' serves as an authoritative source of international law.").

45 *See* Anthea Elizabeth Roberts, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 AM. J. INT'L L. 757, 776 & n. 199 (2001); s*ee also* Margaret L. Satterthwaite, *Rendered Meaningless: Extraordinary Rendition and The Rule of Law*, 75 GEO. WASH. L. REV. 1333, 1351 & n. 114 (2007) ("According to this principle, States—as sovereign equals—are entitled to act as they please where there are no prohibitive rules to the contrary."). *But see* Hugh Handeyside, *The Lotus Principle in ICJ Jurisprudence: Was The Ship Ever Afloat?*, 29 MICH. J. INT'L L. 71, 72 (2007) (finding discrepancies among interpretations of the case such that "there [does not] appear to be any clear consensus on the decision's core holdings; in fact, commentators have read the decision in alarmingly divergent ways").

46 *See* Wright, *supra* note 35, at 17.

47 *See id.* at 17 ("This would appear to be a case in which frequent practice has not established a rule of law because the practice is accompanied not by a sense of right but by a sense of wrong.").

48 *See* JULIUS STONE, *Legal Problems of Espionage in Conditions of Modern Conflict*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 29, 39 (1962).

49 *See* Deeks, *supra* note 38, at 612.

50 *See* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 328 (2015) ("[T]he Snowden leaks . . . contained information about NSA programs that collected massive amounts of communications information from average citizens, both American and foreign. These disclosures produced significant pressure on the U.S. government . . . to rein in their activities.").

51 *See* Deeks, *supra* note 38, at 643–44.

the 2016 presidential election.[52] The U.S. and China have signed a bilateral treaty curtailing economic espionage.[53] Despite all this, there has yet to be a call for a general shutdown of intelligence agencies.[54] Customary international law will likely continue to accept espionage as a broadly allowable activity, but how intelligence agencies operate may in time have to comport with certain oversights reflecting widely held social values.

2. Statecraft and Preemptory Self-Defense.

Other scholars have argued that the use of espionage is allowable as both a necessary part of statecraft and a means of peremptory self-defense under both the U.N. Charter and customary international law.[55] This view claims espionage serves as a form of either arms control or conflict prevention by making aware the capabilities of other states, serving as a mechanism to promote stability and peace.[56]

The functionalist statecraft position argues the collection of information ultimately serves to facilitate stability in international politics.[57] One commentator likens international politics to a prisoners' dilemma where the flow of information alleviates the potential costs imposed by a lack of trust between parties.[58] The

---

52 *See* Mark Mazzetti & Adam Goldman, *"The Game Will Go On" as U.S. Expels Russian Diplomats*, N.Y. TIMES (Dec. 30, 2016), https://www.nytimes.com/2016/12/30/us/politics/obama-russian-spies.html?_r=0.

53 *See* Kim Zetter, *US and China Reach Historic Agreement on Economic Espionage*, WIRED (Sept. 25, 2015), https://perma.cc/VUH7-VU25.

54 As Section IV will explain, even in the face of pressures to cutback espionage, the tipping point for a reduction in intelligence activities is perched extremely high given strategic cost-benefit considerations.

55 *See* Radsan, *supra* note 10, at 604.

56 *See, for example*, Daniel S. Gressang IV, *The Shortest Distance Between Two Points Lies in Rethinking the Question, in* STRATEGIC INTELLIGENCE: THE INTELLIGENCE CYCLE 123, 125 (Loch K. Johnson ed., 2007) ("Beyond meeting the immediate information needs of decision makers, however, intelligence must also be forward looking, capable of providing decision makers with an accurate and timely assessment of future threats and possible threats, above and beyond the bounds of the immediate."); s*ee also* Scott, *supra* note 37, at 224 ("Intelligence is necessary to give substance and effect to the right of self defense . . . Appropriate defensive preparations cannot be made without information about potential threats.").

57 *See, for example*, Scott, *supra* note 37, at 222–23 (describing the "New Haven School" view of international politics held by scholars such as Myres S. McDougal where "special measures to gather secret information from closed societies are necessary to maintain world public order"). Functionalism refers to a theory of international relations that predicts state cooperation to maximize their own prosperity. For a more detailed description, see Baker, *supra* note 44, at 1097–1102; *see also* HASTEDT, *supra* note 5, at 50 (expressing the danger of surprises for governments as it "invalidates the fundamental assumptions on which policies are based" and acts as a "power multiplier" by the state who surprises its enemies).

58 *See* Chesterman, *supra* note 7, at 1090.

information can lead reluctant parties to negotiate since it reveals the validity of preferences and intentions, and the accuracy of the bargaining positions.[59] Post-negotiations, espionage then serves as a monitoring mechanism, ensuring the parties' on-going compliance with the agreement.[60]

Two concerns confront legalizing espionage purely because of its functional value in improving cooperation.[61] First, there are alternative institutions states can turn to for ensuring compliance, such as a third-party monitor.[62] Second, this view downplays state interest in collecting information for the purpose of bad behavior, such as extortion and coercion.

On the self-defense front, Professor Julius Stone, a distinguished scholar on jurisprudence and international law, defends permissibility by suggesting there is "reciprocally tolerated espionage" for ensuring mutual inspection and maintaining world stability.[63] He posits that the world has a common interest in having no countries be able to conduct a surprise attack.[64] He described espionage as having a "red-light function" and a "green-light function."[65] The former is when espionage is used to serve a common-interest of the states to warn the perpetrating state of any surprise attacks, while the latter is when espionage is used to inform the perpetrating state of an opportunity to strike.[66] This mutual check-and-balance has gotten progressively more important in a world with weapons of mass destruction.[67] However, he recognized a limitation in the inability to differentiate

---

59 *See* Baker, *supra* note 44, at 1106–07; *see also* KRISTIN M. LORD, *National Intelligence in the Age of Transparency*, *in* STRATEGIC INTELLIGENCE: UNDERSTANDING THE HIDDEN SIDE OF GOVERNMENT 181, 184–85 (Loch K. Johnson ed., 2007) (describing the three main arguments made by scholars and policy makers for why greater transparency increases national security and reduces conflict: (1) it "clarif[ies] the intentions of governments and reduces misperceptions"; (2) "reduce[s] uncertainty about the military capabilities of states and prevent[s] leaders from overestimating threats; and (3) "help[s] people to know each other better and humanize other groups, making it harder to use violence against them").

60 *See* Baker, *supra* note 44, at 1109–10.

61 *See* LORD, *supra* note 59, at 181 ("[T]ransparency holds perils as well as promise. It can highlight differences rather than shared values. It can show aggression and hate rather than cooperation and friendship. It can show violations of, not adherence to, global rules and norms. In certain circumstances, it can exacerbate conflicts and make war more likely.").

62 *See, for example*, International Atomic Energy Agency, *About Us: Overview*, https://perma.cc/TSZ9-6J9N (last accessed Jan. 26, 2017).

63 *See* STONE, *supra* note 48, at 31.

64 *See id.* at 40.

65 *Id.*

66 *See id.* at 42–43.

67 *See, for example*, Radsan *supra* note 10, at 606 (discussing the importance of shared intelligence for monitoring purposes using American and Soviet negotiations over nuclear stockpiles during the Cold War as an example).

when something was red-light or green-light. This is extremely problematic since states will naturally reject all activities then as illegitimate.

Another commentator suggests that if self-defense is presumably an inherent right of a state, then the right to conduct espionage is a corollary derivative.[68] This is because effective self-defense presumably requires both the acquisition of information to know when an armed attack might occur, and in order to repel and armed attack, the capabilities of potentially hostile states.[69]

Nonetheless, the self-defense principle is riddled with inherent ambiguity in international law.[70] The right is outlined in Article 51 of the U.N. Charter, allowing "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[71] There has been debate over the interpretation of the language, mainly whether the self-defense is available if and only if an armed attack occurs.[72]

Recent scholarship has described a shift towards an expansive view of the principle because of its more and more aggressive application in modern state practice, essentially a contemporary evolution in customary international law.[73] Historically, the international community has adopted modified formulations of the traditional Caroline test,[74] originally holding anticipatory self-defense as only justified with a showing that its necessity was "instant, overwhelming, leaving no choice of means, and no moment of deliberation."[75] This has been developed and

---

68 *See* Baker, *supra* note 44, at 1096 ("[E]nsur[ing] that the right to self-defense retains substantive meaning, international law must permit states to predict armed attack").

69 *See id.*

70 *See* Sean D. Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILL. L. REV. 699, 706–18 (2005) (presenting four schools of thoughts on the self-defense doctrine).

71 U.N. Charter art. 51. This served only to codify a well-established right to self defense under customary international law.

72 "Armed attack" is a specific term of art that carries certain ambiguities in cyber space as scholarship and international law continues to debate over its application in this new domain. For a detailed discussion of this debate, see CHRISTOPHER S. YOO, *Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures, in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 188–94 (John David Ohlin et al. eds., 2015).

73 For a more thorough discussion on the precedents and justifications of the expanding principle, see generally John Alan Cohan, *The Bush Doctrine and The Emerging Norm of Anticipatory Self-Defense in Customary International Law*, 15 PACE INT'L L. REV. 283 (2003).

74 John Yoo, *Using Force*, 71 U. CHI. L. REV. 729, 741 (2004) ("Most writers on international law consider the Caroline test the leading definition of the permissible use of force in anticipation of an attack.").

75 *Letter from Daniel Webster to Henry Fox (Apr 24, 1841), in* BRITISH DOCUMENTS ON FOREIGN AFFAIRS: REPORTS AND PAPERS FROM THE FOREIGN OFFICE CONFIDENTIAL PRINT (PART I, SER. C) 153, 159 (Kenneth Bourne & D. Cameron Watt, eds., 1986).

refined as requiring imminence or immediacy.[76] The definitional boundaries of this requirement, however, are a subject of controversy.[77] The introduction of cyber technology further complicates the doctrine.[78] Imminence is problematic when applied to espionage. If there is an immediate concern for national security, the self-defense argument can apply in full force. However, it becomes more difficult to support constant espionage, especially between nation states that are not at war or on hostile terms. This is referred to as peacetime espionage, which is presumably much more common.[79]

B. Espionage as an Impermissible Activity

1. Violations of Sovereignty and Territorial Integrity.

Professor Quincy Wright, a renowned scholar in the fields of international law and international relations, is often cited as one of the main supporters of the view that espionage violates international law because there is a duty "to respect the territorial integrity and political independence of other states."[80] Professor Wright reaches this non-intervention doctrine based on Article 2 of the U.N. Charter,[81] which declares "sovereign equality for all its Members,"[82] and prohibits the "threat or use of force against the territorial integrity or political independence to any state,"[83] and the restriction of international "intervention in matters which are essentially within the domestic jurisdiction of any state."[84] He argues that

---

76 *See, for example*, Cohan, *supra* note 73, at 328–30; Yoo, *supra* note 74, at 741.

77 *See, for example*, Cohan, *supra* note 73, at 287–88 (describing the implications of how U.S foreign policy toward Iraq in 2003 broadens temporal allowances, sometimes referred to as "Bush Doctrine").

78 *See, for example*, Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 437–38 (2011) (describing the difficulties of determining the imminence of threats with cyber intrusions, as well as other issues like proportionality). Alluded to earlier in the Comment, and as Section V later explains, cyber intrusions have become a daily issue, which further muddies the applicability and analysis of anticipatory and reactionary actions.

79 Without exact details on the volume of espionage operations, this claim is merely based on the intuition that there appears to be extensive on-going intelligence operations and most developed countries are not "at war" with one-another (regardless of whether relations are amicable).

80 *See* WRIGHT, *supra* note 35, at 12; *see also* Pelican, *supra* note 39, at 371–72 (citing Professor Wright); Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 628 (2007) (citing Professor Wright); Radsan, *supra* note 10, at 32 (citing Professor Wright).

81 *See* WRIGHT, *supra* note 35, at 2–3.

82 U.N. Charter art. 2(1).

83 U.N. Charter art. 2(4).

84 U.N. Charter art. 2(7).

regulating peacetime espionage is up to a state's discretion, and other states have the duty to respect this exercise of domestic jurisdiction.[85]

The non-intervention principle was later upheld by the International Court of Justice in *Nicaragua v. United States* as "forbid[ding] all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely."[86] This finds further support from the language in the *S.S. Lotus* case when the Permanent Court of International Justice declared "the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another State."[87]

Critics of this view often cite the lack of enforcement by any states for these violations as casting doubt on their relevance in customary international law.[88] This is, in essence, the absence of impermissibility argument. However, when Edward Snowden divulged the extent of the NSA's surveillance program in 2013, it drew comments from Brazil, the Bahamas, and Indonesia about espionage and a breach of sovereignty or a violation of international law.[89] The International Court of Justice has also recently held that the sovereignty violation argument is plausible regarding interference with communication by a state, although never definitively ruled on the issue.[90] Again, there are signs of a turning tide.

2. Related International Instruments.

Provision 17 of the International Covenant on Civil and Political Rights states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . . Everyone has the right to the protection of the law against such interference or attacks."[91] This has been invoked recently by some states, alongside the European Convention on Human Rights, to condemn surveillance activities of the NSA and GCHQ conducted on

---

85 *See* WRIGHT, *supra* note 35, at 13.

86 Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 202–209 (June 27).

87 *See* S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7). It is notable that the same case appears to support two divergent views on espionage. *See supra* note 45 and accompanying text.

88 *See* Deeks, *supra* note 38, at 643.

89 *See id.* at 643–44.

90 *See id.* at 644–45 (citing Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Austl.), Provisional Measures Order, 2014 I.C.J. 147, 148 (Mar. 3)).

91 International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171. An identical provision can be found in the Universal Declaration of Human Rights. *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 12 (Dec. 10, 1948).

private citizens.[92] This is a very modern interpretation and application of these documents, but it is generating sufficient pressure for government agencies to reconsider their practices.[93] In time this may well establish itself as a norm.

In the case where diplomats or embassies are used for espionage, states have accused each other of violating the Vienna Convention on Diplomatic Relations because Article 41 requires "it is the duty of all persons enjoying such [diplomatic] privileges and immunities to respect the laws and regulations of the receiving State."[94] Since espionage is typically criminalized under the victim state's domestic laws,[95] this is easily a violation. Article 31 provides for diplomatic immunity from the criminal prosecution,[96] but Article 9 provides a means for states to terminate a diplomat's residence by declaring them persona non grata and requiring the perpetrating state to recall the individual.[97] Diplomatic espionage, however, appears to have become an expected norm, and only in rare occurrences would rise to the level of Article 9 condemnation.[98]

IV. REGULATING ESPIONAGE

The previous Section presented various arguments for why espionage is permissible or impermissible based on existing international law in the absence of a formal treaty. Some commentators have suggested instead to introduce a global regulatory body to settle cyber space ambiguities and gaps.[99] This Section explains why states have been unable to reach a multilateral treaty or any form of international regulation, and outlines permissible practices over peacetime espionage, and why they will continue to stay away from formalities.

---

92 *See* Deeks, *supra* note 38, at 635.

93 *See id.* at 636.

94 Vienna Convention on Diplomatic Relations art. 41, Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95 [hereinafter VCDR].

95 *See, for example*, 50 U.S.C. § 3093(e)(1) (2014); Official Secrets Act, 1911, 1 & 2 Geo. 5, c. 28 (Eng.).

96 VCDR, *supra* note 94, art. 31.

97 *Id.* at art. 9. For more details on espionage and diplomats, see Chesterman, *supra* note 7, at 1087–90.

98 *See* Mazzetti & Goldman, *supra* note 52 ("For more than 70 years, Moscow has filled its embassy and consulates in the United States with intelligence operatives—as Washington does with its own diplomatic outposts in Russia—giving them the mission of stealing the most significant secrets of a long-time adversary.").

99 *See generally, for example,* Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 PENN. ST. L. REV. 1005, 1031–32 (2015) ("Regardless of the form of the global regulatory agency, the potential costs of large-scale cyberattacks, both economic and personal, should convince the international community to centralize its cybersecurity efforts."); *see also* Paulina Wu, *Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N.*, 16 CHI. J. INT'L L. 281, 310–11 (2015) (arguing that the U.N. should regulate social media for terrorist content).

A. Difficulties

1. Strategic Incentives.

Strategic interests present a vast barrier for regulating espionage. States engage in espionage for national security, and nothing plays a greater priority than survival, creating no incentives to constrain these operations.[100]

In terms of future lawmaking, as Professor Matthew Waxman argues, legal line drawing has "distributive effects on power, and is therefore likely to be shaped by power relations."[101] For example, countries with less traditional espionage capabilities might opt to increase cyber espionage capacities to gain relative power in the international stage. This can be especially likely if the cost-efficiency of developing cyber espionage capacities is greater than the return for investing in traditional espionage. Meanwhile, certain nations have an established existing cyber espionage capacity, and are incentivized to push initiatives that would continue their dominance in the area. An anti-cyber espionage treaty would unlikely be acceptable to these nations while an anti-cyber espionage development stance would be held oppressive by weaker states, who have an interest to invest in more development to shrink the gap in information gathering abilities. All around, the state of affairs is not amenable to a treaty or regulation as it unfortunately has not reached an unacceptable tipping point (as opposed to the nuclear and space arms race during the Cold War, or economic espionage between the U.S. and China in the past few years).

2. Secrecy.

The secrecy of espionage creates two problems for regulation. Foremost, since secrecy is, in most cases, essential to the information collection's effectiveness, it does not lend itself to effective monitoring by other states to ensure compliance with any multilateral regulation.[102] There is no incentive to be transparent about activities that go undetected.

The secrecy of information regarding the actual capabilities of states also creates further tension. States have an interest in maintaining confidentiality regarding their abilities. There is the fundamental value of surprise in any activity involving national security and defense. The problem then is, if multiple countries believe they have the advantage in this field or could have the advantage, no one has an incentive to stop developing more espionage capabilities. At the negotiating table, they would all in turn believe they have more bargaining power than the other parties and would seek better terms than acceptable to the opposing party.

---

100 *See* Deeks, *supra* note 38, at 601.

101 Waxman, *supra* note 78, at 424–25.

102 *See* Deeks, *supra* note 38, at 608.

Even internally, states have to struggle with the concept of "plausible deniability," making it difficult to legislate and provide transparent and public oversight of certain intelligence activities.[103] Further, there is perhaps even a reluctance by legislators to discuss espionage because of the common view that it is an immoral activity,[104] all of which inevitably perpetuates the secret nature of intelligence activities.

B. International Law's Role

Long have scholars pondered at the reason why any state and international actor abide by international law.[105] This Subsection looks at why the determination of whether espionage is permissible or impermissible under existing international law is important despite the unlikelihood of regulation.

1. Expressive Function.

Scholarship has posited that law is able to influence behavior because it "signal[s] the underlying attitudes of a community or society" and actors are generally motivated to acquire approval.[106] This is independent of the actual punishment the law dictates for improper conduct.[107] What matters in fact is the shame accompanying any finding of violation.[108] The public declaration of legality or illegality for espionage (or more likely, a subset of espionage activity) can curtail bad behavior absent explicit regulation, that is monitoring and legal remedies.

Understandably, this reputational harm carries a value that may not overcome a state's strategic interest in certain settings, but at minimum it will affect behavior at the margin. A potential consequence of this may be a decrease in activities that are less justifiable for national security, such as surveillance of private individuals or commercial organizations, and borderline cases where the activity can be interpreted as an offensive activity rather than a defensive one.

Indeed, this phenomenon has already begun to surface. For example, in the U.S. there has been an increase in litigation over the legality of certain types of intelligence activities.[109] This then has resulted in more domestic legal

---

103 *See* HASTEDT, *supra* note 5, at 63.

104 *See id.* at 63.

105 *See* Harold Hongju Koh, *Why Do Nations Obey International Law?*, 106 YALE L.J. 2599, 2599–60 (1997).

106 *See* Richard H. McAdams, *An Attitudinal Theory of Expressive Law*, 79 OR. L. REV. 339, 340 (2000).

107 *See id.* at 339.

108 *See* Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2032–33 (1996).

109 *See* Deeks, *supra* note 38, at 623–24.

constraints,[110] indicating a shift by governments to concern itself with compliance (especially given the transparency of their operations now).

2. Legitimate Institution.

Violations of international law would also trigger the oversight of transnational institutions such as the International Court of Justice and the U.N. Victim states of espionage would likely want to turn to international law as a mechanism of imposing at minimum declaratory judgments of wrongdoing, which would require arguing for a prohibition of espionage.[111] Meanwhile, non-governmental organizations often, in their mission to protect individuals with little regard to state political interests, will turn to international law for agreements by states to be bound by international regulations.[112] Although the efficacy of these bodies may be in doubt, they provide a better channel than domestic institutions in acquiring recourse given the inability for national court systems to impose effective foreign punishment. Arguably remedies can come from state sanctions, but disapproval via international law can better legitimize a finding of "wrongdoing" by a state.

V. RE-EVALUATING ESPIONAGE IN THE MODERN ERA: A CALL FOR CLEARER GUIDELINES

The modern era provokes fresh analysis of the longstanding inconclusiveness in espionage law. Given the new reality of cyber technology, states should move towards establishing a guideline of permissible or impermissible activity; international law needs more clarity and certainty with respect to espionage. This is important as countries drift towards behavior that continues to destabilize international politics. The allegations of Russian cyber intrusions to sway the U.S. election highlight the possibility of escalation in the future.[113] Meanwhile, private individuals and entities can bear onerous financial costs in the face of state-sponsored cyber espionage. It is estimated that the "average cost of a data breach is now $4 million, a nearly 30 percent increase over the past three years."[114]

---

110 *See id.* at 623–24.

111 *See id.* at 633–34.

112 *See id.* at 633.

113 *See* Amanda Taub, *D.N.C. Hack Raises a Frightening Question: What's Next?*, N.Y. TIMES (July 29, 2016), http://www.nytimes.com/2016/07/30/world/europe/dnc-hack-russia.html?_r=0.

114 Tim Starks, *Potential Ramifications of the DNC Hack*, POLITICO (June 15, 2016), https://perma.cc/8V3F-MXDZ (quoting analysis by IBM Security and the Ponemon Institute).

Disagreements in the cyber space context are pervasive at every level. Nations do not agree on how the necessary terminology should be defined,[115] how cyber space itself should be viewed,[116] or how international governance of cyber space should be approached.[117] The best attempts at governance so far include the Budapest Convention[118] and the African Union Convention on Cyber Security and Personal Data Protection.[119] Both conventions, however, lack direct relevance to the area of cyber espionage.[120]

This Section will argue that the present condition is fragile. There are several fracture points that may finally crack the ambivalence states have shown to regulating the legality of espionage. Recent scholarship has begun to doubt the earlier view of applying existing principles to cyber space.[121] This Section will first highlight these and then reevaluate the traditional arguments pertaining the permissibility of espionage.

A. Catalysts of Change

1. More Indistinguishable Warfare.

By looking at several definitions offered below, this Section highlights the difficulty in articulating the differences between cyber espionage and a cyber attack. The crux of the issue is the broad definition of espionage as collection of information with no restriction on the means. This has frustrating real world implications since espionage is traditionally regarded as acceptable behavior while

---

115 *See* Waxman, *supra* note 78, at 422; Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602, 661 (2011). On one hand, the U.S. government offers to embrace cyberwarfare as a problem that involves "hostile act[s] using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions," and on the other, the Shanghai Cooperation Organization (in which Russia and China are participants) believes in an "information war" that involves "mass psychologic[al] brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party." *See* Hathaway, *supra* note 18, at 824–25. (alterations in original).

116 *See* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L. J. 317, 336–40 (2015).

117 *See id.* at 330–31 (discussing the conflicting views of states holding either a "multistakeholder vision" or "sovereign-based vision" of Internet governance).

118 Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167 [hereinafter Budapest Convention].

119 African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, A.U. Doc. EX.CL/846(XXV).

120 These documents mainly address domestic obligations to regulate cybercrime, and are ratified only by a small subset of countries; *see also* Henry Rõigas, *Mixed Feedback on the 'African Union Convention on Cyber Security and Personal Data Protection'*, INT'L CYBER DEVELOPMENTS REVIEW (Feb. 20, 2015), https://perma.cc/795P-X22V (sharing critics' views that the document's provisions are too vague and give rise to opportunity for abuse).

121 *See* YOO, *supra* note 72, at 188.

an attack by a state triggers jus ad bellum and jus in bello analysis.[122] This problem then lends itself to supporting a need to provide uniform agreement in permissible and impermissible activity between states in cyber space, especially in what target states can consider espionage or an attack, such that the target state can respond accordingly without violating international law.

a) Definitional Concerns

The *Tallinn Manual* is a commonly cited document in discussions on cyberwarfare since it represents the collective views of a group of international experts gathered by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).[123] The purpose of the original document was to provide a non-binding instructional manual applying existing laws to cyberwarfare.[124]

It narrowly defines cyber espionage as "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party."[125] This is the official definition adopted by NATO.[126] It is important to note that cyber espionage, as it is defined in the *Tallinn Manual*, is meant to consider the alignment of traditional war conventions with cyber espionage during times of armed conflict, and not peace-time espionage.[127] The document does not provide a clear analysis on the topic of cyber espionage as it was beyond the scope of the project.[128] This is mainly due to the group's belief that there is an "absence of a direct prohibition in international law on espionage *per se*."[129]

---

122 Jus ad bellum refers to the laws and principles regarding when war is permitted or would be a "just war." Jus in bello refers to international humanitarian law and laws governing warfare.

123 *See* NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 45 (Michael N. Schmitt et al. eds., 2013), https://perma.cc/DHK8-7WFG [hereinafter TALLINN MANUAL].

124 *See id.*

125 *See id.* at 159.

126 NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, CYBER DEFINITIONS, https://perma.cc/FB67-RXEU (last visited Jan. 19, 2016) [hereinafter NATO CYBER DEFINITIONS].

127 TALLINN MANUAL, *supra* note 123, at 159 ("Cyber information gathering that is performed from outside territory controlled by the adverse party to the conflict is not cyber espionage but, in certain circumstances, may be punishable under the domestic criminal of the State affected or of the neutral State from which the activity is undertaken."). This leaves a gap in reality since states may undergo military cyberespionage activity while not at war, and in these cases would not be linked to domestic criminal activity.

128 *See* TALLINN MANUAL, *supra* note 123, at 18 ("Cyber espionage . . . pose[s] real and serious threats . . . [h]owever, the Manual does not address such matters because application of the international law on uses of force and armed conflict plays little or no role in doing so.").

129 *See id.* at 50.

Although the *Tallinn Manual* offers a definition for NATO, as an example of the variance, countries party to NATO have presented alternative definitions. The U.S. Department of Defense's dictionary of military terms conspicuously does not define cyber espionage or cyber attack, and instead references "cyberspace operations" as "[t]he employment of cyber space capabilities where the primary purpose is to achieve objectives in or through cyber space".[130] Cyber espionage then would simply be espionage conducted as a cyber space operation.

In what seems to be an inconsistency, a separate document produced by the EastWest Institute as a collaborative effort between Russian and American experts to provide more definitive language as a basis for recurring bilateral discussions, then provides another agreed upon definition of cyber espionage as: "a cyber operation to obtain unauthorized access to sensitive information through covert means."[131] Cyber operations include "organized activities in cyber space to gather, prepare, disseminate, restrict or process information to achieve a goal."[132] This definition is accepted by the NATO CCDCOE as authoritative with respect to the two countries.[133]

b) A Soldier in a Spy's Clothing

The core problem raised by the definitions is that the collection of information itself does not specify limitations to the methods.[134] In no articulation is there an attempt to ensure a clear distinction from hostile activity normally deemed a violation of international law. For example, if State X hacks State Y to acquire classified information, this is both cyber espionage and potentially a cyber attack. How is State Y supposed to behave then when the ultimate goal is not prohibited under existing international law, but the means can be a violation? It seems to allow states to reduce liability for the latter by claiming it is merely espionage, and since cyber attack analysis continues to be imprecise and uncertain, there is further confusion about the appropriate responses under international law.

---

130 DEPARTMENT OF DEFENSE, DICTIONARY OF MILITARY AND ASSOCIATED TERMS (Feb. 15, 2016), https://perma.cc/C44F-7ZA2.

131 EASTWEST INSTITUTE, RUSSIA-U.S. BILATERAL ON CYBERSECURITY—CRITICAL TERMINOLOGY FOUNDATIONS 2 (James B. Godwin III et al. eds., Feb. 2014), https://perma.cc/79P7-L3SP.

132 *Id.* at 41.

133 *See* NATO CYBER DEFINITIONS, *supra* note 126.

134 A lot of emphasis has been put on the idea of disruption or destruction, but there has been little discussion as to how far the causation chain should be considered. For example, is it still considered disruption if the intent was to steal pertinent information on prominent politicians with the hopes of removing them from office? *See* Waxman, *supra* note 78, at 422 ("efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them"); Hathaway et al., *supra* note 18, at 826 ("A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.").

The *Tallinn Manual* indeed finds actions enabling cyber espionage may in themselves rise to use of force.[135] This analysis attempts to bifurcate the intrusion and the espionage itself as two separate concepts,[136] and even goes further by arguing that armed attack analysis should abide by strict liability as the "intention is irrelevant in qualifying an operation as an armed attack and that only the scale and effects matter."[137] If this is the case, a large portion of peacetime cyber espionage might be swallowed up by the cyber attacks analytical framework under jus in bello and jus ad bellum.

Cyber intrusions present a new twist to the old problem of identifying the intentions of foreign actors in the realm of national defense. Parallels can be drawn to the use of spy aircraft during the Cold War, as the malware deployed can be changed on-the-fly to achieve a destructive capacity rather than mere surveillance (and often does so to wipe its traces from the hardware). For the victim state in both cases, there is a fear that the vehicle is intended for combat rather than surveillance. A counterargument is that this is no different than a traditional spy who can cause immense physical harm, and thus cyber espionage should be treated the same as traditional espionage.[138] This view underplays the evidentiary and prevention issues inherent with cyber espionage. For a traditional spy to deliver a similar destructive payload, this would likely require extensive physical preparations that are more readily observable by the potential target and presents opportunities to hinder the efforts. It is not clear the extent to which this is the same in the cyber context. On its face, the tracking and information necessary to prevent a cyber attack of the same scale appears to be more difficult.

Furthermore, granted the difference in the potential consequences of the two scenarios is minute, there is an important distinction in the allowed response. Whereas the Russian military shot down a U-2 spy plane during the Cold War with no international legal repercussions (as the global community seemed to have agreed that this was within their sovereign right),[139] a parallel physical and destructive response to a cyber attack could be highly controversial.

Victim states' ability to respond is hampered by a narrow selection of potential avenues imposed upon them by international law. Since espionage itself is not definitively illegal, states are uncertain what countermeasures, or perhaps even acts of self-defense, are proportional and what would violate international

---

135 *See* TALLINN MANUAL, *supra* note 123, at 50–51.

136 *See id.* at 92 ("Non-violent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks.").

137 *See id.* at 56.

138 *See* Pelican, *supra* note 39, at 385.

139 *See id.* at 371.

law.[140] Cyber attacks and cyber espionage look identical from a technical standpoint when perpetrated and initially detected. Both require the targeting of vulnerabilities and the destruction of cyber defenses to access information databases.[141] There are several practical problems between responses to physical threats versus cyber threats. First, the victim state does not immediately know who is behind the intrusion. Second, the victim state is also in the dark as to the intent of the intrusion and its potential destructive capacity, whereas these are better known variables in the traditional context (for example, an aircraft would have known capacities). The slow response time and inaction that accompanied the hack of the U.S. DNC is a recent example of this problem.[142]

Without clear ways to retaliate as a means of deterrence, the calculus becomes extremely asymmetrical where actors have very little to lose by constantly deploying remote cyber espionage.[143] Thus, cyber space is an arena that greatly favors offense over defense. We would only need to look at the Russia-Georgia conflict in 2008 to see how an inaccurate appraisal of the situation could cause severe consequences, as Georgia underestimated the role of the initial cyber intrusions prior to Russia's eventual invasion.[144] Ultimately, the lack of clarity allows states to abuse the use of cyber attacks under the pretense of espionage to avoid worse violations.

Furthermore, even if there was a clear means of retaliation, cyber technology blurs traditional conceptualizations of state responsibility. For

---

140 *See* Scott J. Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 20 (2016) ("[T]he overt use of countermeasures is risky, as the invocation of countermeasures does not shield the victim State if the precipitating activity is later found lawful."); *see also, for example*, Julie Hirschfeld Davis & Gardiner Harris, *Obama Considers 'Proportional' Response to Russian Hacking in U.S. Election*, N.Y. TIMES (Oct. 11, 2016), http://www.nytimes.com/2016/10/12/us/politics/obama-russia-hack-election.html?rref=collection%2Ftimestopic%2FCyberwarfare.

141 *See* Brown, *supra* note 38, at 624–25 (2016) (arguing the distinction problem in cyber space between attacks and espionage are much greater than its traditional counterpart since soldiers and spies are easier to tell apart by their uniforms or weapons).

142 *See* Eric Lipton, David E. Singer, and Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

143 *See* Alexander Melnitzky, *Defending America against Chinese Cyber Espionage through the Use of Active Defenses*, 20 CARDOZO J. INT'L & COMP. L. 537, 570 (2012) (arguing that offense in cyber space always has the advantage and that a country cannot rely on mere increases in cyber defense capabilities). The International Court of Justice has discussed the possibility of constant smaller attacks being eventually aggregated to reach the armed attack threshold under the U.N. Charter; but this would require the need to accurately attribute the attacker in every case to ensure the aggregation is actually the same party. *See* YOO, *supra* note 72, at 186–90.

144 *See* John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html.

example, the inability to attribute an intrusion by a nation state against another was not a problem generally contemplated by traditional war doctrines.[145] A cyber intrusion can be routed through infected computers without their owners' permission, decreasing the verifiability of the attacker's origin.[146] This raises several concerns. First, the International Law Commission (ILC) Draft Articles for State Responsibility have taken the stance that non-state actions can be imputed to the state if they were committed on behalf of the State government.[147] The problem is that there is no clear and easy method for a victim state to be able to prove the connection between the state and the private actor, especially given cyber specialists' ability to mask their identity and to raise the doubt necessary about their actual origin.[148] The uncertainty surrounding the actor's true identity severely impedes a victim state's ability to respond. Second, if the infected computers belong to a neutral and separate state, does that state have a duty to prevent this from happening? It is not clear how the principle of neutrality should apply in these situations.[149]

Another related example is the difficulty states have in determining the military nature of cyber tools. Attempts to regulate the cyberweapons trade have come to a standstill because states cannot agree on how to distinguish legitimate defensive cyber tools and offensive cyberweapons.[150] For instance, the *Tallinn Manual* opts to characterize the difference based on effect.[151] This naturally conjures a problem of only knowing ex post whether something is a weapon. Reasonably, this is a classic problem of dual-use tools, even for something as archaic as a hammer or an ax. There have been attempts to create a clearer framework,[152] but cyberweapon regulation will remain unlikely in the near future.

---

145 *See* Waxman, *supra* note 78, at 444 (discussing the implications of attribution problems in cyber space).

146 *See, for example*, Paul Sonne, *What WikiLeaks Really Revealed About the CIA's Spying Techniques*, WALL ST. J. (Mar. 11, 2017) https://www.wsj.com/articles/what-wikileaks-really-revealed-about-the-cias-spying-techniques-1489233601.

147 *See* Raboin, *supra* note 115, at 642–43.

148 *See id.* at 644–45.

149 *See* Hathaway et al., *supra* note 18, at 855.

150 *See* Damian Paletta, *U.S. Firms Fight Global Cyberweapon Deal*, WALL ST. J. (Oct. 15, 2015), http://www.wsj.com/articles/u-s-firms-fight-global-cyberweapon-deal-1444952599 ("Officials can't agree on the legal distinction between nefarious computer programs that spy on networks and the software that helps companies avoid hackers. Some believe there is no distinction.").

151 *See* TALLINN MANUAL, *supra* note 123, at Rule 13 (indicating a focus on the effect of a tool).

152 *See generally*, *for example*, Trey Herr & Paul Rosenzweig, *Cyber Weapons and Export Control: Incorporating Dual Use With the Prep Model*, 8 J. NAT'L SEC. L. & POL'Y 301 (2015).

2. Distorted Cost-Benefit.

The relative ease and safety of cyber espionage disrupts the traditional cost-benefit analysis of spying, as the benefits have massively increased and costs have significantly decreased. This has resulted in ever growing violations of privacy rights by foreign actors,[153] economic espionage and violation of trade agreements,[154] and most dangerously, interference in state affairs by other nations.[155]

Before the internet and cyber space, states risked assets by having them spy on foreign soil, allowing them to be subjected to any punishment deemed appropriate by the target state.[156] The Internet and network infrastructure now allows "spies" to work relatively safely outside a target state, generally in their home state.[157] Even assuming the act is attributable to a particular organization or individual, it is unlikely the victim state can detain the actor outside of its own or an ally's jurisdiction without cooperative extradition relationships.[158]

Cyber espionage capacities are also cheaper to invest in than traditional espionage and its related tools.[159] Rather than expending time and money in developing a vast intelligence network, malware and other similar tools capable of

---

153 *See, for example*, Mark Fahey & Nick Wells, *Yahoo Data Breach is Among the Biggest in History*, CNBC (Sept. 22, 2016), https://perma.cc/92A2-N497 (highlighting notable hacks of enormous private information databases).

154 *See, for example*, Kim Zetter, *Chinese Military Group Linked to Hacks of More Than 100 Companies*, WIRED (Feb. 19, 2013), https://perma.cc/4FPJ-PE48 (describing economic cyberespionage conducted by a Chinese military group on over 100 American companies).

155 *See, for example*, Mary Louise Kelly, *Obama: Espionage is Being 'Turbocharged' by the Internet*, NPR (Dec. 16, 2016), https://perma.cc/WG78-C728 (quoting President Obama in calling for new rules to govern cyberespionage because of its increasing use and effectiveness in global geopolitics).

156 The death penalty has been used in various countries in the past, and some even today. *See, for example*, Ian Lee, *Cairo Court Issues Death Sentences in Qatar Espionage Case*, CNN (May 7, 2016), https://perma.cc/EPR7-Q4BC; Javier C. Hernandez, *China Sentences Man to Death for Espionage, Saying He Sold Secrets*, N.Y. TIMES (Apr. 19, 2016), https://perma.cc/X8QA-M6U7; *see also generally*, Ryan Norwood, *None Dare Call It Treason: The Constitutionality of the Death Penalty of Peacetime Espionage*, 87 CORNELL L. REV. 820 (2002) (discussing historical use of the death penalty in the U.S. and its recent emergence as an issue).

157 MI5 Security Service, CYBER, https://perma.cc/M3KR-2BJ8 (last accessed Dec. 19, 2016) ("[Cyber espionage] allows a hostile actor to steal information remotely, cheaply and on an industrial scale. It can be done with relatively little risk to a hostile actor's intelligence officers or agents overseas.").

158 *See* Jonathan Keane, *This Ain't CSI: How the FBI Hunts Down Cyber Criminals Around the Globe*, DIG. TRENDS (Aug. 2, 2015), https://perma.cc/M8JH-SPGS (exploring the difficulties of catching cyber criminals in nations that do not have extradition treaties); s*ee also, for example*, David Talbot, *Cyber-Espionage Nightmare*, MIT TECH. REV. (June 10, 2015), https://perma.cc/RH4D-9NPB.

159 *See* GEORG KERSCHISCHNIG, CYBERTHREATS AND INTERNATIONAL LAW 171 (2012).

retrieving information are less expensive, and are becoming even more so as experience and learning curves increase cost efficiency.[160]

Further, the sheer volume of information that both exists and can be collected has exponentially amplified the potential benefit of espionage.[161] Society has become increasingly reliant on network connectivity for personal and commercial use.[162] This in turn churns out millions of terabytes of collectible information.[163] Big Data can generate incredible value, but it creates enormous vulnerabilities.[164] Beyond personal information, intellectual property and trade secrets have become common targets of economic espionage by states or private entities since information is a key value driver for most commercial enterprises. For instance, a report by the United States Patent and Trademark Office found intellectual property intensive industries contribute more than $6 trillion dollars to the U.S. gross domestic product.[165] Since a lot of the value in this information is in its privacy (for example, intellectual property or private individual information), its theft is essentially its destruction.[166] The necessary precautions to prevent cyber intrusions are becoming wildly burdensome for private entities.[167]

---

160 *See* Max Smeets, *How Much Does a Cyber Weapon Cost? Nobody Knows*, DEF. ONE (Nov. 21, 2016), https://perma.cc/DNV5-7ZLX (describing four processes that make cyber weapons cheap: labor productivity gains, standardization, leveraging existing tools, and shared experience effects).

161 This Comment assumes more information is advantageous for intelligence gathering; arguably, to extract these benefits, substantial costs may have to be incurred to sift through the voluminous data. With the proliferation of machine learning and other analytical tools, the Comment argues that this cost-benefit likely tips towards being favorable rather than unfavorable for intelligence agencies. On a separate note, it should be noted that the benefits of information are necessarily corresponding vulnerabilities for states who hold large collections of valuable data.

162 For example, McKinsey Global Institute projects the Internet of Things can encompass up to 11% of the global economy by 2025. JAMES MANYIKA ET AL., MCKINSEY GLOB. INST., UNLOCKING THE POTENTIAL OF THE INTERNET OF THINGS (2015), https://perma.cc/W73Y-834V.

163 *See, for example*, James Manyika et al., McKinsey Glob. Inst., Big Data: The Next Frontier for Innovation, Competition, and Productivity (2011), https://perma.cc/K7H8-5Y9E ("[B]y 2009, nearly all sectors in the US economy had at least an average of 200 terabytes of stored data (twice the size of US retailer Wal-Mart's data warehouse in 1999) per company with more than 1,000 employees."); Steve Lohr, *The Age of Big Data*, N.Y. TIMES (Feb. 11, 2012), http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html.

164 *See* Brown, *supra* note 38, at 621 (discussing how the "speed of access and exfiltration" in cyber space creates a wider range of problems than traditional espionage).

165 *See* Justin Antonipillai & Michelle K. Lee, Econ. and Statistics Admin. & U.S. Patent and Trademark Off., Intellectual Property and the U.S. Economy: 2016 Update at ii (2016), https://perma.cc/27GW-EWD6.

166 *See* KERSCHISCHNIG, *supra* note 159, at 172. *See* Talbot, *supra* note 158.

167 *See, for example*, Jim Finkle, *Hacking Is Such a Problem that the Cost of Cyber Insurance is Skyrocketing*, VENTUREBEAT (Oct. 11, 2015), https://perma.cc/8UFD-Z6MQ.

3. Increased Visibility.

Either as a result of leaks or voluntary transparency, the increasing public knowledge of intelligence operations has brought the lack of strict regulation into the spotlight.[168] One of the reasons why historically there has been a vacuum in regulation is because espionage did not affect the average citizen, but this has changed with cybercapabilities.[169] Professor Deeks, a scholar of international law and national security, in a recent article suggested there has been an increase in coalitions of non-state actors with a shared interest to impose "greater restraints" on intelligence activities.[170] These restraints could come in the forms of naming and shaming of states, both domestic and international litigation, pressures on the U.N., and peer constraints among states. For instance, the U.N. General Assembly has called on states to review their intelligence operations to ensure they uphold a right to privacy.[171] Consequently, there has been a recent surge of interest for intelligence agencies to become more legitimate through increased oversight and transparency, and a commitment to operate within acceptable legal, moral, and sociological limits.[172] This is in contrast to a traditionally common perception that intelligence agencies are institutions working in the shadow of the government, rather than a branch accountable to the public.[173] The U.S. has started to bring prosecutions against individuals engaged for alleged state-sponsored cyber espionage.[174] These are not likely to amount to any actual arrests, but they nonetheless serve as a means to impute reputational damage for bad state actors.

4. Weaponization of Data, Information Wars.

The introduction of cyber technology and its free flow of information has brought worries about how this can be weaponized. This concern has historical roots in the International Convention Concerning the Use of Broadcasting in the Cause of Peace, which sought to prohibit the spread of hostile propaganda,

---

168 A recent example is the Vault 7 WikiLeaks incident, where hackers publicized classified CIA information, revealing an extensive collection of various cyber intelligence activities. *See* Shane Harris & Paul Sonne, *Wikileaks Dumps Trove of Purported CIA Hacking Tools*, WALL ST. J. (Mar. 7, 2017), https://www.wsj.com/articles/wikileaks-posts-thousands-of-purported-cia-cyberhacking-documents-1488905823.

169 *See* Deeks, *supra* note 38, at 608.

170 *See id.* at 633.

171 G.A. Res. 68/167, ¶ 3 (Dec. 18, 2013) ("[T]he same rights that people have offline must also be protected online, including the right to privacy.").

172 *See* Deeks, *supra* note 38, at 628–29.

173 *See, for example*, Rachel Brand, *Transparency in the Intelligence Community*, THE FEDERALIST SOC'Y. (Oct. 29, 2015), https://perma.cc/YHP3-9H75.

174 *See* Talbot, *supra* note 158 (discussing the U.S.'s attempt to prosecute five alleged agents of China's People's Liberation Army Unit 61398 for hacking multiple American companies).

incitements of war, and falsehood.[175] Russia has in fact called for the U.N. to treat the spread of subversive ideas by governments as an act of aggression.[176] The Shanghai Cooperation Organization has recognized the threat of "information wars".[177] This fear was brought back into the spotlight after the leaks of emails during the 2016 U.S. presidential election.[178]

The concern of an information war will likely then spark a desire for arms control, in this case the collection of information. Since subversive information is likely confidential information, states have a strong incentive to both increase their espionage activities while publicly decrying its impermissibility. States with more established institutions and more complex systems are likely asymmetrically affected under this type of warfare, and would be incentivized to impose common regulation, while really targeting weaker states who can engage in this type of activity with less fear of effective reciprocity.

B. Impact on Traditional Legality Arguments

The following Sections will reveal that the permissibility view is losing its force with respect to cyber espionage, prompting a contemporary reconsideration of the ambiguity as to its legality. This mainly stems from three areas: growing discontent over information collection, weakening self-defense justifications, and the ballooning risk of information flow. Despite the sovereignty and territoriality argument maintaining a status quo position, cyber technology causes a net rebalancing tipping the scale towards impermissibility, but insufficiently to render the outcome obvious. The justifications offered though, are clearly no longer sufficient to command a persuasive rationale for espionage's broad continuing permissibility.

---

175 International Convention concerning the Use of Broadcasting in the Cause of Peace, Sept. 23, 1936, 186 L.N.T.S. 301.

176 *See* Tom Gjelten, *Seeing the Internet as an "Information Weapon"*, NPR (Sept. 23, 2010), https://perma.cc/BDL9-F4W3.

177 *See supra* note 115. The Shanghai Cooperation Organization was originally formed by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan, with India and Pakistan becoming members in near the future. The group was originally the Shanghai Five, and continues to serve as a forum between the countries to foster cooperation in politics, trade, economy and culture. For more information, see ELEANOR ALBERT, COUNCIL ON FOREIGN RELATIONS: THE SHANGHAI COOPERATION ORGANIZATION (Oct. 14, 2015), https://perma.cc/5KWF-JYYT.

178 *See, for example*, Dmitri Trenin, *Information is a Potent Weapon in the New Cold War*, THE GUARDIAN (Sept. 17, 2016), https://perma.cc/QPT4-4B8T; Zack Beauchamp, *Russia Has Weaponized the American Press,* VOX (Oct. 17, 2016), https://perma.cc/R6M8-KPKP.

1. Espionage as a Permissible Activity.

a) Absence of Impermissibility

Cyber technology presents a significant wrinkle with the absence of impermissibility argument, which states that espionage is permissible because the conduct is not condemned under customary international law. Although cyber espionage itself has not received a lot of direct attention, cyberwar and cyber attacks have.[179] Even if state conduct may not be pointing to any disallowance of espionage in general, where cyber espionage is carried out in a manner similar or identical to a cyber attack, such as through hacking, customary international law may soon evolve to hold broad categories of cyber activities (particularly the use of certain cyber tools) as violations.[180] This will ultimately turn on the extent to which spillover effects from regulation of cyber attacks and cyber war may implicate cyber espionage because of overlapping technology.

b) Statecraft and Self-Defense

The low entry costs for cyber espionage and its increased accessibility perhaps improves the statecraft tool argument because it expands the information flow between countries. The concern is the parallel amplification of distrust. For example, there was international disapproval of the U.S. tapping German Chancellor Angela Merkel's phone. This was followed by a humorous revelation that the German intelligence community was in fact doing the same thing.[181] Again where cyber espionage overlaps with cyber attacks, these activities sow more conflict than cooperation.

The world is also not so devoid of conflicts such that the monitoring rationale for self-defense is less compelling. The concern is the shift in where the line is drawn between defensive and offensive measures. With recent accusations of countries engaging in information wars and weaponizing information,[182] it is

---

179 *See* Meetings Coverage, General Assembly, Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment, U.N. Meetings Coverage GA/DIS/3512 (Oct. 28, 2014).

180 *See* Kevin Townsend, *Rise in State-Sponsored Cyber Espionage: The Tipping Point of Cyber Warfare*, SECURITY WEEK (Aug. 23, 2016), https://perma.cc/S9A9-B7XU.

181 *See, for example*, Anna Sauerbrey, *The German Government's Surveillance Hypocrisy*, N.Y. TIMES (June 10, 2015), https://www.nytimes.com/2015/06/11/opinion/the-german-governments-surveillance-hypocrisy.html; Anthony Faiola, *Germans, Still Outraged by NSA Spying, Learn Their Country May Have Helped*, WASH. POST (May 1, 2015), https://www.washingtonpost.com/world/europe/nsa-scandal-rekindles-in-germany-with-an-ironic-twist/2015/04/30/030ec9e0-ee7e-11e4-8050-839e9234b303_story.html?utm_term=.a55727f9e0d9.

182 *See, for example*, Mark Galeotti, *Putin Is Waging Information Warfare. Here's How to Fight Back*, N.Y. TIMES (Dec. 14, 2016), https://perma.cc/D8HD-QP39.

difficult for self-defense to allow a blanket excuse for all espionage and intelligence related activity.

Another concern raised by cyber espionage is the role of proportionality when justifying espionage as self-defense.[183] Whereas prior to the cyber era, wide collection of information was costly or cumbersome, intelligence agencies had to have a sufficient suspicion in a target ex ante before engaging in espionage.[184] With the introduction of software that can cast a wide net, the situation seems to have reversed itself where suspicion is developed ex post.[185] It is not absolutely obvious this is facially disproportionate in all scenarios, but it appears hard to justify without some cognizable threat to national security. This becomes even more imprecise if there needs to be a calculable balance. For example, how much harm is inflicted by infiltrating the privacy of every individual in a nation who sends emails and browses the internet?

2. Espionage as an Impermissible Activity.

a) Sovereignty and Territoriality

The main thrust behind this view lies in territorial sovereignty and how foreign espionage is a violation of this inherent right. But modern technology introduces a new question: how does territoriality operate in a domain like cyber space? Cyber espionage introduces a problem very similar to the same legal questions asked when aviation technology became popular, and then inevitably again when satellite technology bloomed during the Cold War.[186]

The introduction of new domains in the past eventually led to formal treaties regarding their use and conceptualization. The Chicago Convention on International Civil Aviation cemented state sovereignty of the airspace over its territory,[187] and the need for permission for non-civil aircraft (that is, aircraft used in military, customs and police services)[188] to enter a state's airspace.[189] Similarly, when space travel became available, the Outer Space Treaty prohibited all claims

---

183 *Proportionality*, Black's Law Dictionary (10th ed., 2014) ("The principle that the use of force should be in proportion to the threat or grievance provoking the use of force.").

184 *See* DARRELL COLE, JUST WAR AND THE ETHICS OF ESPIONAGE 53–54 (2014).

185 *See id.* at 53–54.

186 *See* Chesterman, *supra* note 7, at 1082–87.

187 Convention on International Civil Aviation art. 1, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295 [hereinafter Chicago Convention].

188 *Id.* at art. 3(a)–(b).

189 *Id.* at art. 3(c).

of state sovereignty by appropriation or by occupation.[190] In relation to espionage, there is a common understanding that fly-over espionage violates state sovereignty under customary international law, whereas there has been no formal prohibition against satellite espionage.[191]

Cyber space raises issues that do not find exact parallels in existing legal frameworks, because cyber space is not a physical domain. However, it does exist on physical infrastructure.[192] Thus, two competing narratives have emerged.[193] One asserts that territorial sovereignty extends to cyber space.[194] The other asserts cyber space is a "global commons" not subject to sovereignty.[195] There is not likely to be any resolution of this debate in the near future, since there are divergent strategic and political interests at work. States that want more regulation of internet content argue for sovereignty, while states that want more free flow of information argue for a shared commons approach. This undermines the violation of territoriality justification since territory or sovereignty in cyber space is definitionally unclear. Under a global commons approach, intelligence activities in cyber space are presumably permissible since states have either no claim or conceded their claim on the information.[196] Alternatively, if territoriality extends to cyber space, the problem becomes inevitably where are state boundaries drawn, and derivatively, where are they crossed?

A very easy case under this argument would involve a spy using physical hardware to collect information on an isolated network; for example, using malware stored on a portable hard drive and connecting it to a system not connected to the wider internet. In this case, the violation of territoriality and sovereignty argument is much stronger and is more akin to traditional forms of espionage. The uncertainty then only pertains to situations of remote cyber espionage.

---

190 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies art. 2, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

191 *See* Chesterman, *supra* note 7, at 1083–87.

192 *See* Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 459–60 (2016).

193 *See* Eichensehr, *supra* note 116, at 336–40.

194 *See* TALLINN MANUAL, *supra* note 123, at 15–16.

195 Global commons refer to domains that "lie outside of the political reach of any one nation State." *See* UNITED NATIONS ENVIRONMENT PROGRAMME, IEG OF THE GLOBAL COMMONS, https://perma.cc/6K7Y-8L8Z (last accessed Jan. 29, 2017).

196 This is unlikely to be true in the absolute sense. The likely analogous situation would be espionage conducted between vessels in international waters or in the Antarctic. Literature and analysis of espionage between satellites might also be informative.

3. Cyber Espionage's Overall Impact.

Modern technology has introduced new complications to espionage propelling a reconsideration of the traditional scholarship. The existing ambiguity was created by a combination of both state and academic ideologies. Traditionally, state practice both condemned and accepted espionage in a contradictory fashion—foreign espionage is illegal whereas national intelligence operations are legitimate. Meanwhile, scholars debated the merits of how espionage comports with existing doctrines of international law. The permissibility view acquired more proponents, but it is uncertain whether this was simply ex post rationalization of continuing state practice. However, cyber espionage has stirred the conventional international complacency by bringing the permissibility of foreign intelligence operations into the daily public spotlight, has become less defensive and more offensive, and has evolved into a point of discourse rather than a tool for political stability. Until states can agree on a uniform conceptualization of cyber space though, the territoriality argument regarding cyberespionage also remains in analytical limbo. If the scholarship can be seen as a scale that has justified espionage in the past decades since the arguments tipped towards permissibility, the current changes in aggregate appear to be shifting in the other direction.

VI. A PIECEMEAL APPROACH TO REGULATING ESPIONAGE

This Section provides one example of how states can address the tension created by the unsustainability of the traditional ambiguity expressed in Section V when it clashes with the barriers to formal wide-reaching regulations articulated in Section IV. This Comment suggests that one viable approach is for states to carve out narrower sets of activities falling within espionage through norms rather than formal instruments. State-sponsored private espionage would be a good initial candidate, as low hanging fruit, since it is likely more amenable to wide agreement.

A. Soft Incremental Approach

With no treaty in sight, states have shown an interest in at least establishing minimum guidelines and norms to stop the escalating arms race in cyber space.[197]

---

197 *See* Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶¶ 9–15, U.N. Doc. A/70/174 (July 22, 2015), https://perma.cc/Q57P-77C4 (establishing a small set of norms to be adopted by the twenty participating states). Kate Conger, *Obama and Clinton Weigh in on Cyber Warfare Tactics*, TECHCRUNCH (Sept. 6, 2016), https://perma.cc/VG8D-6BSY (discussing the U.S.'s call for guidelines and norms in cyber space). For a discussion on how norm setting should be analyzed as a process, see generally Finnemore & Hollis, *supra* note 192.

Even if there is no formal agreement, norm setting has various advantages.[198] As one scholar explains, norms require looser agreements among a less rigid set of parties, increasing the speed of application as compared to an official treaty.[199] Norms can also develop through practice rather than a formal document, and thus are more flexible to change since there states are not strictly bound to a predetermined set of rules.[200] Finally, norms still improve both state coordination and clarity between states regarding generally allowed and disallowed actions.[201] However, a broad governing norm, given the numerous strategic barriers, seems unrealistic, and states should approach the issue on a more narrow basis by carving out rules for specific activities.

There have been attempts at far-reaching and broad solutions but they appear unrealistic either because they are too expansive in scope or they rest on imprecise analysis. Some have advocated for an extreme approach, banning cyber espionage altogether. This is highly controversial and would have difficulties gaining the necessary political traction given strategic considerations and the existing status quo. Proposals from other scholars have included allowing cyber attacks as an umbrella term to include cyber espionage;[202] and using new terminology such as cyber intrusion to create a sliding scale rather than a binary categorization,[203] which may improve clarity as to whether intrusions should be

---

198 Eichensehr, *supra* note 116, at 361–65 (discussing the various advantages of norm setting). Alternatively, there is an extensive canon on the debate over the advantages and disadvantages of using "soft law", non-binding obligations in international law. *See generally, for example*, Gregory C. Shaffer & Mark A. Pollack, *Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance*, 94 MINN. L. REV. 706 (2010); Jean Galbraith & David T. Zaring, *Soft Law as Foreign Relations Law*, 99 CORNELL L. REV. 735 (May 2014).

199 *See* Eichensehr, *supra* note 116, at 361–65.

200 *See id.*

201 *See id.*

202 *See, for example*, Major Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65 (2009) (arguing that cyberespionage should simply fall under the cyberattacks framework and hopefully deter states since it increases the chances of it leading to triggering armed self-defense); *see also* Craig Forcese, *Pragmatism and Principle: Intelligence Agencies and International Law*, 102 VA. L. REV. ONLINE 67, 68 (2016) ("[I]n the absence of definitive, subject-matter specific law in the area, analysts have arrived at dramatically different conclusions about international law's relationship with spying."); TALLINN MANUAL, *supra* note 123, at 16 ("The International Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty."). *But see* Demarest, *supra* note 34, at 324–25 ("[A]ny attempt at a precise definition [of espionage] is difficult.").

203 James E. McGhee, *Hack, Attack or Whack; the Politics of Imprecision in Cyber Law*, 4 J. L. & CYBER WARFARE 13, 41 (2014) (proposing a two-tiered analysis where cyber intrusion is used as a catch-all term until it can later be further defined as a cyberattack, a cybercrime, or cyberespionage); s*ee also* Williams, *supra* note 23 (suggesting that cyber intrusions should be analyzed by the U.S. under

afforded more deference simply because they can be considered espionage. The switch to grouping all intrusions as cyber attacks would allow states to enact countermeasures against any intrusion.[204] These narrower theories seem limited. They may require distinguishing the use of bugs and malware that destroy cybersecurity defenses versus methods like phishing where the hacker simply provides a cyber trap or bait. Instead of engaging with the traditional analytical frameworks used for espionage, they veer the analysis towards the cyber attack and cyberwar literature.

There are solutions that are viable without having to remove the analysis away from espionage entirely. For example, the U.S. and China have managed to negotiate an economic espionage treaty. Even if it is difficult to police, the signaling has proven to provide great success; breaches in the U.S. have dropped 90%.[205] This suggests that regulating specific activities within the broader umbrella of espionage can be productive.

One area arguably requiring attention is in state sponsored cyber espionage through private entities.[206] Countries use this compartmentalization to create plausible deniability, and then leverage the absence of an extradition treaty to protect these organizations from any criminal prosecution by the victim state. The following Subsections will present first why this type of behavior needs to be stemmed, why it is a good candidate to carve out, and what justifications support this norm. Finally, this Section ultimately evaluates the pragmatism of this suggestion.

1. Examples of Exploitation and Abuse.

Although attribution is hard, there have been instances where states have found sufficient evidence to have a strong belief that private entities are engaging in cyber espionage on behalf of their government. For example, U.S. intelligence agencies have long asserted "P.L.A. Unit 61398" is a private organization operated by the Chinese government.[207] This organization has allegedly hacked private and

---

a covert action framework rather than an intelligence analysis framework because of the blurry distinction given cyberespionage).

204 This would not have been allowed in a world that still distinguished cyberespionage from cyberattacks, as countermeasures are only acceptable against unlawful behaviour. *See* Shackelford, *supra* note 140, at 17. Without the espionage categorization, the proportionality analysis also changes for the countermeasure analysis, allowing states to increase the level of their retaliation.

205 *See* Joseph Menn & Jim Finkle, *Chinese Economic Cyber-Espionage Plummets in the U.S.: Experts*, REUTERS (June 21, 2016), https://perma.cc/59WX-T55X.

206 *See* Leonid Bershidsky, *Cyberwar Has Gone Public, and That's Dangerous*, BLOOMBERG VIEW (Jan. 13, 2017), https://perma.cc/W5B8-74T7.

207 *See* David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking against U.S.*, N.Y. TIMES (Feb. 18, 2013),

governmental organizations for industrial data and information on American infrastructure. The U.S. has recently formally prosecuted alleged members of the organization.[208] Many agree these prosecutions will likely be fruitless, as the Chinese government continues to deny involvement, and without any extradition treaties, these alleged perpetrators will continue to go about their business.

There are other notorious hacking groups generally thought to be state-sponsored espionage organizations: Fancy Bear (Russian),[209] Equation Group (American),[210] Tarh Andishan (Iranian),[211] and Dragonfly (Eastern European).[212] Beyond these, there are also professional private cyber intelligence organizations such as the Italian Hacking Team, and the two German groups FinFisher (Lench IT Solutions PLC) and Trovicor.[213] In each case, these organizations and their activities exacerbate concerns raised by cyber espionage because they allow states to engage in behavior with essentially minimal liability. It utterly upends the cost structure traditionally limiting widespread espionage.

2. Justifications and Benefits.

The disallowance of privately conducted espionage would carry several benefits in reestablishing stability among transnational actors. First, it strikes at the core of the problem by disincentivizing states from hiding behind private organizations to conduct proxy information gathering by reinserting a more powerful reputational cost to espionage that was eliminated by the use of easily dismissible scapegoats. It also removes the ability for states to engage in otherwise impermissible behavior by using these proxy organizations. One of the concerns with this puppet-puppeteer relationship is the lack of responsibility states have to face for their conduct and the moral hazard of impunity from other nations.

Second, the traditional functional and realist rationales supporting the allowance of espionage in the first place do not exist when conducted through

---

http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

208 *See* Talbot, *supra* note 158.

209 *See* Andrew E. Kramer, *Top Russian Cybercrimes Agent Arrested on Charges of Treason*, N.Y. TIMES (Jan. 25, 2017), https://www.nytimes.com/2017/01/25/world/europe/sergei-mikhailov-russian-cybercrimes-agent-arrested.html?_r=0.

210 *See* Robert McMillan & Shane Harris, *Hacking Group Releases Files, Says It Is Ceasing Operations*, WALL ST. J. (Jan. 12, 2017), https://www.wsj.com/articles/hacking-group-releases-files-says-it-is-ceasing-operations-1484271598.

211 *See* Sam Jones, *Cyber Warfare: Iran Opens a New Front*, FIN. TIMES (Apr. 26, 2016), https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3.

212 *See Energy Firms Hacked by "Cyber-Espionage Group Dragonfly"*, BBC (July 1, 2014), https://perma.cc/99JQ-DTWC.

213 *See, for example*, Mattathias Schwartz, *Cyberwar for Sale*, N.Y. TIMES (Jan. 4, 2017), https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html.

private entities. It does not foster stability, but rather stirs distrust and conflict, since countries are tirelessly tracking down bad actors and then facing denials and roadblocks to catching those whom they deem to be international criminals. Cooperation between states then is likely to breakdown. As more states begin to develop mature cyber capabilities and engage in this type of behavior, it is unclear how international actors will function under a system where private organizations take over inter-state activities without the responsibility of being a state.

Third, in contrast, supporting such a norm would in fact foster cooperation among states by setting a platform towards future negotiations on how to govern state conduct in the cyber realm through incremental moves.[214] Understandably, the strength of this justification rests on how states view the incremental nature of a carveout like this is. For instance, this strict prohibition can be seen as a large leap in international policy when intelligence operations have been rarely constrained. How policy is framed will be pivotal to the success of any progress towards more regulation and oversight.

Lastly, this type of disengagement from state activity can lead to curbing private threats on international security, such as cyberterrorism or hacktivism. When these organizations lack state affiliation, it would create a more amenable atmosphere to allow prosecution of "criminals" and remove the conflict of interest created by their connection with state-sponsored activity. This will serve to relax concerns about private actors engaging in the realm of war as nations agree on the impermissibility of their involvement.

An analogous issue is the state use of mercenaries and private military contractors. This example may be instructive of the problems that arise when private individuals are engaged in customarily state activities.[215] The use of mercenaries is subject to a lot of controversy, and has been condemned by dozens of states, although not by the world's largest military powers.[216] Perhaps this may indicate that this Comment's suggestion would fall prey to the same issue where states with a more vested interest are unlikely to move, but an important

---

214 For an example of further analysis of the benefits of incrementalism in law making, see Susan Block-Lieb & Terence C. Halliday, *Incrementalism in Global Lawmaking*, 32 BROOK. J. INT'L L. 851, 852 (2007) ("Incremental development of global law is more often championed where law reformers possess limited authority and where the subject is either controversial or technical (or both)."); Oona A. Hathaway, *Between Power and Principle: An Integrated Theory of International Law*, 72 U. CHI. L. REV. 469, 531 (2005) ("Rather than confront states immediately with a legal regime that couples challenging goals with strong sanctions for failure to meet them, states can be gradually led toward stronger legal rules.").

215 *See, for example*, Dan Roberts, *U.S. Jury Convicts Blackwater Guards in 2007 Killing of Iraqi Civilians*, THE GUARDIAN, (Oct. 23, 2014), https://perma.cc/4VYW-TUUA.

216 *See* G.A. Res. 44/34, International Convention Against the Recruitment, Use, Financing, and Training of Mercenaries (Dec. 4, 1989) (missing notably the U.S., China, Russia, India, France, Japan, and the U.K.).

distinction here though might be private espionage creates mutually costly problems for these countries since they are routinely subjected to their intrusions.

3. Pragmatism?

Any proposal in the cyber space field is likely to face skepticism. As explained in Section IV, regulation in this area is extremely difficult given the pragmatic concerns of different states. Nonetheless, this prohibition against private actors engaging in espionage may gain traction as long as one of the current cyber power states are willing to take the first step. Having brought forth this suggestion, it would then be difficult for any country to justify why private actors should be allowed to conduct espionage on any sovereign state. The existence of these private groups has been sustained by the deniability of their corresponding state sponsors that there is any connection and affiliation. Given the clear evidence of this type of behavior, a rejection of this by any state is necessarily admitting to using private actors to conduct espionage.

The concern is that first movers would only likely be motivated by strategic disadvantage. That is, as Section IV alludes to, given that any state believes they have the strategic upper-hand in the cyber espionage arena, they are unlikely incentivized to curb the conduct. The impacted state would then realize that by being the first mover, they are at a bargaining disadvantage. Therefore, there is only appeal to negotiate when the victim state has suffered harm sufficient to overcome the cost of being in a weakened negotiating position.

However, an alternative potential pressure point may come from internal private and public denunciation of governmental espionage activity resulting from significant impacts in economic activity or human rights violations.[217] A recent example may be the problems being raised by the Vault 7 disclosures, which revealed the extent to which the CIA exploited bugs in private technology as part of its surveillance programs.[218] Of course, the catalyst would need to be relevant to the particular norm being requested.

VII. CONCLUSION

International law cannot remain stagnant and ignore the enormous benefits brought to information collection by cyber espionage. When espionage was reserved to small scale operations and imposed targeted and specific harm, an artful ambiguity was reasonably sustainable. The ability now to engage in constant

---

217 *See* Ian Bremmer, *WikiLeaks: The Real Cost of 'Forced Transparency'*, TIME (Mar. 16, 2017), https://perma.cc/7MXY-2JBG; Brent Bambury, *Vault 7: How the CIA's Secret Stash of "Zero Day" Hacks Could Leave Your Devices Vulnerable*, CBC RADIO (Mar. 10, 2017), https://perma.cc/ZT5J-LHF7.

218 *See* Robert McMillan, *Tech Firms Rush to Assess Damage from CIA Leak*, WALL ST. J. (Mar. 8, 2017), https://www.wsj.com/articles/tech-firms-rush-to-assess-damage-from-cia-leak-1489028040.

wide-reaching surveillance and activities that can be interpreted as offensive operations necessitates new legal reforms that properly reflect the capabilities of modern technology. Although arguably the policing and enforcement of anything related to cyber space is difficult, public consent to the adoption of guidelines could up the ante by increasing reputational costs. As Professor Stone once described it, international stability will "depend[ ] on being contemporaneous in our thinking, and not pretending that we can either govern or preserve ourselves in a transformed world, by the use of notions no longer applicable."[219]

[219] *See* STONE, *supra* note 48, at 38.