Chicago Journal of International Law

Volume 18 | Number 2 Article 6

1-1-2018

Enforcing a Prohibition on International Espionage

Jared Beim

Follow this and additional works at: https://chicagounbound.uchicago.edu/cjil

 Part of the Law Commons

Recommended Citation
Beim, Jared (2018) "Enforcing a Prohibition on International Espionage," *Chicago Journal of International Law*: Vol. 18: No. 2, Article 6.
Available at: https://chicagounbound.uchicago.edu/cjil/vol18/iss2/6

This Comment is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in Chicago Journal of International Law by an authorized editor of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.

Enforcing a Prohibition on International Espionage

Jared Beim*

Abstract

Peacetime espionage is an incredibly important and common occurrence in modern international relations, yet its legal status is far from clear. This Comment explores the practice's legal background, as well as the arguments for and against its legality. While there can be many benefits to peacetime espionage, and while few countries have "clean hands," it seems unworkable to overcome the presupposition that most espionage is an "intervention" as defined by the ICJ in Nicaragua v. U.S.*, even if the prohibition on espionage is often unenforced. With the conclusion that most peacetime espionage is likely illegal under international law, this Comment attempts to ascertain how this prohibition can be enforced. After examining the ICJ's prohibition on "intervention," the ICC's jurisdiction over "crimes of aggression," the U.N. Security Council's prohibition on "force," and the Council of Europe's Convention on Cybercrime, no panacea was found. Therefore, in situations where domestic law is unable to effectively enforce this prohibition, this Comment argues that countermeasures are the best way to deter state actors from engaging in acts of peacetime espionage. However, in certain situations where extreme versions of peacetime espionage are carried out upon weak countries unable to make use of countermeasures, reliance on the ICJ, the ICC, the U.N. Security Council, or the Council of Europe may be feasible.*

Table of Contents

---

* J.D. Candidate, 2018, The University of Chicago Law School. I would like to thank Professor Nicholas Stephanopoulos for his valuable feedback throughout the writing process. I would also like to thank Charles Eaton, Zac Henderson, Abigail Majane, Caroline Wood, Benjamin Moss, and Jasmine Mehdizadeh for their thoughtful comments.

I. INTRODUCTION

Espionage has a glamorous image in popular culture, leading many to think about James Bond in a fancy tuxedo secretly traveling to exotic locales. In a sense, this portrayal is not always inaccurate. Still, espionage takes many forms, and can be generally defined as "the process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems)."[1] The need for information has advanced in modern times, as have the methods deployed to gain such information. For these reasons, the consequences of espionage can be tremendous, sometimes even critical to wartime success.[2]

As will be discussed in more detail, international law is quite clear on the limited permissibility of wartime espionage, but strangely silent on the permissibility of peacetime espionage. Section II of this Comment focuses on the legal background of wartime espionage and the limited usage that international law tolerates. Section III explores whether peacetime espionage is outlawed by international law and from where this prohibition originates. Section IV considers whether such a prohibition can be effectively enforced. Section V examines possible mechanisms for enforcing this prohibition on peacetime espionage. Finally, Section VI recommends a strategic combination of the discussed mechanisms in order to enforce this prohibition.

II. LEGAL PERMISSIBILITY OF WARTIME ESPIONAGE

A. Wartime Espionage

This Comment will first explore the legal background of wartime espionage to shed light on the legality of peacetime espionage. Hugo Grotius' summary of international law as applied to spies is as follows:

> [S]pies, whose sending is beyond doubt permitted by the law of nations - such as the spies whom Moses sent out, or Joshua himself - if caught are usually treated most severely. "It is customary," says Appian, "to kill spies." Sometimes they are treated with justice by those who clearly have a just case for carrying on war; by others, however, they are dealt with in accordance with that impunity which the law of war accords. If any are to be found who refuse to make use of the help of spies, when it is offered to them, their refusal

---

1 *Espionage*, SECURITY SERVICE M15, https://perma.cc/N857-RP93 (last visited Nov. 18, 2017).

2 Gregory Elder, *Intelligence in War: It Can Be Decisive*, CIA, https://perma.cc/53D7-R3UX (last updated June 26, 2008).

> must be attributed to their loftiness of mind and confidence in their power to act openly, not to their view of what is just or unjust.[3]

Not much has changed since Grotius' 1625 legal summation. Spies are severely punished in almost every country.[4] One of the first codifications of laws of wartime espionage in modern times was contained within the Declaration of Brussels in 1874.[5] While the rules announced by the Declaration were not adopted by the participating powers, the rules did proclaim that "the employment of measures necessary for obtaining information about the enemy and the country . . . are considered permissible" even if deceptive means were used to obtain the intelligence.[6] However, this legality was restricted purely to wartime espionage.[7] Still, the Declaration specifically states:

> A spy if taken in the act shall be tried and treated according to the laws in force in the army which captures him . . . . [A] spy who rejoins the army to which he belongs and who is subsequently captured by the enemy is treated as a prisoner of war and incurs no responsibility for his previous acts.[8]

Interestingly, this is a very merciful statute of limitations: as soon as a spy returns back to his/her own army, the infiltrator loses the status of spy.[9] Additionally, military members "who have penetrated within the zone of operations of the enemy's army, with the intention of collecting information, are not considered as spies if it has been possible to recognize their military character."[10] The Declaration of Brussels, therefore, places a large emphasis on the deceitful nature of espionage, rather than the simple act of gathering information.[11]

The 1907 Hague Rules, which deal with spies in a similar way, remain good law, including the prohibition on prosecuting spies for previous acts of espionage (as long as they had already rejoined their army) and the prohibition on punishing

---

3 HUGO GROTIUS, THE LAW OF WAR AND PEACE, Book III, ch. IV xviii 655 (F. Kelsey trans., Oxford 1925) (1625).

4 BOLESLAW A. BOCZEK, INTERNATIONAL LAW: A DICTIONARY 461 (2005) ("The regular penalty for espionage in wartime is death, regardless of whether or not the spy succeeds in obtaining information or conveying it to the enemy.").

5 Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 331 (1996).

6 Project of an International Declaration Concerning the Laws and Customs of War, Adopted by the Conference of Brussels, art. 14, Aug. 27, 1874, 148 Consol. T.S. 133 [hereinafter Declaration of Brussels].

7 Demarest, *supra* note 5, at 332.

8 Declaration of Brussels, *supra* note 6, arts. 20–21.

9 *See also* Headquarters, War Dep't, Gen. Orders No. 100, art. 104 (Apr. 24, 1863) [hereinafter Lieber Code] (noting that Abraham Lincoln's instructions regarding warfare during the American Civil War were harsh to spies caught in the act, but merciful to spies caught later).

10 Demarest, *supra* note 5, at 332.

11 Declaration of Brussels, *supra* note 6, art. 22.

a spy without trial.[12] The Geneva Convention of 1949 instituted additional safeguards for protecting persons accused of espionage, including "trial with counsel, an appeal process after penalty is imposed, and a six-month waiting period before a death penalty can be carried out."[13]

It is apparent that the law of war has recognized a legitimate need for intelligence, and therefore has not intended to stop the practice altogether. Instead, the law has focused on specifically punishing traitorous spying, and recognizes that "since little personal deceit is involved in most technical intelligence gathering, the law of war rejects individual punishment for engaging in such activities."[14]

B. Peacetime Espionage

Espionage is exceedingly common: "all developed nations, as well as many lesser-developed ones, conduct spying and eavesdropping operations against their neighbors."[15] Further, such actions are not limited to hostile states, as even allied countries regularly spy on each other.[16] In 2010, it was reported that "some 1,271 government organizations and 1,931 private companies work on programs related to counterterrorism, homeland security, and intelligence in about 10,000 locations across the United States."[17] Additionally, in the U.S., there are hundreds of thousands of cyber attacks every day intending to extract information, many of which are successful.[18]

In the 1960s, Israeli spy Eli Cohen infiltrated the upper echelons of Syria's military and political society, going so far as to be groomed for the position of Deputy Minister of Defense by friend and Syrian president Amin al-Hafez.[19] During his time in Syria, Cohen transmitted an incredible amount of data back to Israel via radio.[20] Famously, he feigned concern for Syrian soldiers exposed to the heat in the Golan Heights and had eucalyptus trees planted at the Syrian

---

12 Demarest, *supra* note 5, at 334–35.

13 *Id.* at 336; *see also* Convention (IV) Relative to the Protection of Civilian Persons in Time of War, art. 75, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

14 Demarest, *supra* note 5, at 338.

15 Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1091 (2003).

16 McKay Coppins, *Spies Among Us: Modern-Day Espionage*, NEWSWEEK (July 20, 2010) https://perma.cc/3A2g-AMME.

17 *Id.*

18 *Id.*

19 Lawrence Joffe, *Amin al-Hafez Obituary*, THE GUARDIAN (Feb. 16, 2010), https://perma.cc/Z7DZ-BCP2.

20 *Eli Cohen*, JEWISH VIRTUAL LIBRARY, https://perma.cc/K943-C8D4 (last visited Jan. 28, 2017).

fortifications, which Israel later used as targets during the Six-Day War.[21] When the Syrian military finally caught wind of the high amount of data leaked from the country, Cohen was caught and executed.[22] This vignette is emblematic of the fact that peacetime espionage is often perceived as an issue of domestic law, even though it clearly involves international action.[23]

III. IS PEACETIME ESPIONAGE ILLEGAL?

This Comment will now examine peacetime espionage, and the more uncertain legal status surrounding it. Importantly, while peacetime espionage has always had an important role in international relations, the law around it is remarkably unclear.[24] Richard Falk, a professor emeritus of international law, observed that "[t]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture."[25]

Peacetime espionage can be correctly (but imprecisely) defined as espionage that does not qualify as wartime espionage under the 1907 Hague Rules and the Geneva Convention of 1949.[26] This means that wartime espionage is a fairly limited phenomenon that contains a lesser amount of conduct. This Comment will first consider the arguments that peacetime espionage is illegal, then consider the arguments that peacetime espionage is, in fact, legal.

A. Arguments Against Legality of Peacetime Espionage

The interpretive maxim *expressio unius est exclusio alterius* stands for the principle that "the expression of one subject, object, or idea is the exclusion of other subjects, objects, or ideas."[27] For instance, in the 19th century case of *Steinlein v. Halstead*, the defendant argued that certain assignments were void since the attachment of a certificate was not completed.[28] However, the court held that

---

21 *Id.*

22 *Id.*

23 Demarest, *supra* note 5, at 330.

24 Richard A. Falk, *Foreword*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW v (Roland J. Stanger ed., 1962).

25 *Id.*

26 Demarest, *supra* note 5, at 330–32.

27 Clifton Williams, *Expressio Unius Est Exclusio Alterius*, 15 MARQ. L. REV. 191, 191 (1931).

28 Steinlein v. Halstead, 8 N.W. 881, 881 (Wis. 1881).

since the statute did not expressly require the attachment of a certificate, it was not a valid requirement.[29]

For espionage, therefore, the *expressio unius* maxim suggests that since international law allows wartime espionage in specific situations under certain rules, no such allowance exists for peacetime espionage. Since international law expressly allows wartime espionage, but is silent on peacetime espionage, it follows that espionage is outlawed in times of peace. This interpretive maxim has long been considered part of international law.[30] An example in contemporary law can be seen in Article 4 of the 1907 Hague Rules, where the maxim is used to distinguish between legitimate and illegitimate combatants.[31] The consequence of this distinction is that a fighter who doesn't adhere to the basic principles of Article 4 relinquishes its protections.[32] However, many scholars in recent times have greatly criticized *expressio unius* as a canon of construction, finding its reliability suspect.[33]

Another argument for why peacetime espionage is illegal is the basic principle that a country cannot legally violate another country's sovereignty under international law. As it applies to espionage, this argument was best articulated by Professor Wright, a "founding father" in the study of international relations.[34] Wright argued that "[i]n time of peace . . . espionage and, in fact, any penetration of the territory of a state by agents of another state in violation of the local law, is also a violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of other states."[35]

There is precedent for the illegality of state interference in the sovereignty of another country, and such interference does not need to rise to the level of a

---

29 *Id.* at 883 ("Nor must the maxim *expressio unius exclusio alterius* be ignored or underrated . . . . There are many of the requirements of this statute whose performance is essential to the validity of the assignment, and made so in express terms; but this, as we have seen, is not one of them.").

30 *See* OPPENHEIM'S INTERNATIONAL LAW, pts. 2–4, at 1275–82 (Sir Jennings & Arthur Watts eds., 1995).

31 William H. Taft, IV, *The Law of Armed Conflict after 9/11: Some Salient Features*, 28 YALE J. INT'L L. 319, 321 (2003).

32 *Id.*

33 *See* Etienne Mureinik, *Expressio Unius: Exclusio Alterius?*, 104 S. AFR. L.J. 264, 264–65 (1987) (noting Lopes LJ's argument that the maxim of *expressio unius* is often applied without good reason, "that the applicability of the maxim varies greatly with the circumstances of the case, that it is open to many qualifications and exceptions, that the exclusion of what is not expressed is often inadvertent, [and] that the maxim is often unhelpful").

34 Inis L. Claude, Jr., *The Heritage of Quincy Wright*, 14 J. CONFLICT RESOL. 461, 461 (1970).

35 Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, *supra* note 24, at 12.

physical invasion. For example, in *Nicaragua v. United States*,[36] the International Court of Justice (ICJ) ruled that the U.S. had violated its customary international law obligations "not to use force against another State" and "not to violate [another State's] sovereignty" by supporting the rebelling Contras.[37] The ICJ found that a prohibited intervention does not necessarily require the use of force, but rather that a "prohibited intervention[ ] is particularly obvious in the case of an intervention which uses force."[38] This decision, accordingly, stood for the principle that armed force is not necessary to violate international law's prohibition on intervention.[39] In a basic sense, any espionage that takes secret information is a prima facie "intervention" and therefore is a violation of another country's sovereignty, likely a greater violation than was found in *Nicaragua v. United States*.

B. Arguments for Legality of Peacetime Espionage

Expressio unius, when viewed from an alternative perspective, can actually support the argument that peacetime espionage is not prohibited by international law. While the previous *expressio unius* argument was framed from a baseline that all espionage is illegal and international law grants a pocket of permissible conduct during wartime, the inverse argument can be framed from a baseline that all espionage is legal except for the pocket of impermissible conduct expressly banned during wartime.[40] Since peacetime espionage is not explicitly prohibited by the U.N. Security Council or treaties, it can be argued that no such prohibition exists.

Further, while Wright argued that any penetration of a state's territory by agents of another state violates international law, this view was not without its critics. Professor Stone, a premier legal theorist in the field of international law and a contemporary to Wright, took a less absolute view.[41] Stone was writing at a time when the legality of the U.S.'s aerial espionage of the U.S.S.R. was being debated. He took issue with Wright's conclusion that such conduct was absolutely prohibited by international law, and instead focused on the collateral illegality of

---

36 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14 (June 27) [hereinafter *Nicar. v. U.S.*].

37 *Id.* at 147.

38 *Id.* at 107–08.

39 *Id.*

40 In other words, it is possible to also use *expressio unius* to argue that international law does not prohibit peacetime espionage since international law does not expressly ban it.

41 *About Professor Julius Stone*, U. OF SYDNEY, https://perma.cc/EWD4-32BA (last updated May 3, 2017).

the espionage.[42] He concluded that since a satellite in outer space was not violating the territorial integrity of the U.S.S.R., it was entirely possible for peacetime espionage to be performed in a legal way.[43] In other words, Stone argued that it was not the espionage itself that was illegal, but certain means to further such espionage that could violate international law.

Stone believed that technological advancements in the realm of espionage would continually evolve, and that espionage would soon advance to a point where most, if not all, necessary intelligence gathering would no longer rely on territorial intrusion.[44] Further, Stone argued that when countries like the U.S. and the U.S.S.R. have a need for information about their opponent's possible decision to launch a surprise attack, and the countries are unwilling to negotiate an inspection regime, such information can be obtained through mutually tolerated reciprocal espionage.[45] The crux of Stone's argument is that "some part of espionage activity in our existing world represents not the divisive interest of each side against the other, but the common interest of both."[46]

This view is not without modern adherents. Notably, some scholars argue that "espionage facilitates state cooperation and ultimately international security," since treaty enforcement methods, such as verification and enforcement measures, can be insufficient in comparison to espionage.[47] In this view, mutually tolerated reciprocal espionage creates opportunities for cynical countries to be more certain that their partners are complying with treaties, potentially encouraging such countries to sign mutually beneficial (yet risky) treaties in the future.[48]

Of course, the clear weakness of this theory is that it is only relevant to a specific subcategory of espionage related to treaty compliance in mutually beneficial situations. This theory is insufficient to explain how espionage protects

---

42 Julius Stone, *Legal Problems of Espionage in Conditions of Modern Conflict*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, *supra* note 24, at 34.

43 *Id.*

44 *See id.* ("[W]ith satellites like Midas, and other technical developments, we are approaching a situation in which the military reconnaissance function can be exercised from outer space or from the periphery of territorial waters, and there will be no collateral illegality involved in the major spying activities.").

45 *See id.* at 40–42 ("If you do not have a system of international inspection and if you can't get one (and I think it is quite likely that we can't) then the function which international inspection is supposed to serve still needs fulfilling.").

46 *Id.* at 42.

47 Luke Pelican, *Peacetime Cyber-Espionage: A Dangerous but Necessary Game*, 20 COMMLAW CONSPECTUS 363, 373–74 (2012).

48 Baker, *supra* note 15, at 1104 ("[W]ith the availability of espionage, states are more willing to enter into potentially-risky cooperatives. When armed with such tools as spying and eavesdropping, states enjoy greater certainty that they will be able to validate international compliance, or at least detect when other participants are failing to comply . . . .").

international security in most other categories of espionage.[49] Further, the fact that a country tolerates an illegal activity does not necessarily mean such activity becomes legal.

A more universal argument focuses on the prevalence of espionage, rather than any specific justification. While Wright argued that "in principle, all peacetime espionage in foreign territory is illegal," he conceded that "when all are engaging in it, it seems unreasonable to single out one state for utilizing a particular form of espionage, even though that form carries possibilities of hostile action going beyond espionage."[50] In a sense, this argument is similar to Stone's mutually tolerated espionage theory, but the better analogy is to the equitable "clean hands" doctrine: it can be argued that countries that engage in espionage have no business complaining when other countries engage in it as well.

Of course, all espionage is not created equal, as perhaps satellite surveillance meant to verify treaty compliance may be quite innocuous while espionage that destabilizes a country is surely not. Clearly, there are some forms of espionage that are not worth punishing (if only for the sheer volume of espionage that modern technology has facilitated), while it might be exceedingly important to prosecute other forms.

C. Peacetime Espionage is Likely Illegal Under International Law

While *expressio unius* can theoretically be used to characterize peacetime espionage as either legal or illegal depending on the baseline legality, it seems unlikely that the background assumption would be that espionage is legal without an express prohibition. At the risk of being tautological, and starting at the definition of espionage, the presupposition that it is illegal to take information that is not publicly available is difficult to overcome.[51] While Stone's point that there cannot be illegality without physical territorial intrusion is persuasive, it is outdated. Ironically, Stone argued that technology would make territorial intrusion unnecessary for useful espionage, but the rise of the internet has created a world where a remote agent can be more intrusive than a physical breach. While the question of whether cyberspace is legally considered a country's territory is outside the scope of this Comment, the low threshold for "intervention" under *Nicaragua v. United States* implies that the vast majority of modern espionage, including

---

49 Though it is possible that inside knowledge of another state's capabilities and plans could deter disastrous foreign policy mistakes or general bellicose behavior. Perhaps mutually assured destruction, for instance, is more effective when states are aware that their opponents share their fear of nuclear war.

50 Wright, *supra* note 35, at 21.

51 *See Espionage*, *supra* note 1.

computer hacking, would be intrusive enough to reach that threshold.[52] Further, even accepting Stone's argument that satellite surveillance is not prohibited by international law, such surveillance is only one form of espionage, and its usefulness might be quite limited. Finally, Stone's theory of mutually tolerated reciprocal espionage does nothing to defeat the argument that the espionage is nonetheless illegal, and that such illegality is simply not being enforced. Therefore, for the above reasons, this Comment will assume that most peacetime espionage (except perhaps aerial surveillance) is prohibited by international law. The rest of this Comment will explore the question of how this prohibition can be enforced.

IV. ASSUMING THAT PEACETIME ESPIONAGE IS ILLEGAL, CAN THE PROHIBITION BE ENFORCED?

While treaties are the most obvious mechanism for countries to bind one another, "[u]nder traditional international legal theory, [customary international law] is the primary source of universal international law."[53] Customary international law evolves from widespread norms of state practice, and operates to fill the gaps that written treaties often leave open.[54] This view is strongly supported by Hans Kelsen,[55] who argued that when there is "no norm of conventional or customary international law imposing upon the state . . . the obligation to behave in a certain way, the subject is under international law legally free to behave as it pleases; and by a decision to this effect existing international law is applied."[56] Furthermore, customary international law is universal, requiring no explicit approval by states.[57] It has two elements: "(1) state practice, which provides evidence of custom, and (2) the attitudinal requirement of *opinio juris*, which is the general acceptance of a norm as a legal obligation by the world community."[58]

As a caveat, the simplest and most effective enforcement mechanism often is domestic law. A government can take measures to enforce a prohibition of espionage within its own borders, and none of the above is to say that peacetime espionage violations would not be enforced in this way. However, the specific

---

52 *See Nicar. v. U.S.*, *supra* note 36, at 108 ("[The non-intervention] principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States.").

53 J. Patrick Kelly, *The Twilight of Customary International Law*, 40 VA. J. INT'L L. 449, 451 (2000).

54 Scott Sullivan, *Networking Customary Law*, 61 U. KAN. L. REV. 659, 659 (2013).

55 Hans Kelsen was an influential legal academic who introduced the Pure Theory of Law. *See* Nicoletta Bersier Ladavac, *Hans Kelsen (1881-1973): Biographical Note and Bibliography*, 9 EUR J. INT'L L. 391, 393 (1998).

56 HANS KELSEN, PRINCIPLES OF INTERNATIONAL LAW 553–88 (Robert W. Tucker ed., 2d ed. 1966).

57 Sullivan, *supra* note 54, at 659.

58 Kelly, *supra* note 53, at 452.

nature of espionage often precludes enforcement by domestic law, especially in instances where remote cyber attacks are used or where physical agents manage to escape a target country. Outside of these exceptions, there is no real obstacle for a country to enforce a state prohibition on espionage.[59] Nonetheless, even when a spy is caught within a country's borders, prosecuting a spy may be insufficient to deter the country that sent the spy.[60]

Generally, enforcing international law is difficult.[61] The U.N. Charter barely mentions enforcement, and even when the topic does appear, "the Council is not required to take such measures to 'enforce' the Charter or international law."[62] As an illustration, in the *Nicaragua* case, although the ICJ found for Nicaragua and against the U.S., the ICJ was unable to enforce the judgment.[63] During the case, the U.S. refused to participate in the proceedings, and after the judgment, the U.S. vetoed applicable U.N. Security Council resolutions, effectively preventing Nicaragua from obtaining compensation.[64] Even with a U.N. Security Council resolution and "the threat of the adoption of coercive measures in case of non-compliance[,] it has however been observed that these threats usually have a negligible effect on the conduct of those to whom they are addressed."[65] Article VII of the U.N. Charter empowers the Security Council to issue full-scale sanctions, but doing so is often disfavored due to the high risk of such sanctions

---

59 In other words, if a spy is physically caught by the country he/she is targeting, that country is more than capable of punishing the agent. The more difficult problem is punishing the country that caused the espionage, whether said country sent its own agent or hired a local to act as a spy.

60 There is little empirical evidence to support this theory, but effective deterrence likely depends on the type of agents involved. Small countries with few people who meet the necessary criteria for successful spies might be unwilling or simply unable to risk many agents to countries that execute caught spies. On the other hand, the same country might be undeterred from hiring locals to participate in espionage against the target country. While undoubtedly a small country, Israel continued to send its own agents to Syria after the execution of Eli Cohen. *See* Gadi Sukenik, *From Syria with Love: Mossad Launched Mission 'Blanket' in the 70's to bring Syrian Jews to Israel*, YNET NEWS (Oct. 18, 2005), https://perma.cc/XV9Q-ZHXC.

61 See, for example, Michael A. Lysobey, How Iraq Maintained Its Weapons of Mass Destruction Programs: An Analysis of the Disarmament of Iraq and the Legal Enforcement Options of the United Nations' Security Council in 1997-1998, 5 UCLA J. INT'L L. & FOREIGN AFF. 101, 110 (2000) (discussing how in "1997 and 1998 Iraq deliberately and consistently engaged in non-compliance and obstruction aimed at preventing the Commission from fulfilling its mandate" of disarmament, and how the Security Council was unwilling or unable to use adequate enforcement measures).

62 Oscar Schacter et al., *Compliance and Enforcement in the United Nations System*, 85 AM. SOC'Y INT'L L. PROC. 428, 428 (1991); *see also* Lysobey, *supra* note 61, at 105. ("[E]nforcement remains a vital but often unrealizable element in the furtherance of an international rule of law.").

63 Fred L. Morrison, *Legal Issues in the Nicaragua Opinion*, 81 AM. J. INT'L L. 160, 160 (1987).

64 *Id.*

65 Marco Roscini, *The United Nations Security Council and the Enforcement of International Humanitarian Law*, 43 ISR. L. REV. 330, 344 (2010).

disproportionately harming civilians.[66] Even with smart sanctions,[67] implementation is dependent upon member states, meaning the sanctions' efficacy is doubtful.[68]

A. The Generalized Enforcement Mechanism of Customary International Law

Critics of customary international law such as Professor Goldsmith and Professor Posner argue that such law has little to no impact on state behavior, namely because "international law lacks an enforcement mechanism and, as a result, cannot have any relevance in a one-shot prisoner's dilemma."[69] Other critics argue that customary international law is ineffective because it lacks democratic control over its content: it has a substantial "democracy deficit."[70] In other words, the argument is that domestic law is far superior to international law since "democracy is the political process most likely to generate beneficial norms" and international law is inherently undemocratic.[71]

On the other hand, proponents reject the argument that customary international law normally operates in one-shot situations, and instead argue that

---

66 *Id.* at 345.

67 A smart sanction can be defined as a "sanction against a nation or state that targets specific persons (especially members of the ruling elite) or particular imported (especially military) goods, in order to minimize the adverse effects on the general civilian population." *See Smart Sanction*, OXFORD LIVING DICTIONARIES, https://perma.cc/Z6E4-8XJ2 (last visited Jan. 21, 2017).

68 Roscini, *supra* note 65, at 346.

69 The prisoner's dilemma refers to an imaginary situation where two individuals are accused of having cooperated to commit a crime. The individuals are arrested, and held in such a way that they are unable to communicate with each other. The dilemma is as follows: each prisoner will get a light sentence if neither person confesses to the police about the other's involvement. If one person confesses to the police, the other prisoner will get a heavy sentence while the confessor goes free. If both people confess to the police, both prisoners will get heavy sentences. The general consensus is that a one-shot prisoner's dilemma greatly incentivizes cheating, whereas a prisoner's dilemma with repeat actors incentivizes cooperation; Andrew T. Guzman, *Saving Customary International Law*, 27 MICH. J. INT'L L. 115, 128 (2005); *see also* Jack L. Goldsmith & Eric A. Posner, *Understanding the Resemblance Between Modern and Traditional Customary International Law*, 40 VA. J. INT'L L. 639, 658–59 (2000) (arguing that customary international law does not follow the pattern of a repeat prisoner's dilemma, due in part to the fragility of the cooperation and in part to the fact that "the bilateral prisoners' dilemma cannot, without implausible assumptions, be expanded to a multi-player prisoners' dilemma, where monitoring and other information costs rise, the incentives for any particular nation to defect from cooperation increases, and the incentives for any particular nation to punish deviation decreases").

70 John O. McGinnis & Ilya Somin, *Should International Law Be Part of Our Law?*, 59 STAN. L. REV. 1175, 1177 (2007).

71 *Id.* at 1178.

states are repeat actors with a long-term interest in following custom.[72] These proponents dispute that customary international law violations require multilateral state cooperation to sanction offenders.[73] Instead, "states affected by the violation may choose to take some sort of retaliatory action" rather than rely on explicit coordination between states.[74] Proponents maintain that customary international law more closely represents a bilateral repeat prisoner's dilemma rather than a multi-player version.[75] Additionally, they argue that reputational sanctions can have a natural conforming effect on violators, and reputational sanctions do not require any coordinated action by affected states.[76]

There is undoubtedly no consensus about the enforcement capability of customary international law on public matters. For this reason, the enforcement capability of customary international law on covert matters may be even more suspect.

B. Specific Challenges for Enforcing a Prohibition on Peacetime Espionage

The new cyber world makes it difficult to track clandestine action. As states become more and more reliant on computer systems, and as technology advances, increasing sophistication by hackers may make it difficult to identify violators.[77] However, this is not to say that technological advancements won't increase in such a way as to lessen the relative anonymity that the internet provides, but that is difficult to predict. Relatedly, the rise of end-to-end encryption[78] may mean that the deployment of field agents will continue to increase rather than decrease, as opposed to what may have been predicted in the 1990s and 2000s.[79] The reason

---

72 Guzman, *supra* note 69, at 130.

73 *Id.*

74 *Id.*

75 *Id.*

76 *Id.* at 135.

77 Robert Siegel, *Terrorists Escape Detection Using Common Encryption Tools*, NPR (Mar. 25, 2016), http://www.npr.org/2016/03/25/471891553/terrorists-escape-detection-using-common-encryption-tools ("As authorities in Europe search for suspects in the Brussels attacks and try to disrupt future attacks, they are hampered by technology. Apps that allow you to send encrypted text and voice messages have become the tools of the terrorist trade.").

78 End-to-end encryption "means that messages are encrypted in a way that allows only the unique recipient of a message to decrypt it, and not anyone in between. In other words, only the endpoint computers hold the cryptographic keys, and the company's server acts as an illiterate messenger." *See* Andy Greenberg, *Hacker Lexicon: What is End-To-End Encryption?*, WIRED (Nov. 25, 2014), https://perma.cc/B5J6-H3QX.

79 *See* Siegel, *supra* note 77 ("[P]opular applications like Telegram Messenger, Threema, Kik, Surespot . . . help to achieve a level of encryption, in text messaging in particular, that's very difficult

for this is simply that intercepted encrypted transmissions are often useless to intelligence agencies, causing leaders of the community (such as the director of the FBI) to advocate for special access.[80]

In addition to the difficulty of tracking spies, it can sometimes be difficult to link an agent to a specific country. States may have plausible deniability if they sponsor or tolerate espionage abroad. Further, while the most effective espionage (whether traditional or cyber) will never be noticed by its target, the sheer number of cyber attacks can overwhelm even the most capable intelligence agencies, even if such attacks could conceivably be traced.[81] Moreover, hackers can be highly sophisticated, and it can be difficult to know for sure that a state was involved in any specific theft of information.[82] Non-state actors likely engage in cyber attacks daily, and such attacks can be grand in scope, from sabotaging government websites to stealing important information.[83]

C. Stuxnet as a Case Study[84]

As a recent example, in June of 2010, a security firm in Belarus discovered the existence of malicious software (malware) specifically designed to attack the

---

for authorities to intercept in the first place and, secondly, to decrypt, unwind the message and ascertain what it is that's being conveyed.").

80 Nicole Perlroth & David E. Sanger, *F.B.I. Director Repeats Call That Ability to Read Encrypted Messages Is Crucial*, N.Y. TIMES (Nov. 18, 2015), https://perma.cc/76GT-ZVGM.

81 *See* Jason Koebler, *U.S. Nukes Face Up to 10 Million Cyber Attacks Daily*, U.S. NEWS & WORLD REP. (Mar. 20, 2012), https://perma.cc/S6ZG-K7BK; Ryan Browne, *NATO: We Ward Off 500 Cyberattacks Each Month*, CNN, https://perma.cc/AL3Q-VZEY (last updated July 18, 2017).

82 *See* Christopher D. DeLuca, *The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors*, 3 PACE INT'L L. REV. ONLINE COMPANION 278, 279 (2013) ("The rise of these . . . non-state actors and their growing involvement in world politics challenges the assumptions of traditional approaches to international relations which assume that states are the only important units of the international system.") (quoting Gustaaf Geeraerts, *Analyzing Non-State Actors in World Politics*, 1 POLE PAPERS, no. 4 (1995), https://perma.cc/DF3Z-DR2C).

83 *See id.* at 291–92 ("Al Qaeda 'used the Internet to launch . . . computer attacks,' and that the organization 'also sabotaged other websites by launching denial of service attacks, such as one targeting the Israeli prime minister's computer server.'") (quoting Alex Kingsbury, *Documents Reveal Al Qaeda Cyberattacks*, U.S. NEWS & WORLD REP. (Apr. 14, 2010), https://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks).

84 Some may dispute that Stuxnet can be properly characterized as espionage since the worm was intended to disrupt Iran's nuclear program rather than simply gather information. Regardless, this Comment takes the position that cyberspace has, in some ways, made the old conception of espionage obsolete. Electronic eavesdropping is no passive endeavor, and doing so usually involves breaking into an enemy's network and installing malicious software designed to assert control over the system. In other words, "from the point of view of the object of an attack, [computer network exfiltration] and [computer network attack] look the same as each other, except for the end result. Today's surveillance systems involve breaking into the computers and installing malware, just as cybercriminals do . . . ." For these reasons, this Comment argues that there should not be a

Industrial Control Systems that manage nuclear plants.[85] In all likelihood, the main target of the sophisticated worm was the nuclear program of the country of Iran.[86] The worm seemed to have destroyed "key parts at the [Natanz uranium] enrichment center."[87] According to Dr. Mohammed Ahmadian, an Iranian Atomic Energy Organization official, "the worm may have been transferred to computers at the reactor site via 'CDs and Flash memory sticks,'" rather than via the internet.[88] Many have speculated that the sophistication of the worm, in addition to its Iranian target, is strong evidence that the developer was either Israel or the U.S.[89]

Though the secretive nature of the espionage prevented Iran from making that determination conclusively, it is unclear if catching and prosecuting the spies would actually be an effective deterrent. A country that loses a field agent to a hostile country's government may simply decide to send more field agents to that country. Going further, while there is clearly a limit to the number of capable field agents a country will risk, there is likely no similar limit to the number of times a country will attempt to bribe citizens of a hostile country. To illustrate, assuming that Stuxnet was planted by an agent of the national intelligence agency of Israel (the Mossad), Israel might be deterred by the capture of one of their best agents. Conversely, if the Mossad bribed a Natanz employee or scientist to plant the worm, Iranian capture of an Iranian citizen would likely not deter Israel from further bribery attempts.[90] At worst, the Mossad's future bribery attempts may be rebuffed more often.

---

categorical legal distinction between the forms of espionage intended to gather information and the forms of espionage intended to sabotage another party. *See* Bruce Schneier, *There's No Real Difference Between Online Espionage and Online Attack*, THE ATLANTIC (Mar. 6, 2014), https://perma.cc/6LSG-55YZ.

85 PAUL K. KERR ET AL., CONG. RESEARCH SERV., R41524, THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY 1 (2010).

86 *Id.* at 3.

87 Chance Cammack, *The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression*, 20 TUL. J. INT'L & COMP. L. 303, 304 (2011); *see also* KERR ET AL., *supra* note 85, at 5 ("[S]ome accounts suggest that the malicious software may have slowed down or disabled operations at Iran's enrichment facilities.").

88 KERR ET AL., *supra* note 85, at 3–4.

89 *Id.* at 4.

90 In the case of bribing especially, effective deterrence would likely require the offending country or suborner to be prosecuted directly.

1. Espionage is Not Clearly a Crime of Aggression Under the Rome Statute.

In June 2010, the International Criminal Court (ICC) adopted amendments to the Rome Statute that gave the ICC jurisdiction over the crime of aggression.[91] A crime of aggression is simply defined as an act of aggression.[92] Notably, non-state actors are excluded from the ICC's jurisdiction for this crime.[93]

While the U.N. Security Council can refer ICC jurisdiction in the same way it does for other crimes, "if the conflict is between State parties, a prosecutor for the ICC may only bring his own investigation after first determining whether the Security Council has made a finding of the existence of an act of aggression."[94] The Security Council, under Resolution 3314, determines when a state has committed an act of aggression.[95] Therefore, to prosecute a crime of aggression, the ICC must (1) have jurisdiction over (2) an armed force (3) by a state party in the ICC against another state party in the ICC.[96]

It is unclear whether Israel or the U.S. could be theoretically prosecuted by the ICC for a crime of aggression for the Stuxnet virus.[97] Since the U.S., Israel, and Iran are not parties to the ICC,[98] there could not be jurisdiction over the parties. However, even assuming the aforementioned states were all parties to the

---

91 Assembly of State Parties, Review Conference, the Crime of Aggression, ICC Doc. RC/Res. 6, Art. 8 (June 11, 2010) [hereinafter Kampala Amendment]. The ICC defines a crime of aggression as:

> The planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations.

Id. However, the ICC will not exercise jurisdiction until either thirty parties ratify the amendments or two-thirds of parties vote to activate jurisdiction after January 1, 2017.

92 An act of aggression is defined as:

> The use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. Any [acts such as invasion by armed forces, bombardment and blockade], regardless of a declaration of war, shall, in accordance with United Nations General Assembly resolution 3314 (XXIX) of 14 December 1974, qualify as an act of aggression.

Id.

93 *See Delivering on the Promise of a Fair, Effective and Independent Court: The Crime of Aggression*, COAL. FOR INT'L CRIM. CT., https://perma.cc/AVV7-5DR4 (last visited Jan. 27, 2017) ("Non-State Parties have been explicitly excluded from the Court's jurisdiction into a crime of aggression under this article when committed by that State's nationals or on its territory.").

94 Cammack, *supra* note 87, at 308.

95 *Id.* at 313.

96 *See id.* at 320–24.

97 This, of course, assumes that one of these two countries was responsible for the worm.

98 Cammack, *supra* note 87, at 324.

ICC, the applicability of the crime aggression to the Stuxnet worm is not clear-cut. While the sophistication of the worm is strong evidence that state actors were the developers of the malware, the Kampala Amendment's requirement that the offending party use armed force is problematic. The Kampala Amendment's illustrations of armed force all center around physical violence, and its text states that the acts that qualify as armed force are greatly influenced by U.N. General Assembly Resolution 3314 (XXIX) of 14 December 1974, which only lists traditional warfare as constituting aggression.[99]

Nevertheless, Article 4 of the Resolution clearly states that "[t]he acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter."[100] Therefore, Resolution 3314 surely does not constrain the ICC's view of what constitutes an act of aggression any more than the Kampala Amendment does, as the Kampala Amendment implies the same non-exhaustive language. This means that as long as the acts of physical aggression enumerated in the Kampala Amendment are not actually exhaustive, it is possible that more general acts of traditional espionage and cyber-espionage can be considered to violate the prohibition on crimes of aggression.[101] Still, there does not seem to be precedent for non-physical action being characterized as a crime of aggression.

Moreover, Stuxnet is emblematic of one of the more extreme types of espionage, and it seems unlikely that a more typical and less physically destructive act of espionage (such as simple information theft) could be considered a crime of aggression if even Stuxnet does not obviously meet the criteria.[102] Therefore, this Comment will consider other ways to enforce a prohibition on espionage.

---

99 *See generally* G.A. Res. 3314 (XXIX), at arts. 1–4 (Dec. 14, 1974).

100 *See id.* at art. 4.

101 However, there is reason to believe that even if the ICC were able to prosecute espionage, the Court would not do so. As has been discussed previously, espionage is constantly practiced by many, if not most, countries. It is possible that opening the floodgates with respect to such prosecutions would be a distraction from the ICC's core mission of prosecuting more serious crimes like genocide, crimes against humanity, and war crimes.

102 Interestingly, classifying espionage as a crime of aggression introduces another problem. If the act of espionage itself is a crime of aggression in the same category as armed invasion, it would seem that the espionage can no longer be called "peacetime" espionage. As discussed in Section I, there are clear rules for wartime espionage, and it is unclear how and if such rules could apply to the act of planting a computer worm.

V. POTENTIAL ALTERNATIVE ENFORCEMENT MECHANISMS

A. U.N. Security Council's Prohibition on Force

Article 2(4) of the U.N. Charter summarizes international law's prohibition on force, stating "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[103]

There are two exceptions to this mandate: Articles 39 and 42 allow the U.N. Security Council to "determine the existence of any threat to the peace" and, if necessary, "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."[104] Additionally, Article 51 authorizes the use of force in self-defense, noting that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."[105] Unlike the previous discussion regarding whether Stuxnet could be considered a crime of aggression, "[t]here has been an international consensus among scholars and the U.N. that cyber-attacks may be understood under the U.N. Charter even though such an attack is not explicitly mentioned in the Charter."[106] While articles 2(4), 39, 42, and 51 do not explicitly refer to any specific weapons, "the International Court of Justice in its advisory opinion on nuclear weapons found that these provisions 'apply to any use of force, regardless of the weapons employed.'"[107] Furthermore, the Court held that "the rules of war under the U.N. Charter apply even as new weapons are introduced that were not originally considered or even imagined by the drafters of the Charter."[108]

Therefore, it is plausible that an attack like Stuxnet could be considered force under the U.N. Charter. To illustrate, although no bomb was dropped on the Iranian Natanz reactor, the Stuxnet worm did damage comparable to that of a bomb.

Nevertheless, the U.N.'s traditional understanding of force seems to have required at least some sort of military action,[109] and further, traditional or cyber-

---

103 U.N. Charter art. 2, ¶ 4.

104 *Id.* at arts. 39, 42.

105 *Id.* at art. 51.

106 David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 MINN. J. INT'L L. 347, 356 (2013).

107 *Id.*

108 *Id.*

109 *Id.* at 357–58.

espionage need not rise to the level of destruction that Stuxnet did. While the worm did costly damage to Iran's nuclear reactor, Eli Cohen, for example, did not personally harm any Syrian people or property. For these reasons, it may be implausible for the U.N. to extend the definition of force to cases of mundane computer hacking, even if such conduct does require overwhelming another party's computer systems.[110]

B. European Council Laws

Due to "the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks," the Council of Europe sought to take a step to fight against cybercrime.[111] The Council "established a Committee of Experts on Crime in Cyberspace (PC-CY) in 1997 to draft a binding convention facilitating international cooperation in the investigation and prosecution of computer crimes," resulting in the Convention on Cybercrime.[112] The Council requires parties to approve legislation against cybercrime, to authorize and train law enforcement to investigate and prosecute cybercrime, and to cooperate with other states and parties involved in these efforts.[113] Interestingly, "[t]he treaty also includes a provision granting a participating state jurisdiction over offenses committed within that state's territory."[114] This permits a participating state to assert jurisdiction over a cybercrime concerning every computer system within its territory, even if the culprit committed the offense from abroad.[115] While the treaty was written to help states cooperate to punish individuals that commit cybercrimes, it is potentially applicable to state-sponsored or state-tolerated cybercrimes. The fact that a state has jurisdiction over a cybercrime committed outside its borders could go a long way in prosecuting some of these acts of espionage.

As an example, when Russian hackers attacked American banks to steal sensitive financial information in 2000, the nation of Russia refused to assist the

---

110 However, an agent taking violent action against personnel in pursuit of intelligence would be an entirely different story. Still, it would be the attack on a person that would be the use of force, rather than the theft of information.

111 Convention on Cybercrime, *opened for signature* Nov. 23, 2001, E.T.S. No. 185, https://perma.cc/6QQP-43S9 (last visited Jan. 28, 2017).

112 Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425, 429 (2003).

113 *See* COUNCIL OF EUR., EXPLANATORY REPORT TO THE CONVENTION ON CYBERCRIME ¶ 16 (2001), https://perma.cc/T43G-TTE8.

114 Weber, *supra* note 112, at 432.

115 *Id.*

U.S. with the investigation into the suspects.[116] The U.S. lured the suspects to Seattle with promises of a job at a fictitious security company in order to obtain the hackers' passwords to servers in Russia.[117] The FBI was therefore able to download incriminating evidence from these servers without the consent of the Russian government, sparking an international debate about the legality of such a practice.[118] While there was no mutual assistance treaty regarding cybercrime at the time the U.S. requested Russia's help, there is no guarantee that Russia would have cooperated if there had been such a treaty. Further, Russia would almost surely not assist an investigation into cybercrime that involved the country's government itself. As an illustration, assuming that the Russian government perpetrated the hack of the Democratic National Committee during the 2016 U.S. presidential election, it's implausible to suggest that the mutual assistance provision from the Convention on Cybercrime would convince Russia to present evidence of its own wrongdoing.[119] Still, the Convention on Cybercrime is binding, and it does encourage the parties to agree to have disputes handled by arbitration or the ICJ.[120] In a narrow category of espionage, the Convention on Cybercrime may be effective.

C. Countermeasures

As previously discussed, the U.N. Charter notes an "'inherent right of individual or collective self-defence if an armed attack occurs . . . until the Security Council has taken measures necessary to maintain international peace and security."[121] Alternatively, "[c]ountermeasures are nonviolent 'measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter.'"[122] In other words, since countermeasures are meant to address wrongful acts less severe than armed attack, such measures seem to be a promising way to enforce a prohibition on espionage.

---

116 Robert Lemos, *FBI "Hack" Raises Global Security Concerns*, CNET (Mar. 28, 2002), https://perma.cc/FAB5-GC78.

117 *Id.*

118 *Id.*

119 The U.S., as an observer state at the Council of Europe, ratified the Convention on Cybercrime. *See* Dan Kaplan, *Senate Ratification of Cybercrime Treaty Praised*, SC MEDIA (Aug. 4, 2006), https://perma.cc/FV4T-PUX8.

120 Convention on Cybercrime, *supra* note 111, at art. 45.

121 U.N. Charter, *supra* note 103, at art. 51.

122 David E. Pozen, *Self-Help and the Separation of Powers*, 124 YALE L. J. 2, 54 (2014) (quoting *Draft Articles and Commentary on Responsibility of States for Internationally Wrongful Acts*, 2 Y.B. INT'L L. COMM'N 31, 128 (2001)).

Countermeasures are not to be confused with retorsion, defined as a state's retaliation against another state, but still consistent with the retaliating state's obligations under international law.[123]

Using the *Nicaragua* Court's distinction between force and non-intervention, it is potentially lawful for a state to deter espionage by using countermeasures, as introduced by the *Naulilaa* case by reference to the customary international law of reprisals.[124] This concept was further developed by the International Law Commission's (ILC) Articles in 2001.[125]

The U.N. General Assembly adopted Resolution 56/83, which annexed the text of the ILC's articles to the Resolution.[126] The ILC Articles require that countermeasures are:

> (1) aimed at the state that violated its obligations towards the injured state, (2) limited to the temporary non-performance of the obligations of the injured state and should as far as possible be reversible so as to allow for the resumption of the performance of the original obligation, (3) terminated when the wrongdoing state has complied with its obligations, (4) commensurate with the injury suffered and have as their purpose to induce the wrongdoing state to comply with its obligations under international law.[127]

In addition to the requirement that the countermeasure be proportionate to the harm suffered,[128] the "prevailing view is that countermeasures cannot involve the use of force or affect peremptory norms, fundamental human rights obligations, humanitarian obligations prohibiting reprisals, or obligations to respect the inviolability of diplomatic and consular agents, premises, archives and documents."[129] Some have argued that under a theory of cyber self-defense, American companies should be authorized to "hackback" and retaliate against cyber attacks intended to steal information.[130] For this purpose, Symbiot, Inc. provided "hackback" models that included "accessing, disabling, or destroying the hacker's assets."[131] As an important note, a government is liable for wrongful

---

123 *Countermeasures*, 25 U.N. Legis. Ser. 304, 304–05 (2012).

124 Naulilaa Incident Arb. (Port. v. Ger.), 2 R.I.A.A. 1011, 1025–26 (1928).

125 Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, art. 22, U.N. Doc. A/56/10 (2001).

126 G.A. Res. 56/83, at 1 (Jan. 28, 2002).

127 Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage under International Law*, 40 N.C. J. INT'L L. & COM. REG. 443, 516–17 (2015).

128 *See* G.A. Res. 56/83, *supra* note 126, at art. 51 ("Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question.").

129 Lotrionte, *supra* note 127, at 517.

130 Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275, 279–80 (2013).

131 *Id.* at 293.

countermeasures performed by private actors if it allows such companies to "hackback."[132]

However, "ambiguity exists between customary law and the ILC Articles as to when an injured state's right to carry out countermeasures begins and ends."[133] The ILC failed to include any mandatory dispute settlement procedures in the final text.[134] Instead, the ILC Articles require an injured party to give notice to the offending party and offer to negotiate before beginning countermeasures.[135] "[T]he countermeasures must be suspended if the 'wrongful act has ceased' and 'the dispute is pending before a court or tribunal which has the authority to make decisions binding on the parties.'"[136] Plainly, "the ILC Articles create a bar to the continuance of countermeasures once the offending conduct stops and the matter is submitted 'to any third party dispute settlement procedure.'"[137] While the countermeasures for intellectual property theft may seem clear, it is less obvious what the non-force countermeasure to traditional espionage or political cyber-espionage would be.

In the same way that the U.S. embargoed foreign trade with Cuba,[138] countries can take trade measures against one another when espionage is used. A notable example of economic response to non-economic action is the U.S.'s use of tariffs in 1940. After Japanese invasions of Manchuria (1931), China (1937), and French Indochina (1940), President Roosevelt ordered a trade embargo on American steel and oil, greatly harming the Japanese war effort.[139] If a country is plagued by another country's espionage, it seems to be a simple step for the victim to cease trade with the spying country. It is further possible for such a country to legally respond by freezing assets of the offending country, delaying trade obligations to the offending country, or setting up tariffs on the products of the offending country.

However, a significant weakness of the universal viability of countermeasures to combat espionage is that weak states will likely be unable to effectively respond. Even if the illegal espionage can be proven, it is difficult for

---

132 *See* Lotrionte, *supra* note 127, at 519 ("[B]y retaining the services of a private entity to carry out the countermeasures, the state assumes responsibility and any liability that attaches for any wrongful actions taken by the company.").

133 *Id.* at 520.

134 *Id.* at 521.

135 *Id.*

136 *Id.* at 522 (quoting G.A. Res. 56/83, art. 52(3)).

137 *See* Lotrionte, *supra* note 127, at 523.

138 Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996, 22 U.S.C. §§ 6021–91 (1996).

139 *Japan's Quest for Power and World War II in Asia*, ASIA FOR EDUCATORS, https://perma.cc/EGD3-G3WA (last visited Nov. 18, 2017).

a weak country to have an effective countermeasure against a stronger country without a powerful ally or substantial leverage.[140] Additionally, a stronger country can justify its own aggression against a weaker country either by simply claiming that the weaker country also engaged in espionage, or by providing some evidence to that effect, while responding in a disproportionate way (such as with their own cyber attacks).[141] While these criticisms are significant, the possibility of failure in some situations does not demonstrate that countermeasures should not be used.

D. Domestic Law

Almost every country will punish espionage committed against it, and this has likely been one of the primary historical deterrents to engaging in espionage.[142] It is a tremendous risk for field agents to go into enemy territory alone, with little hope of rescue, to gather information. However, the information age has allowed more and more espionage and information theft to occur remotely, which frustrates the ability of states to physically punish spies. Still, the primary concern with state-sponsored espionage lies with the action by a country's government. Therefore, while international arrest warrants and raids can possibly enforce prohibitions on espionage against lone wolves, such methods are insufficient to enforce against offending governments. Punishing a spy within a country's borders seems to be an entirely different animal than attempting to extradite a government spy back to the targeted country.[143]

VI. SOLUTION

The greatest apparent flaw with most of the aforementioned enforcement mechanisms is simply that their effectiveness is inconsistent or only applicable in

---

140 See Robert K. Omura, *Chasing Hamlet's Ghost: State Responsibility and the Use of Countermeasures to Compel Compliance with Multilateral Environmental Agreements*, 15 APPEAL: REV. CURRENT L. & L. REFORM 86, 105 (2010) ("Weaker states are unlikely to seek countermeasures against a more powerful wrongdoer, largely because the impact on the more powerful wrongdoer is likely to be minimal and the benefits of association with the non-compliant party will often outweigh the costs.").

141 It is unclear what a state would have to gain by using countermeasures against a non-offending state, but it is possible. Regardless, the possibility of bad faith is limited by the requirements that a state offer to negotiate with the offending state before using countermeasures, and that the countermeasures cease as soon as the dispute is brought before a court or tribunal with binding authority.

142 Murdoch Watney, *Restricting Excessive State-on-State Cyber Espionage Under International Law: A Quest of Futility?*, *in*, ISSE 2014 SECURING ELECTRONIC BUSINESS PROCESSES 134, 134 (Helmut Reimer et al. eds., 2004).

143 Further, while losing an individual spy may impose a significant cost on the offending country, it is plausible that effective countermeasures would be able to impose an even higher cost by targeting the offending country directly.

narrow situations. The very nature of espionage is that the act is secretive, and this often means that the obvious damage is small (at least initially). Furthermore, the aforementioned enforcement mechanisms have sometimes been unable to stop extreme human rights violations, so their efficacy for something more minor like espionage is in question.[144] Sanctions, even if implemented and enforced, can be cheated by countries that are powerful in the international arena, severely lessening their consequences. Additionally, the most capable international bodies, such as the ICC, may not have the jurisdiction or the interest in handling mundane espionage cases. For these reasons, countermeasures seem to be the best way to actually enforce a prohibition on espionage. It allows the affected party to respond quickly and without approval from often distracted or disinterested international parties.

To remedy the scenario where a powerful country uses espionage against a country that will be incapable of deploying countermeasures, this Comment suggests supplementing the use of countermeasures with any of the previously discussed enforcement mechanisms available. In other words, a weak country experiencing a more extreme form of espionage may be able to rely on the ICJ, the ICC, the U.N. Security Council, or the Council of Europe, depending on the situation, to end a stronger country's malevolent behavior. Particularly destructive or intrusive espionage may get the attention of the international community in a way that low-level espionage would not. Of course, this is far from an ideal situation, and many instances of espionage experienced by a weak country will still likely go unpunished. Still, this Comment argues that a combination of countermeasures and international bodies such as the U.N. Security Council will be able to prevent some of the espionage that would otherwise continue undiscouraged.

VII. CONCLUSION

This Comment has shown the challenge of even determining the legality of peacetime espionage, let alone the difficulty of enforcing a prohibition on it. Espionage dates back millennia, and it shows no signs of slowing down. Recent technological advancement has complicated the issue, but has not fundamentally transformed it. Importantly, the most successful espionage will never be recognized, meaning that some significant espionage will always fall through the cracks. This is a truth that must be accepted when attempting to enforce a prohibition on any such secretive activity. It must further be remembered that it can be difficult to enforce international law, especially when the competing interests and considerations of many states tasked with enforcement conflict with

144 *See, for example*, *Burundi: ICC Withdrawal Major Loss to Victims*, HUM. RTS. WATCH (Oct. 27, 2016), https://perma.cc/X7LH-9ZFJ (discussing the country of Burundi's withdrawal from the ICC after being accused of extreme human rights abuses).

the law. Regardless, countermeasures may be able to put at least one solution directly into the hands of the affected parties. While espionage will surely continue for the foreseeable future, it is perhaps possible to stop some of the more egregious violations.