Countering State-Sponsored Cyber Economic Espionage Under International Law

Catherine Lotrionte[†]

---

† Dr. Catherine Lotrionte is the Director of the CyberProject at Georgetown University, School of Foreign Service. She also served as a former Assistant General Counsel, CIA and Counsel to the President's Foreign Intelligence Advisory Board at the White House from 2002-2006. Recently, she was appointed to the World Economic Forum's Global Agenda Council on Cybersecurity.

I. Introduction

The end of the Cold War confrontation brought about a major shift in the national security priorities of most modern industrial countries, away from the diminishing Soviet military threat and toward new priorities, including economic espionage. Whereas states previously engaged in espionage primarily for military and foreign policy purposes, today, intelligence operations concentrate more intensely on conducting, or guarding against, economic espionage. States have come to recognize the significant role the economy plays in the stability of the state, informed by the demise of the Soviet Union, caused by a failed internal economy, without any military confrontation between superpowers.

The fate of the Soviet Union provides a stark reminder that national security rests on a strong economic foundation, not mere military strength.[1] Although traditional issues of arms control and energy production are still important, new issues of intelligence and security, expanding financial markets, and international trade in a networked community have joined them.[2] With the advent of

---

1 *See* PETER SCHWEIZER, FRIENDLY SPIES 30-31 (1993) ("The business of trade negotiations is as central to U.S. national security interests now as arms control negotiations were during the last forty years.").

2 *See generally* OFFICE OF THE UNDER SEC'Y OF DEF. FOR ACQUISITION & TECH., REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON INFORMATION WARFARE – DEFENSE (1996) [hereinafter DEFENSE SCIENCE BOARD] (reporting on "information

the Internet, economic competition has come to be played out in the cyberspace domain, intensifying competition in every industrial sector, with a corresponding rise in economic espionage by some states.[3]

This new economic world order calls for closer examination of the role of international law in providing minimum public order where economic espionage has proliferated.[4] As scholars have noted, intelligence can function to improve world public order, support cooperation, promote peace, reduce international tension, and develop prescriptive norms of international law.[5] But in a world where economic competition places no limits on what intelligence will be used for, the development of international law to govern economic competition in the cyber domain will be important for shaping future state behavior and providing stability to international economic order.

As for the development of international law related to cyber operations, most contemporary legal analysis has focused on the obligations of states conducting cyber operations in response to "attacks" that rise to the level of a "use of force" or "armed attack."[6] For the past ten years, scholarly work in this area has

---

warfare" focusing on the vulnerability of the U.S. national infrastructure from cyber attacks).

3 John Stanton, *Industrial Espionage Becoming "Big Business,"* NAT'L DEF. (July 2001), http://www.nationaldefensemagazine.org/archive/2001/July/Pages/Industrial_Espionage7002.aspx?PF=1.

4 *See* Myres S. McDougal et al., *The Intelligence Function and World Public Order*, 46 TEMP. L.Q. 365, 370-71 (1973).

5 Christopher D. Baker, *Tolerance of International Espionage*, 19 AM. U. INT'L L. REV. 1091, 1097 (2003) (describing how espionage can be viewed as a "functional tool that enables international cooperation"); *see* McDougal et al., *supra* note 4, at 432 (explaining how intelligence collection can increase trust among states, leading to more peaceful relations); *see also* Loch K. Johnson, *Think Again: Spies*, FOREIGN POL'Y, Sept. 1, 2000, at 1, 13, *available at* http://www.foreignpolicy.com/articles/2000/09/01/think_again_spies (commenting on the diverse goals advanced through espionage).

6 MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 (2013) [hereinafter TALLINN MANUAL]. The group of twenty academics and legal practitioners prepared the recently published manual applicable to cyber warfare, drafting 95 "black letter rules" that were meant to restate the existing law; however, the manual does not cover the issue of intervention, and focuses instead on those cyber activities that occur at the level of a "use of force" and "armed attack." *Id.* at 6; *see also* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 886 (1999) [hereinafter Schmitt, *Computer Network Attack*]

focused almost exclusively on United Nations Charter, Article 2(4), prohibiting the use of force,[7] with very little focus on the norm prohibiting intervention.[8] While cybersecurity experts observe that cyber operations today equivalent to a use of force against transportation systems, electricity networks, dams, and chemical or nuclear plants are technically feasible, these types of cyber attacks seem unlikely based on state practice to date.[9] The most malicious activities reported thus far have involved lower level cyber operations, rather than violent attacks.[10] Such activity has included the disruption of websites, infections of computer networks, and theft of valuable data from private companies with

---

(exploring the use of force against computer network attacks); Eric T. Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 208-209 (2002) (proposing that international law evolve to recognize attacks against a nation's computer network constitutes a use of force); Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 270 (2014) (discussing how the law of cyber warfare may mature in the coming decade).

[7] *See, e.g.*, Schmitt, *Computer Network Attack*, *supra* note 6. *See also* Sean Kanuck, Recent Development, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 288 (1996).

[8] Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT & SECURITY L. 211, 221 (2012) (discussing the reasons the norm of non-intervention has been ignored); *see* Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 848 (2001) (analyzing how the non-intervention principle may apply to cyber operations); *see also* Sean Watts, *Low-intensity Cyber Operations and the Principle of Non-intervention*, BALTIC Y.B. OF INT'L L. (forthcoming November 2014) (examining whether low-intensity cyber operations implicate non-intervention principles); Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. (forthcoming 2014) [hereinafter Schmitt, *Cyber Operations*] (focusing on countermeasures for cyber operations below the article 2(4) threshold).

[9] S. SELECT COMM. ON INTELLIGENCE, 113TH CONG., WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 1 (2013). Although noting the importance of cyber economic espionage and hacker attacks, in written testimony to the Senate Intelligence Committee, Director of National Intelligence James R. Clapper, Jr. said there was only a "remote chance" of "a major cyber attack against US critical infrastructure systems during the next two years that would result in long-term, wide-scale disruption of services . . . . The level of technical expertise and operational sophistication required for such an attack . . . will be out of reach for most actors . . . . Advanced cyber actors – such as Russia and China – are unlikely to launch such a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interests." *Id.*

[10] *Id.*

primarily economic effects as opposed to personal injury or death.[11] Some states have found it expedient to resort to non-forcible methods of promoting the state's economic security, such as stealing critical private data, where the acting state believes the information will provide strategic economic advantages in sector it has interests at stake.[12]

While some legal scholars have discussed cyber operations that reside below the Article 2(4) prohibition of the use of force in the U.N. Charter, these scholars have generally not provided any extensive analysis of the non-intervention norm in relation to such cyber operations, leaving questions about the legality of such activities and the possibilities for countering these activities.[13] Because non-forcible economic influence merits more scholarly attention, this Article considers the norm of non-intervention in relation to non-forcible economic interference in other states through cyber means. This Article focuses on two concrete problems of concern: the transnational theft of trade secrets and the resulting economic leverage states apply for political purposes.

In 2013 an international group of experts published the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, a non-binding study examining the public international law

---

11 *See* Jeremy Yohe, *Cyber Attacks Post Threat to Title Companies*, TITLE, Mar. 2013, at 10, 12. In January and March of 2013, cyber attacks against Wells Fargo, J.P. Morgan Chase, Citigroup, U.S. Bancorp, PNC Financial Services, American Express, and Bank of America, disrupting their websites but causing no damage to customer information or the companies' computer networks. *Id.*; *see also* Choe Sang-Hun, *Computer Networks in South Korea Are Paralyzed in Cyberattacks*, N.Y. TIMES, Mar. 20, 2013, http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&_r=0; Nicole Perlroth & David Gelles, *Russian Hackers Amass Over a Billion Internet Passwords*, N.Y. TIMES, Aug. 5, 2014, http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html.

12 *See* European Comm'n, High Representative of the European Union for Foreign Affairs & Sec. Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, at 3, JOIN (2013) 1 (final) (Feb. 7, 2013).

13 Schmitt, *Cyber Operations*, *supra* note 8 (discussing the legal responses to cyber operations that fall below the use of force level). Some legal scholars have begun addressing these lower level cyber operations. *See* Christine P. Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1167-70 (2014) (reviewing lower level cyber attacks on the United States); Sean Watts, *Low-intensity Cyber Operations and the Principle of Non-intervention*, BALTIC YB OF INT'L L. (forthcoming November 2014).

governing cyber warfare.[14] The experts confined their work to *lex lata*, specifically focusing on *jus ad bellum* (uses of force) and *jus in bello* (armed conflict).[15] Notably, the *Tallinn Manual* did not address the norm of non-intervention as it relates to cyber espionage and theft of intellectual property, issues below the Article 2(4) threshold, "because application of international law on uses of force and armed conflict plays little or no role in doing so."[16] Based on previous research done by this author and others, the author disagrees with this position to the extent that respect for the principle of the sovereignty of states, encompassing the norm of non-intervention, "closely allies to legal rules that prohibit the use of force and interstate intervention."[17] The premise of this Article is that the examination of the norm of non-intervention, through its relationship with laws related to the use of force and armed conflict, is critically important to develop a clear context of the norm of non-intervention, providing an international legal framework for addressing the recent violations of international law by states conducting economic espionage.

As scholars assessed previously, and the *Tallinn Manual* correctly anticipated, states have come to understand that international law applies in cyberspace.[18] This Article addresses international law related to the norm of non-intervention as part of this larger body of public international law in order to examine how states can legally respond to the theft of intellectual property through cyberspace, making the case for closer examination of the principles of non-intervention and countermeasures in relation to

---

14 TALLINN MANUAL, *supra* note 6, at 9-11.

15 *Id.* at 5.

16 *Id.* at 4. Just as the Manual touched upon the principle of sovereignty, so too should the Manual have addressed the principle of intervention as it is directly related to the sovereignty of a state as well as the prohibition to use force against another state.

17 Joyner & Lotrionte, *supra* note 8, at 847.

18 U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 7-8, U.N. Doc. A/68/98 (June 24, 2013) ("State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory . . . . States must meet their international obligations regarding internationally wrongful acts attributable to them."). The U.N. Group of Governmental Experts ("UNGGE"), which includes representatives from Russia, China and the U.S., agreed in 2013 that international law applies in cyberspace. *Id.*

cyber economic espionage.[19] It examines the legal issues related to a state's obligations to comply with the norm of non-intervention, and under what circumstances a state may use countermeasures to induce a state to desist in, or refrain from, conducting cyber economic espionage.

This Article utilizes China's conduct of economic espionage against American companies as a case study, identifying relevant international law at issue in countering the theft of intellectual property, including both the legal obligations of a nation and the companies' rights at stake, as well as the options for peaceful dispute settlements, countermeasures, and the dispute settlement mechanism set up by the World Trade Organization ("WTO"). Today, the U.S. has an opportunity to take a pioneering role in seeking to hold states accountable for state-sponsored economic espionage, and to develop a minimum public order in the global economic community.

The first section of Part II of this Article considers the extent of the economic espionage problem, reviewing China's conduct as well as broader state practices. The second section discusses the traditional dimensions of political, military espionage, or intelligence collection that involve the gathering of information through "various surreptitious, intrusive means inside a foreign nation's territory without that nation's knowledge or consent."[20] It then compares such intelligence activities with state practice of economic espionage. The final section of this part reviews how both domestic and international law has, or has not, addressed each category of espionage, arguing that cyber economic espionage, unlike traditional espionage, implicates established international legal norms, and destabilizes economic relations.

Part III contends that there is a legally binding norm of non-intervention that reaches the kind of non-forcible economic

---

19 In discussions with the managing editor of the *Tallinn Manual*, Michael Schmitt, this author was informed that there is a project ongoing, *Tallinn 2.0*, which will "be working beyond the confines of intervention and countermeasures (State responsibility), although those will be key topics . . . . The focus will be State activities, both in terms of actions States may take, as well as responses by States to non-State and State activities." It is the author's opinion that given the state of economic espionage activities, the authors of *Tallinn 2.0* may likely have to address this topic. Email from Michael N. Schmitt to author on August 21, 2014 (on file with author).

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

influence that economic espionage represents. Currently this norm is poorly understood by decision-makers and academics. This Part argues that a reformulation of the norm is needed to incorporate and explicitly recognize the categories of economic intervention that the international legal system assesses as unacceptable. The majority of the Part examines the development of the norm of non-intervention under international law, addressing how it implicates economic acts, concluding that economic espionage, as a form of coercive intervention, is illegal under customary international law, even if traditional espionage is not.

The final part, Part IV, suggests methods for enforcing the rights of victim states against economic espionage. It reviews the history and development of countermeasures under international law, examining how and when a state may employ countermeasures in response to cyber economic espionage. This Part also assesses the viability of establishing an institutional mechanism for enforcing the economic rights of a victim state through the use of the WTO dispute settlement regime. While there are a number of challenges to this legal approach, and further research on the topic would be helpful, this Article examines how member states potentially could assert claims under the WTO's Dispute Settlement Understanding (DSU) against any WTO member that engages in or sponsors cyber economic espionage.[21]

The Article concludes that a state's use of countermeasures under international law in response to economic espionage that falls below the thresholds of "use of force" and "armed attack" may prove an effective option for states facing significant economic loses from cyber economic espionage. It maintains that such countermeasures in response to violations of the norm of non-intervention, coupled with the WTO's role in upholding fair business practices in international trade relations, may enhance international stability and economic development. While not without limitations and challenges, these international legal options provide the international community with the opportunity to achieve greater public order and harmony in international trade and minimize the potential for the escalation of the conflict between states over economic espionage. Although it is uncertain whether states will choose to resolve the present gaps in international law related to economic espionage, this Article hopes

---

21 *But see* Skinner, *supra* note 13, at 1172.

to contribute a useful awareness for the further development of the law in this area, providing more clarity for possible future decision making by state leaders.

Whether the principles of non-intervention and countermeasures or some broader principle of international trade law will be up to the challenge of regulating the increasingly destructive and coercive means of economic intervention in the cyber domain remains to be seen. Certainly, we know that what is at stake is the progress that has been made since the Cold War period and beyond: a global network of security and economic partnership fostering a system of open world trade that fueled productivity and prosperity and was at the cutting edge of almost all of the technological revolutions of the period.

II. The Problem of Economic Espionage

A. The Threat from Economic Espionage

According to *The IP Commission Report*, "[t]he scale of international theft of American intellectual property (IP) is unprecedented – hundreds of billions of dollars per year . . . ."[22] In 2012, the head of the U.S. National Security Agency and U.S. Cyber Command, General Keith Alexander, estimated that American companies have lost $250 billion in stolen information and another $114 billion in related expenses.[23] Moreover, in

---

22 DENNIS C. BLAIR & JON M. HUNTSMAN, JR., THE IP COMMISSION REPORT: THE REPORT OF THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY 11 (2013) [hereinafter THE IP COMMISSION REPORT] (finding that the impact of international IP theft on the U.S. economy exceeds $320 billion annually); *see also* Dennis Blair & Jon Huntsman, Jr., Op-Ed., *Protect U.S. Intellectual Property Rights*, WASH. POST, May 21, 2013, http://www.washingtonpost.com/opinions/dennis-blair-and-jon-hunts%E2%80%A6rights/2013/05/21/b002e10e-c185-11e2-8bd8-2788030e6b44_story.html. Estimates of the costs from economic espionage range from hundreds of billions to $1 trillion. Ellen Nakashima & Andrea Peterson, *Cybercrime and Espionage Costs $445 Billion Annually*, WASH. POST, June 9, 2014, http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/09/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html.

23 Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History,"* FOREIGN POL'Y, July 9, 2012, *available at* http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history; *see also* THE WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 2 (2009) ("[I]ndustry estimates of losses from intellectual property [IP] to data theft in 2008 range as high as $1 trillion.").

March 2013, in an unprecedented break from diplomatic niceties, President Obama's national security advisor, Thomas Donilon, publicly called out the Chinese government for the "cyber-enabled theft" of confidential American proprietary information.[24]

Such cases of state-sponsored cyber economic espionage target companies' business strategies and plans, intellectual property, and expensive research and development projects, eroding their competitive economic advantage in the international market place and placing the acquirer an unfair leap ahead on technological developments.[25] Although the theft of intellectual property ("IP") is not a new phenomenon,[26] the scale of IP theft has increased

---

24 Tom Donilon, Nat'l Sec. Advisor, Remarks at The Asia Society: The United States and the Asia-Pacific in 2013 (Mar. 11, 2013) ("Increasingly, U.S. businesses are speaking out about their serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale . . . . [S]pecifically with respect to the issue of cyber-enabled theft, we seek three things from the Chinese side. First, we need a recognition of the urgency and scope of this problem and the risk it poses – to international trade, to the reputation of Chinese industry and to our overall relations. Second, Beijing should take serious steps to investigate and put a stop to these activities. Finally, we need China to engage with us in a constructive direct dialogue to establish acceptable norms of behavior in cyberspace.").

25 CTR. FOR STRATEGIC & INT'L STUDIES, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE 6 (2013). Economic espionage is also referred to at times as "industrial espionage," which, according to the Department of Justice, is defined "as activity conducted by a foreign . . . government or by a foreign company with the direct assistance of a foreign government against a private United States company for the sole purpose of acquiring commercial secretes." Defense Production Act of 1950, 50 U.S.C. app. § 2170b(e) (2012). Industrial espionage includes a corporation's use of illegal techniques to collect information, such as trade secrets, not voluntarily provided by the source. *See* BENJAMIN GILAD & TAMAR GILAD, *The Business Intelligence System: A New Tool for Competitive Advantage* 209 (AMACOM 1988). For the purposes of this paper the term "economic espionage" is used to describe state-sponsored "industrial espionage."

26 *See* U.S. GEN. ACCOUNTING OFFICE, DEFENSE INDUSTRIAL SECURITY: WEAKNESSES IN U.S. SECURITY ARRANGEMENTS WITH FOREIGN-OWNED DEFENSE CONTRACTORS 2 (1996). The General Accounting Office also reported on the economic espionage activities of countries regarded as allies of the U.S. and listed five countries engaged in direct attempts to steal or bribe away America's technology. *Id.* at 22-26. A 1996 declassified CIA report listed countries that were extensively engaged in economic espionage against the U.S., including France, Israel, China, Russia, Iran, and Cuba. *Current and Projected Nat'l Security Threats to the U.S. and its Interests Abroad: Hearing Before the S. Select Comm. on Intelligence*, 104th Cong. 99 (1996). On Soviet acquisition programs seeking to steal U.S. technology, *see* Katherine A. S. Sibley, *Soviet Industrial Espionage Against American Military Technology and the U.S. Response, 1930-1945*, 14 INTELLIGENCE & NAT'L SECURITY 94, 95-96 (1999), and CENT.

dramatically.[27] Indeed, over the last two decades the Internet became a new tool for the trade of intelligence and a very effective method to conduct economic espionage.[28] Today, according to the Defense Security Service, these attacks on American companies are accelerating, increasing by seventy-five percent between 2011 and 2012.[29] Chinese actors appear to be a significant source of this activity, causing "material" damage to U.S. economic prosperity in recent years.[30] China has attacked sectors of the U.S. economy

---

INTELLIGENCE AGENCY, SOVIET ACQUISITION OF MILITARY SIGNIFICANT WESTERN TECHNOLOGY: AN UPDATE 1 (1985). For a brief account of the Soviet program of the 1970s and the U.S. and allied response, *see* Gus W. Weiss, *The Farewell Dossier*, 39 STUDIES IN INTELLIGENCE, no. 5, 1996. Russia appears to have acknowledged its efforts to collect industrial and trade secrets from other countries. *See* ABRAM N. SHULSKY & GARY J. SCHMITT, SILENT WARFARE: UNDERSTANDING THE WORLD OF INTELLIGENCE 179 (3d ed. 2002).

[27] An FBI study found that of 173 countries, 100 were spending resources to acquire U.S. technology. Peter Schweizer, *The Growth of Economic Espionage: America Is Target Number One*, FOREIGN AFF. (Jan.-Feb. 1996), http://www.foreignaffairs.com/articles/51617/peter-schweizer/the-growth-of-economic-espionage-america-is-target-number-one. Fifty-seven of those countries were engaging in covert operations against U.S. corporations. *Id.*

[28] THE IP COMMISSION REPORT, *supra* note 22, at 18 ("While traditional industrial espionage techniques have been used extensively, cyber methods for stealing IP have become especially pernicious."). The theft of data from computers had been recognized as a concern from the 1960s. *See The Computer and Invasion of Privacy: Hearings Before a Subcomm. of the H. Comm. on Gov't Operations*, 89th Cong. 1 (1966). At Senate hearings designed to formulate new laws to help combat economic espionage, FBI Director Louis Freeh bemoaned the fact that he had so few tools to deal with the data thieves and spies, stating: "We have approximately 800 pending cases involving 23 foreign countries. These are state-sponsored economic espionage – forays and initiatives into the United States, using all the various techniques of intelligence officers, from compromising individuals to unlawful wiretapping, to bribery . . . ." *See Economic Espionage: Hearing Before the S. Selected Comm. on Intelligence and the Subcomm. on Terrorism, Tech., & Gov't Info. of the Comm. on the Judiciary*, 104th Cong. 64 (1996) (statement of Louis Freeh, FBI Dir. of the United States). According to one study, the following countries were extensively engaged in espionage activities against U.S. companies: France, Israel, Russia, China, Iran, Cuba, the Netherlands, Belgium, Germany, Japan, Canada, India and several Scandinavian countries. *See* Thomas J. Jackamo, III, *From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary International Law of Non-Intervention*, 32 VA. J. INT'L L. 929, 944 (1991-92) (citing Bill Gertz, *The New Spy: '90s Espionage Turns Economic*, WASH. TIMES, Feb. 9, 1992).

[29] Tyler Armerding, *Costly Cyberespionage on "Relentless Upward Trend"*, CSO ONLINE (Dec. 18, 2012, 7:00 AM), http://www.csoonline.com/article/2132248/data-protection/costly-cyberespionage-on--relentless-upward-trend-.html.

[30] THE IP COMMISSION REPORT, *supra* note 22, at 12 ("For almost all categories of IP theft, currently available evidence and studies suggest that between 50% and 80% of

and agencies critical to U.S. national security, penetrating the online systems of the U.S. Departments of Homeland Security and State and stealing critical data of companies, including RSA, Coca-Cola, Lockheed Martin, Dow Chemical, Adobe, Yahoo, and Google, to name just a few of the victims.[31] Such activities have resulted in the "greatest transfer of wealth in history."[32]

In the past, cyber intrusions for purposes of stealing intellectual property seemed to provoke little response from the U.S. government.[33] Most of the focus from U.S. defense and intelligence officials and academics has been on the prospect of a "Cyber Pearl Harbor" or a "Cyber 9-11."[34] Warning of cyber attacks have invoked images of massive, sustained power outages

---

the problem, both globally and in the United States, can be traced back to China . . . . Quantitatively . . . China stands out in regard to attacks for IP."). In its most recent 2013 report, the U.S. Trade Representative notes a grave concern with cyber-enabled trade-secret theft from China. *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2013 SPECIAL 301 REPORT 13 (2013); *see also* MANDIANT, EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 20 (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. The Mandiant report linked Unit 61398 of the PLA to a global cyber espionage campaign against nearly 150 companies from 20 economic sectors "designed to steal large volumes of valuable intellectual property." *Id.* at 3.

31 *See* Ellen Nakashima, *In a World of Cybertheft, U.S. Names China, Russia as Main Culprits*, WASH. POST, Nov. 3, 2011, http://www.washingtonpost.com/world/national-security/us-cyber-espionage-report-names-china-and-russia-as-main-culprits/2011/11/02/gIQAF5fRiM_story.html. General Keith Alexander had stated that one U.S company alone had lost $1 billion worth of intellectual property over the course of a couple of days. *Id.*

32 Keith B. Alexander, Nat'l Sec. Agency, Keynote Address at AEI Event: Cybersecurity and American Power (July 9, 2012); *see also* David E. Sanger & Mark Landler, *U.S. and China Agree to Hold Regular Talks on Hacking*, N.Y. TIMES, June 1, 2013, http://www.nytimes.com/2013/06/02/world/asia/us-and-china-to-hold-talks-on-hacking.html. The U.S. International Trade Commission estimated that in 2009, Chinese theft or infringement of U.S. intellectual property cost almost one million U.S. jobs and caused $48.2 billion in U.S. economic losses due to lost sales, royalties, or license fees. Of the $48.2 billion, about $36.6 billion was attributable to lost sales, the remaining $11.6 billion was the combination of lost royalty and license payments. *See* THE IP COMMISSION REPORT, *supra* note 22, at 25.

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

34 *See* Leon Panetta, Sec'y of Def., Dep't of Def., Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012). Former U.S. Secretary of Defense, Leon Panetta has warned that adversaries could use cyber tools to gain control of critical industrial control systems and launch attacks on critical U.S. infrastructure, producing widespread destruction equivalent to a "cyber-Pearl Harbor." *Id.*

across the country, breaking pipes and disabling ATM machine and air traffic control systems. Although it is important for defense planners to prepare for such scenarios, a massive cyber attack has not occurred since the U.S. began to rely on networks to support important national activities.[35] Current evidence indicates that actual damage resulting from cyber operations are more equivalent to attacks that fall below the traditional threshold of armed attacks under international law.[36] Instead of buildings falling and people dying, the cyber attacks are slow, methodical, and stealthy, targeting business secrets. Persistent intrusions and hacking, sometimes ratcheting up to low-end but nonetheless damaging attacks such as those on Estonia in 2007, currently dominate the cyber realm.

Most recently, in departure with past practice, the issue of Chinese cyber economic espionage and its damage to U.S. economic competitiveness has become a top priority for U.S. policy-makers.[37] On May 19, 2014, the Department of Justice announced the indictment of five members of the People's Liberation Army of China for computer hacking, economic espionage, and other offences, targeting six U.S. companies in the nuclear power, metals, and solar products industries.[38] The

---

35 *See* Martin Libicki, *Don't Buy the Cyber Hype*, *FOREIGN AFFAIRS* August 14, 2013.

36 Evan F. Kohlmann & Rodrigo Bijou, *Planning Responses and Defining Attacks in Cyberspace*, 126 HARV. L. REV. F. 173, 174 (2013) ("[T]he federal government must establish policies that firmly signal a commitment to protect American businesses and warn hostile actors that they cannot inflict critical damage on the U.S. economy without consequences.").

37 Sanger, Barboza & Perlroth, *supra* note 33 ("Obama administration officials say they are planning to tell China's new leaders . . . that the volume and sophistication of the attacks have become so intense that they threaten the fundamental relationship between Washington and Beijing."); *see also* Mike Rogers, Chairman, House Permanent Select Comm. on Intelligence, Opening Statement at the Open Hearing: Cyber Threats and Ongoing Efforts to Protect the Nation (Oct. 4, 2011), http://intelligence.house.gov /sites/intelligence.house.gov/files/documents/100411CyberHearingRogers.pdf ("China's economic espionage has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy.").

38 Press Release, Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014). At the time of the indictment, FBI Director James B. Comey noted: "For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries." *Id.*

indictment was the first-ever cyber economic espionage criminal case between two nations, indicating that the U.S. government has escalated its efforts against the Chinese government's cyber espionage after previous diplomatic attempts failed to deter China's activities.[39] China denounced the indictment, denying the charges[40] and citing recent revelations by Edward Snowden to support the argument that the U.S. engages in its own cyber espionage, including collecting intelligence related to trade negotiations.[41]

These recent U.S. diplomatic and criminal efforts to curb Chinese cyber economic espionage have been part of a broader strategy to hold China accountable for a growing campaign of commercial cyberspying. Notably, six of the seven criminal cases brought under the Economic Espionage Act of 1996 in 2010 involved some link to China, although none of these cases targeted Chinese government officials.[42] Skeptics, however, citing the lack of any visible progress in abating the scale of the threat from China, raise doubts about how effective these U.S. actions have been.[43] Prospects of effectively curbing Chinese economic espionage seem grim: the 2013 U.S.-China working group on cybersecurity was suspended following the announcement of the indictments, and there is a little likelihood that the U.S. will get custody of the PLA officers, limiting any deterrent effect by

---

39 Ellen Nakashima, *Indictment of PLA Hackers is Part of Broad U.S. Strategy to Curb Chinese Cyberspying*, WASH. POST, May 22, 2014, http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html.

40 Timothy M. Phelps & Julie Makinen, *China Blasts "Absurd" U.S. Charges of Cyberespionage*, L.A. TIMES, May 19, 2014, http://www.latimes.com/nation/nationnow/la-na-nn-china-cyber-spying-20140519-story.html.

41 Michael Riley, *Snowden's Leaks Cloud U.S. Plan to Curb Chinese Hacking*, BLOOMBERG NEWS, June 30, 2013, http://www.bloomberg.com/news/print/2013-07-01/snowden-s-leaks-cloud-u-s-plan-to-curb-chinese-hacking.html.

42 OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 5 (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

43 *See* Lolita C. Baldor, *Chinese Cyber Attacks on U.S. Continue Totally Unabated, Leon Panetta Complains*, HUFFINGTON POST, Sept. 20, 2012, http://www.huffingtonpost.com/2012/09/20/chinese-cyber-attacks-leon-panetta_n_1899168.html. Richard Bejtlich, president of Mandiant, described the issue, stating, "[t]he Chinese don't seem to care. So I don't have any hope that the dialogue is reaching anyone of note." *Id.*

possible prosecutions.[44] Even after the criminal indictments, the Chinese government continues to conduct economic espionage against U.S. companies.[45]

Thus, this Article examines other options under existing international law that the U.S. government could consider in the face of the Chinese actions. In adopting a policy decision based on international law, the U.S. would reinforce the legitimacy of its actions and increase the likelihood of international support, showing the U.S.' commitment to the rule of law, thereby reducing the appeal of economic espionage.[46]

Some commentators, recognizing the significant impact on trade relations from economic espionage, have proposed that the U.S. government bring trade sanctions against China,[47] while others have recommended the WTO as a forum to address economic cyber espionage.[48] Some have raised doubts about the

---

44 *See* Jack Goldsmith, *The USG Strategy to Confront Chinese Cyber Exploitation, and the Chinese Perspective*, LAWFAREBLOG.COM (Feb. 21, 2013, 1:17 PM), http://www.lawfareblog.com/2013/02/the-usg-strategy-to-confront-chinese-cyber-exploitation-and-the-chinese-perspective/.

45 *See* Nicole Perlroth, *2nd China Army Unit Implicated in Online Spying*, N.Y. TIMES, June 9, 2014, http://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html (linking the theft of design schematics for satellite and aerospace technology from U.S. companies to another military unit of the PLA, Unit 61486).

46 *See* COUNCIL ON FOREIGN RELATIONS, U.S. TRADE AND INVESTMENT POLICY 50 (Report no. 67 2011), http://i.cfr.org/content/publications/attachments/Trade_TFR67.pdf. Traditionally, in order to resolve trade disputes, most developed countries rely on tools such as unilateral trade sanctions and trade remedies such as countervailing duties and voluntary export restraints. *Id.* There are already indications of retaliation and counter-retaliation in the trade sector based on the Chinese espionage and the U.S indictment. The Chinese announced retaliatory measures that include new inspection procedures for U.S. technologies. Perlroth, *supra* note 45. SolarWorld, one of the victims named in the U.S. indictment has announced that the Chinese hacking was retaliation for it bringing, and winning, on a trade complaint of unfair business practices against China in the first instance. *See* Shane Harris, *U.S. Manufacturer Wants Commerce Dept. to Penalize China for Cyberattack*, FOREIGN POL'Y, July 1, 2014, http://complex.foreignpolicy.com/posts/2014/07/01/us_manufacturer_wants_commerce_dept_to_penalize_china_for_cyberattack_0. The U.S. is considering imposing high tariffs and import duties against Chinese solar goods, effectively blocking them from the U.S. market. *Id.*

47 Diane Cardwell, *Solar Company Seeks Stiff U.S. Tariffs to Deter Chinese Spying*, N.Y. TIMES, Sept. 1, 2014, http://www.nytimes.com/2014/09/02/business/trade-duties-urged-as-new-deterrent-against-cybertheft.html.

48 Richard A. Clarke, Op-Ed., *A Global Cyber-Crisis in Waiting*, WASH. POST, Feb. 7, 2013, http://www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html ("[V]ictims of Chinese

efficacy of the WTO mechanism to address cyber espionage issues;[49] moreover, the WTO has shown little interest in addressing the issue to date.[50]

The use of countermeasures, as discussed in this Article, may serve two functions: to reduce state incentives to conduct economic espionage and minimize the likelihood that victim states will resort to the destabilizing characterization of economic espionage as an armed attack, potentially escalating the conflict.[51] The use of countermeasures can provide states with a legal basis for effective responses to economic espionage, buying time for the potential establishment of international consensus to prohibit cyber methods of IP theft for competitive advantage through a new treaty, state practice, or new interpretations of WTO agreements as applicable to economic espionage.[52]

Certainly, such countermeasures would be unnecessary if we lived in a world of a centralized government with command and control that subjected legal disputes to general and effective international adjudication.[53] Of course, we do not exist in such a world under general international law today. The question

---

economic espionage should seek to establish clear guidelines and penalties within the World Trade Organization system."); *see also* JAMES A. LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, CONFLICT AND NEGOTIATION IN CYBERSPACE 49-51 (2013) (suggesting that the U.S. should pursue cyber espionage and intellectual property theft claims against China in the WTO). To date, the U.S. has only brought one case to the WTO under TRIPS against China but it did not pertain to espionage. *See China-Measures Affecting the Protection and Enforcement of Intellectual Property Rights*, WORLD TRADE ORG., www.wto.org/english/tratop_e/dispu_e/cases_e/ds362_e.htm (last visited Oct. 4, 2014).

49 *See* David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies*, 17 AM. SOC'Y INT'L L. 2 (2013). Fidler argued that cyber espionage conducted outside the territory of the WTO member is not covered by the WTO Agreements and therefore would not be appropriate for WTO review. *The IP Commission Report* highlighted the fact that the WTO dispute mechanisms take too long, making the recapture of damages improbable. THE IP COMMISSION REPORT, *supra* note 22, at 19.

50 Fidler, *supra* note 49, at 3.

51 Lewis, *supra* note 48, at 49 ("Even a credible hint that the United States is considering [going to the WTO] would have an immediate effect on Chinese decision making."). Jim Lewis at CSIS has noted that even the threat of a claim by the U.S against China at the WTO could go far in deterring its conduct. *Id.*

52 *See* WILLIAM A. OWENS ET AL., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 250 (2009).

53 *See e.g.* G.A. Res. 56/83, ¶ 2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83, art. 50(2)(a) (Jan, 28, 2002) [hereinafter ARSIWA].

remains, however, whether such a situation currently exists under a "specialized" area of the law under the WTO. Is it possible that arbitral panels can be informed by the principles of general international law such as the norm of non-intervention along with the specialized rules of the trade regime to compel states to comply with their international obligations while providing the needed reparations to those states injured by the wrongful actions of other states through acts of economic espionage? Before examining the appropriate legal responses to economic espionage, as an initial matter, one must assess the wrongfulness of economic espionage under international law. In doing so, the next section investigates the distinction between traditional espionage and economic espionage according to state practice.

B. Distinguishing Political/Military Espionage From Economic Espionage

"[V]irtually every nation has some type of intelligence service – if not both civilian and military," at least the latter.[54] With over a hundred established and acknowledged intelligence services responsible for espionage activities across the globe, each nation practices intelligence in ways that are specific to that nation's legal and governmental bureaucratic framework.[55] There is no uniform

---

[54] MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 313 (4th ed. 2009).

[55] *Id.* at 11 (providing a detailed review of the intelligence services of Britain, China, France, Israel, and Russia as well as a less detailed but useful assessment of the intelligence services of Australia, Canada, Germany, New Zealand, Pakistan, South Korea and Japan); *see also* Johnson, *supra* note 5, at 18 (highlighting Namibia as an example of a lesser-developed nation that has practiced espionage). After the Cold War, more information became publicly available about different countries' intelligence services. Previously, although governments knew other countries had intelligence services, little was discussed publicly, leaving minimal publicly available information for scholars and non-governmental experts to analyze. Even a relatively transparent government like the UK, with a long existing intelligence service, did not officially acknowledge the existence of its internal and external intelligence services, MI5 and MI6, until 1993. Even lesser-developed nations conduct intelligence collection. *Id. See generally* SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE (2011) (examining the political and legal status of Britain and the U.S.' intelligence services); PHILIP H. J. DAVIES & KRISTIAN C. GUSTAFSON, INTELLIGENCE ELSEWHERE: SPIES AND ESPIONAGE OUTSIDE THE ANGLOSPHERE (2013) (examining the historical and cultural origins of intelligence in several countries including India, China, Pakistan, India, Iran, Japan, Indonesia, Ghana, Argentina, Sweden, Argentina and Russia); STUART FARSON ET AL., PSI HANDBOOK OF GLOBAL SECURITY AND INTELLIGENCE VOLS. (2008) (examining a

approach of intelligence services across countries, since intelligence organizations are "unique expressions of [a nation's] history, needs, and preferred governmental structures."[56] Fundamentally, however, all intelligence services exist for the same reason: "to hide some information from other governments, who, in turn, seek to discover hidden information . . . ."[57] In other words, the general purpose of espionage is to obtain "clandestinely information in regard to military or political secrets" to protect the national security of the nation.[58] Espionage is one aspect of a nation's intelligence work, encompassing the government's efforts to acquire classified or otherwise protected information in order to deal with threats from actual or potential adversaries.[59] That information can come from a foreign government, enemy or ally,[60] as well as a foreign entity, such as foreign corporations. And while just about all nations conduct such espionage, they all maintain the right to prosecute those they catch spying within their territory under their domestic criminal laws.[61]

Under the traditional practice of states, if a foreign official sent to a country under official cover, holding an official government job, is compromised violating domestic laws by spying, the officer will have diplomatic status and will be immune from prosecution.[62] Typically, the officer will be declared *persona non*

---

wide range and variety of national intelligence systems within other countries including seven countries from the Americas, eight from Asia and Australasia, ten from Europe including Russia, five from the Middle East and one from Africa) [hereinafter PSI HANDBOOK].

56 LOWENTHAL, *supra* note 54.

57 *Id.* at 1.

58 L. OPPENHEIM, INTERNATIONAL LAW: A TREATISE § 455 (Ronald F. Roxburgh ed., 3d ed. 1920).

59 The term "adversary" is broad in the sense that it encompasses both enemies and allies. For example, a friendly government with which one is negotiating a treaty may be an adversary in the context of the negotiation; at a minimum the sides are competing for maximum benefit from the agreement.

60 It is accepted practice that under certain circumstances allies will feel it necessary to collect intelligence from within the territory of an ally. Diplomacy and realpolitik have a bottom line that dictates that nobody can be trusted, no matter how close the alliance.

61 W. Hays Parks, *The International Law of Intelligence Collection*, *in* NATIONAL SECURITY LAW 433, 433-34 ((John Norton Moore & Robert F. Turner eds., 1990).

62 Vienna Convention on Diplomatic Relations, April 18, 1961, Art. 31.

grata ("PNG") and expelled from the country.[63] For example, during the Cold War, rough "rules of the road" for spying were developed between the U.S. and Soviets. When one side crossed a red line established by those rules there typically followed reciprocal expulsions of intelligence officers and reductions in diplomatic missions. This process was a mechanism for regulating the friction created by espionage.

Although expulsions are embarrassing and cause diplomatic tension, it is rare for the expelling state to claim that these activities themselves violate international law even while saying such acts are inconsistent with diplomatic activities.[64] Those with no official cover and no diplomatic immunity can be arrested and prosecuted under domestic criminal laws; however, in many of these cases, these individuals are exchanged for similarly-situated agents detained in the offender's state.[65] As one commentator

---

63 William Drozdiak, *French Resent U.S. Coups in New Espionage*, WASH. POST, Feb. 26, 1995, at A1. In 1995, in one particularly embarrassing incident for the U.S., a number of CIA officers were PNG-ed from Paris when it was discovered that they were conducting an operation that involved recruiting French officials to gather information about France's position on sensitive trade and technology negotiations involving the entertainment industry. The French government had been trying to restrict the number of U.S.-made films shown in France and given the importance of such exports to the U.S. economy, the CIA was gathering intelligence in order to inform US policymakers about how the French were going to play their hand. The CIA was also caught bribing a senior member of France's Ministry of Communications, in order to get details about the French negotiating position at GATT talks on telecommunications. *Id.*; s*ee also* RICHARD HOLM, THE AMERICAN AGENT (narrating a former CIA chief officer stationed in Paris who was PNG-ed because the U.S. operational compromise details how he was told by the U.S. Ambassador that France's Minister of Interior had asked that a number of CIA officers to quietly leave the country. Only after the media reported the incident did France PNG the individuals); NIGEL WEST, SEVEN SPIES WHO CHANGED THE WORLD 172-73 (1991) (discussing how the U.S. Department of Justice in the 1960s arranged for a number of KGB officials operating under UN cover in NY to leave the U.S. and return to Moscow without being tried).

64 S*ee* Jeffrey H. Smith, *Keynote Address*, 28 MICH. J. INT'L L. 543, 544 (2007) (Discussing the legitimacy of espionage under customary international law, and stating "I can recall no instance in which a receiving state has said that these activities violate international law.").

65 WEST, *supra* note 63, at 154-77. On February 10, 1962, Colonel Rudolph Abel, a KGB officer who had been convicted and sentenced to thirty years for spying within the U.S., was exchanged by the U.S. for the American U-2 pilot Gary Powers who had crashed in the Soviet Union in May 1960 on a reconnaissance mission to collect information on the locations of Soviet Union's ICBMs. *Id. See also*, LEON PANETTA WITH JIM NEWTON, WORTHY FIGHTS 281-84 (2014). The July 2010 arrest of ten deep-cover Russian spies, 'illegals" or sleeper agents, who had been operating in the U.S for at

observed regarding state practice and understanding of espionage during the Cold War: "[t]he principle implicitly recognized by Premier Kruschev and Presidents Eisenhower and John F. Kennedy was that espionage is an organic branch of foreign relations and foreign policy, similar to diplomatic exchanges and summit conferences."[66]

By the 1960s computers began to play a role in the business of intelligence.[67] Since at least the 1980s, the U.S. government, specifically the National Security Agency ("NSA"), indicated that it was concerned about the vulnerability that computers posed to the protection of the information they held, having significant implications for sensitive government data stored in them as well as industry information.[68] Indeed, evidence exists that nations have been utilizing their intelligence and military agencies to conduct espionage through cyberspace, or computer network exploitation,[69] for decades.[70] Making use of the cyber domain in

---

least a decade. Mikhail Fradkov, the head of the Russian intelligence service, SVR, acknowledged that the ten spies captured were his spies and agreed to a swap the spies for four Russians jailed in Russia for alleging spying for the U.S. or Britain. *Id.*

66 SANCHEZ DE GRAMONT, THE SECRET WAR (1962).

67 Michael Warner, *Cybersecurity: A Pre-History*, 27 INTELLIGENCE & NAT'L SEC. 781, 782 (2012).

68 *Id.* (arguing that "the 'cyber' issue is not new at all, but rather has taken a half-century to develop"). *See generally* Nat'l Sec. Agency, *Computer Virus Infections: Is NSA Vulnerable?*, 4 CRYPTOLOGIC QUARTERLY 47 (1985), https://www.nsa.gov/public_info/declass/cryptologic_quarterly.shtml (follow "Computer Virus Infections: Is NSA Vulnerable?" hyperlink) (warning about the dangers that viruses pose to computer networks).

69 WILLIAM A. OWENS ET AL., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 70 (2009). *See also* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63, 63 (2010) (defining cyber exploitation as "the use of actions and operations – perhaps over an extended period of time – to obtain information that would otherwise be kept confidential and is resident on or transmitting through an adversary's computer systems or networks"); THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT 354 (2000) (discussing the complications involved in determining the legality of cyber exploitation operations from cyber attack operations). "The technology of computers and the Internet allows a lawful act of espionage to morph into an unlawful use of force at the speed of light." *Id.*; *see* Lewis, *supra* note 48, at 20 (estimating that forty countries have or are acquiring cyber weapons for combat); s*ee also* William J. Lynn, III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFF. (Sept.-Oct. 2010), http://www.foreignaffairs.com/print/66687 (stating that more than 100 foreign intelligence organizations try to hack U.S. networks); North Atlantic Treaty Organization (NATO) Standardization Agency, *NATO Glossary of Terms and Definitions* (AAP-6 of

this manner has many advantages, allowing the state to conduct collection remotely, not requiring proximity for access, and eliminating the need to recruit a human asset to acquire access, thereby lowering the costs, increasing the volume of information taken, and minimizing the chances of being detected and the political and diplomatic ramifications that would follow.[71]

Since the emergence of some states' practice of economic espionage, U.S. officials have consistently drawn a line between spying for national security or foreign intelligence purposes and spying on companies to give a competitive advantage to one's own businesses.[72] For U.S. practice, the former may include economic intelligence conducted against foreign nations and foreign entities, as well as intelligence conducted against sovereign owned enterprises, for the purpose of supporting U.S. national security, as opposed to supporting any private interests.[73] At times, economic intelligence can include publicly available information, typically

---

2013) 2-C-11; http://fas.org/irp/doddir/other/nato2008.pdf (defining computer network exploitation (CNE) as an "[a]ction taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage.").

70 Warner, *supra* note 67, at 784 (noting that "the world's first case of computer espionage" may have been in 1968 when West German authorities captured an East German spy working in a subsidiary the German subsidiary of IMB). Another early case of state-sponsored cyber espionage occurred in 1986 when a system administrator, Cliff Stoll, determined that West German hackers, hired by the KGB had broken into the computers of the Department of Defense and contractors. *Id.* at 788.

71 DEFENSE SCIENCE BOARD, *supra* note 2 (describing that advantages of "information warfare").

72 Intelligence refers to information relevant to a government's formulation and implementation of policy to further its national security interests and to deal with threats from actual or potential adversaries. In the most obvious case, this information has to do with an adversary's capabilities and plan for military action. Potential or actual enemies try to keep this type of information secret. Other types of secret information may be important as well, for example, information about the country's diplomatic activities or intentions as well as its intelligence activities. One aspect of intelligence activities, and the focus of this Article, involves the collection of this type of secret information. There are various methods used to collect this information. In short, intelligence espionage is a component of the struggle between adversaries that deals primarily with information. This Article focuses on intelligence information collection (espionage) done through the Internet.

73 *See* CIA's Public Affairs Staff, *A Consumer's Guide to Intelligence* (July 1999) (defining economic intelligence as "intelligence regarding foreign economic resources, activities and policies including the production, distribution, and consumption of goods and services, labor, finance, taxation, commerce, trade, and other aspects of the international economic system.").

not in the purview of intelligence agencies, such as national gross domestic product and inflation rate figures, as well as more privileged information, kept secret by many states and therefore the target of foreign intelligence services, such as budgetary allocations for defense, and national research and development expenditures.[74]

While economic intelligence about countries may be publicly available, some countries seek to keep such information secret. Under these circumstances, the work of the U.S. intelligence community, and its ability to collect secret information, would be useful to U.S. national security interests. For example, most economic data about the Soviet Union was kept secret, including the size of its gold reserves and the annual sales of gold on the world market.[75] Knowing whether a foreign government is planning on devaluing its currency or change its stance at trade talks would be economic intelligence that would be used for intelligence agencies to provide to U.S. policymakers. Economic intelligence can also be useful in notifying top government officials if bid competitions are being skewed in favor of a foreign country. In sum, economic intelligence, at times collected clandestinely, can help policymakers make critical decisions related to national security such as whether to raise the interest rates, what position to take in trade negotiations, in assessing the economic capability of a potential military adversary, or following the developments affecting the flow of vital strategic resources.[76] Such collection of economic intelligence has been an accepted function of intelligence agencies since at least World War I.[77]

---

[74] *Id.*

[75] *See* United States. Congress. Joint Economic Committee. THE FORMER SOVIET UNION IN TRANSITION, 399 (1993).

[76] COUNCIL ON FOREIGN RELATIONS, *Making Intelligence Smarter*, Report Prepared by an Independent Task Force appointed by the Council on Foreign Relations (Oct. 1, 1996) (describing economic intelligence involving questions such as trade policy, foreign exchange reserves, the availability of natural resources, and agricultural commodities).

[77] *See* Jeffrey T. Richelson, *A Century of Spies: Intelligence in the Twentieth Century*, OXFORD UNIVERSITY PRESS, 1995, at 426-428; Samuel Porteous, *Looking Out for Economic Interests: An Increased Role for Intelligence*, 19 WASHINGTON QUARTERLY, 191-203 (Fall 1996) (Canadian Security Intelligence Service intelligence analyst, Samuel Porteous, stating, "[p]roviding this type of information to economic policymakers and other government decision-makers is a generally acknowledged function of Western intelligence services."); William J. Clinton, *Statement on the Economic Espionage Act*, U.S. NEWSWIRE, Oct. 15, 1996 ("Economic intelligence will play an increasingly important role in helping policymakers understand economic trends.

The U.S. intelligence agencies conduct counterintelligence activities involving economic issues focused on areas such as trade negotiations, protection of American firms against penetrations by foreign intelligence agents, and uncovering bribes and corruption involving foreign businesses or officials that make it difficult for U.S. firms to compete in developing countries and elsewhere.[78] As U.S. officials have consistently maintained, U.S. intelligence agencies do not collect the trade secrets of foreign companies and provide those secrets to U.S. companies.[79] Since the indictment of the Chinese PLA members, U.S. officials have taken great pains to reiterate the distinction between spying on foreign officials and conducting economic intelligence, which they say is essential to protecting U.S. national security from governments spying on corporations for economic gain, which they consider forbidden.[80] States that fail to draw this difference have pointed out that the U.S. definition of spying for national security includes using national intelligence resources to secure advantages in trade negotiations and on other international economic issues.[81] These states see no difference between the two. But can we really draw

---

Economic intelligence can support U.S. trade negotiations and help level the economic playing field by identifying threats to U.S. companies from foreign intelligence services and unfair trading practices.").

78 Clinton, *supra* note 77. In early 1994 the CIA and NSA collected information that revealed that the French were using bribes in order to secure a contract with Saudi Arabia for military equipment and civilian airliners. The information related to the bribery that the CIA and NSA had collected allowed President Clinton to present the information to King Fahd of Saudi Arabia, ultimately resulting in the French losing the contract and the part of the award related to airliners went to Boeing and McDonnell Douglas. *See* Drozdiak, *supra* note 63.

79 Although the U.S. has imposed its own prohibitions on conducting economic espionage, other countries have alleged that the U.S. uses its intelligence collection to help U.S. corporations gain commercial advantages. *See* Duncan Campbell, *Interception Capabilities 2000,* Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment Programme Office) (the European Parliament charging the U.S. and its allies with using the "Echelon" collection system to help their corporations). The charges were rebutted by former DCI James Woosley in a press briefing stating that the targeting of foreign corporations were limited to sanctions enforcement, sale of material and products used in the production of weapons of mass destruction, and detention of bribery attempts by non-U.S. corporations in competition with American ones. FOREIGN PRESS CENTER BRIEFING, INTELLIGENCE GATHERING AND DEMOCRACIES: THE ISSUE OF ECONOMIC AND INDUSTRIAL ESPIONAGE (March 7, 2000).

80 *See* Nakashima, *supra* note 39.

81 *See* Campbell, *supra* note 79.

such a distinction in practice based on the purpose and impact of these activities?

Depending on the country that is conducting traditional espionage, its goals and objectives may vary.[82] The U.S., like most countries, conducts intelligence operations in foreign countries in order to know more about the internal military, political, economic, and social developments in those countries, information that would otherwise be impossible to know from open sources.[83] This information helps states make difficult political decisions by better informing their decision-makers with critical data.[84] For example, information regarding a state's preferences in international negotiations is typically difficult to acquire quickly through conventional sources, especially since such preferences could be in constant flux during the negotiations.[85] Intelligence sources and methods may therefore provide the best chances of accounting for real-time information shifts under such circumstances.

As distinguished from economic intelligence, there is economic espionage or the use of intelligence assets to collect valuable business data from foreign companies, providing such information to the collecting state's own private entities to gain economic advantages. Among intelligence services, the issue of economic espionage has been treated differently over the years depending on the country and the degree of involvement a government has in a nation's industrial base. In the former Soviet Union, the needs of the nation were the same as the needs of industry, and there was no distinction between the government and the different branches of the economic system. So, if the KGB gathered intelligence on a planned defense buy with some details

---

82 *See* Parks, *supra* note 61 at 433-34 ("Nations collect intelligence to deter or minimize the likelihood of surprise attack, to facilitate diplomatic, economic, and military action, in defense of a nation in the event of hostilities, and in times of 'neither peace nor war,' to deter against actions by individuals, groups, or a nation that would constitute a threat to international peace and security.").

83 The focus of this Article is on foreign intelligence collection operations and not other aspects of intelligence functions such as analysis, counterintelligence and covert action. The terms "intelligence collection" and "espionage" are used interchangeably.

84 Parks, *supra* note 61.

85 Kenneth W. Abbott, *"Trust But Verify": The Production of Information in Arms Control Treaties and Other International Agreements*, 26 CORNELL INT'L L. J.1, 14, (1993) ("In a complex collective entity like a state, full sets of cardinal or interval preferences may never be clearly defined.").

of the bids being offered by other countries, there was no hesitation about passing on those details to the Soviet Union's defense manufacturers. The same was true in France, where the state has a significant share of the industrial base and the government is seen as an extension of the company.

When the end of the Cold War diminished the threat of a military confrontation between military rivals, some countries increased the use of state intelligence collection tools to target foreign private businesses for the benefit of their own private companies.[86] In the early 1990's, U.S. government reports indicated that economic espionage was "becoming increasingly central to the operations of many of the world's intelligence services."[87] According to the former Chairman of the Senate Intelligence Committee, Senator Boren, economic espionage was increasingly a function of economic competition between the U.S. and even its allies.[88]

Since 1995, the executive branch of the U.S. government has reported annually to Congress on the threat from foreign economic

---

86 *See* JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA, 5 (1997).

87 REPORT ON U.S. CRITICAL TECHNOLOGY COMPANIES, REPORT TO CONGRESS ON FOREIGN ACQUISITION OF AND ESPIONAGE ACTIVITIES AGAINST U.S. CRITICAL TECHNOLOGY COMPANIES 5 (1994), *noted in* FIALKA, *supra* note 86, at 5; s*ee also* FIALKA, *supra* note 86, at 9-13 (describing three waves of economic espionage against the U.S. between 1950 and 1996; first from Russia, then Japan and China).

88 Tom Squitieri, *New Course May Be Economic Espionage*, USA TODAY, Apr. 25, 1991, at 11A (quoting Senator Boren: "More and more the aim of espionage is to steal private commercial secrets for the sake of national economic purposes, rather than to steal military secrets for building military strengths in the spying countries. It's against private commercial targets in the U.S., carried out not by foreign companies but by foreign governments."); *see also* H.R. REP. NO. 104-788, at 5 (1996), *reprinted in* 1996 U.S.C.C.A.N. 402; GLENN P. HASTEDT, ESPIONAGE: A REFERENCE HANDBOOK 60 (2003) ("The top twelve states placing economic spies in the United States are China, Canada, France, India, Japan, Germany, South Korea, Russia, Taiwan, Great Britain, Israel and Mexico."). The French were particularly aggressive in their efforts to collect U.S. and other nations' corporate secrets. *See* RICHARD HOLM, THE AMERICAN AGENT: MY LIFE IN THE CIA 417-420 (2003) (describing the CIA's response to French intelligence service's (DGSE) operations to conduct economic espionage against American companies); *see also* Larry Reibstein et al. *Parlez-Vous Espionage?* NEWSWEEK, Sept. 23, 1991, at 40 (reporting DGSE chief, Pierre Marion, established a twenty-agent branch to acquire the secret technologies and marketing plans of private companies with the knowledge of President Mitterand). Britain, Germany, the Netherlands, and Belgium have also been involved in such operations. *See* Jay Peterzell, *When 'Friends' Become Moles*, TIME, May 28, 1990, at 50; SCHWEITZER, *supra* note 90, at 145.

espionage targeted against U.S. industry.[89] The reports reveal an ever-increasing level of economic espionage conducted against American companies, resulting in staggering losses.[90] By the late 1990s, it was readily apparent that economic espionage was a serious problem for the United States.[91] Foreign governments were employing traditional intelligence collection methods used during the Cold War to spy on each other, as well as specialized economic collection methods, to steal trade secrets.[92] As intelligence experts observed, governments had "adapt[ed] classic spy techniques from military and political espionage endeavors to conduct economic espionage."[93]

Arguably, economic espionage has been part of intelligence work since commerce began and the U.S. would appear to be a prime target for such activities. There is abundant evidence of numerous states, including China, South Korea, Japan, France, Russia, Israel and Germany, conducting economic espionage against the U.S. over the years.[94] In the face of such evidence, however, the U.S. has maintained a policy that prohibits U.S. intelligence agencies from carrying out economic espionage.[95] As frustration grew in the 1990s with the overwhelming evidence of such activities against the U.S., even by allies, a debate arose

---

89 See e.g., Archives, NATIONAL COUNTERINTELLIGENCE CENTER, http://www.ncix.gov/publications/archives/index.php (last visited Nov. 4, 2014).

90 An estimate of cost to the U.S. economy from economic espionage done in 1991 by the White House Office on Science and Technology put the damage at "one hundred billion dollars annually." *See* SCHWEITZER, *supra* note 1, at 24.

91 *See, e.g.*, United States v. Hsu, 155 F.3d 189, 194 (3rd Cir. 1998) ("By 1996 . . . nearly $24 billion of corporate intellectual property was being stolen each year.").

92 Ronald E. Yates, *Cold War: Part II, Foreign Intelligence Agencies Have New Targets – U.S. Companies*, CHI. TRIB, Aug. 29, 1993, at C1.

93 Edwin Fraumann, *Economic Espionage: Security Missions Redefined*, 57 PUB. ADMIN. REV. 303 (1997).

94 FIALKA, *supra* note 86, at 5.

95 The prohibition is based on social, cultural, and legal traditions of America, both for philosophical and practical reasons. Leo Cherne, *quoted in* PETER SCHWEITZER, FRIENDLY SPIES: HOW AMERICA'S ALLIES ARE USING ECONOMIC ESPIONAGE TO STEAL OUR SECRETS 15 (1993) (Leo Cherne, a former member for the President's Foreign Intelligence Advisory Board, describing that prohibition on U.S. intelligence agencies from conducting economic espionage and how "the U.S. is truly handicapped by its culture, laws, the nature of our society and our belief in the market economy in our dealings with foreign countries . . ."). For a list of the different challenges that were identified with the intelligence community sharing corporate secrets with American companies see LOWENTHAL, *supra* note 54, at 384-85.

among individuals inside and outside of the U.S. intelligence community over whether the U.S. ought to change its policy against economic espionage, with some supporting the idea of the U.S. conducting economic espionage in order to "level the playing field" in trade relations.[96] Supporters for a change in policy argued that "America's unwillingness to engage in economic espionage seriously handicaps the United States *vis-a-vis* our major economic competitors"[97] and that by engaging in the activities ourselves, other states would be deterred.[98] It was suggested that the NSA and the Central Intelligence Agency ("CIA") might use their talents to spy on foreign companies in the same way the French spied on U.S. corporations.[99] Such notions, however, did not receive support from either U.S. companies or the intelligence community.[100]

As mentioned above, economic espionage, in contrast to espionage for political and military purposes, is a government's efforts to collect protected information from a foreign corporate entity or individual and to provide that information to a private or state-owned enterprise.[101] Its purpose is to provide advantages to a state's own private sector, eliminating the need to invest in research and development programs, increasing its competitiveness on the international trade market, while disadvantaging the other state, preventing it from capitalizing on its innovation, and potentially denying it access to the global marketplace.[102] The proprietary information stolen by the intelligence and military personnel can include sales projections,

---

96 Admiral Stansfield Turner, the DCI under President Carter, gathered together senior CIA officials to discuss the possibility of a plan to have the U.S. intelligence community conduct economic espionage/state-sponsored industrial espionage. They rejected Turner's ideas. *See* Jeff Augustini, *From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage*, 26 LAW & POL'Y INT'L BUS. 459, 484 (1995).

97 SCHWEIZER, *supra* note 1, at 15

98 *Id.* at 489-90.

99 SCHWEIZER, *supra* note 1, at 290-94.

100 *Id* at 14; s*ee also* William T. Warner, *Economic Espionage: A Bad Idea*, NAT'L L. J. 12, 13 (Apr. 12, 1993) (Former DCI Robert Gates, referred to the idea of the U.S. intelligence community conducted economic espionage as a "moral and legal swamp.").

101 Economic espionage is distinguished from "industrial" or "corporate" espionage, which consist of the efforts of private companies stealing information from other companies.

102 SCHWEIZER, *supra* note 1, at 24.

pricing data, customer lists, product development data, basic research, marketing strategies, development plans, employee data, contract proposals, future estimated profits, proprietary software, and strategic planning.[103] In these ways, traditional espionage is distinguishable from economic espionage not only in purpose, scope, and method, but also in that traditional political, military intelligence collection fundamentally is a struggle between adversaries that deals primarily with information itself, in contrast with economic espionage that involves much more than the actual information collection; it is about economic competition on the global trade market.[104] Moreover, while there is reciprocal acceptance and benefits between states from traditional espionage, the only outcome for economic espionage is economic benefits for one state alone and economic losses to another.

Recognizing the gravity of the threat from economic espionage, the U.S. Congress adopted the Economic Espionage Act (EEA) in 1996, making the theft of trade secrets from U.S. companies a federal crime, and providing law enforcement with a new enforcement tool.[105] The EEA provides for criminal prosecution of an individual who takes, possesses, duplicates, transfers, or sells trade secrets for purposes of using the trade secrets to benefit a foreign nation or any agent thereof.[106] Although the EEA criminalizes actions that would constitute industrial espionage, such as one domestic firm misappropriating the trade secrets of another, or a disgruntled employee stealing his or her employer's trade secrets, the EEA was primarily passed to address the problem of foreign economic espionage, which is the focus of this Article.[107]

---

103 *Economic Espionage: Joint Hearing Before the Select Comm. on Intelligence of the U.S. Senate and the Subcomm. on Terrorism, Tech., and Gov't Info. of the Comm. on the Judiciary of the U.S. Senate,* 104th Cong., 2d Sess., (1996) (statement of Louis Freeh); *see* Fraumann, *supra* note 93.

104 SCHWEIZER, *supra* note 1, at 8.

105 Economic Espionage Act of 1996, 18 U.S.C. §§ 1831—1839 (1996) [hereinafter EEA]. § 1831 criminalizes "economic espionage," which it defines as a theft of trade secrets that benefits a foreign government, foreign instrumentality or foreign agent.

106 *Id*. § 1831 (allowing for prosecution of any who "appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret").

107 *See* 142 CONG. REC. S12207-08, 104th Cong. (1996) (testimony of Arlen Specter). In a statement on the act, President Clinton stated, "Economic espionage and trade secret theft threaten our Nation's national security and economic well-being." William J. Clinton, *Statement on the Economic Espionage Act*, U.S. NEWSWIRE, Oct. 15,

Since the passage of the EEA, there have been about 100 indictments with a handful of convictions,[108] including seven cases out of a total of eleven cases since 2010 related to "stolen IP destined for Chinese entities."[109] And while such prosecutions can contribute to preventing economic espionage, these actions alone are unlikely to accomplish this, especially when states may be the perpetrators acting behind proxies, which may be difficult to prove, and indicted individuals may be abroad, rendering it nearly impossible to gain custody over without state consent.[110] As argued in this Article, solutions to these problems will need to be addressed by international law and international cooperation, necessitating the adoption of adequate international legal procedures.[111]

While some countries have passed laws related to the theft of IP, there is an absence of comprehensive legislation relating to offenses committed in the cyber realm, not to mention theft rising to the level of transnational economic espionage.[112] There is no universally accepted norm when it comes to the theft of information for economic gains. Part of the challenge is that some countries do not respect the IP rights of other states and therefore their national laws reflect a limited attempt to protect trade secrets and criminalize its theft.[113] For those countries where the government plays a role in encouraging industrial espionage, the conflict between economic nationalism and international competition will be an ongoing problem. And while the diversity of such national laws among states can support an argument that there is no shared view of whether state sponsored theft of trade secrets is permissible or not, the fact that a variety of countries have adopted or strengthened measures to protect trade secrets, mainly through WTO membership obligations, is at least evidence

---

1996.

108 THE IP COMMISSION REPORT, *supra* note 22, at 42.

109 *Id.* at 15.

110 Hedieh Nasheri, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING, 2-3 (Cambridge ed., 2005).

111 *Id.*

112 *Id.*

113 For example, one of France's early patent laws gave "to whomever shall be the first to bring to France a foreign industry the same advantages as if he were inventor of it." *Id.* at 91.

of a trend toward delegitimizing this activity.[114] While the trade laws have developed to focus on the protection of trade secrets, the rise of the Internet provides a new means of committing crimes such as state-sponsored economic espionage, which has not been specifically addressed by any laws.[115]

As discussed earlier, the U.S.'s position on economic espionage has always been that there should be a separation between the government and the private sector, and government resources should not be used to benefit specific companies.[116] Economic espionage employs ruthless trade practices that go against the principles of honest business practices and fair competition that the international trade regime promotes, not only distorting the economic balance between the two countries, but also globally. China's goal in stealing IP is to close the technology gap between the U.S. and China, turning American companies into unwilling accomplices to China's plans.[117] A startling book written by two Chinese People's Liberation Army ("PLA") officers, *America, Russia and the Revolution in Military Affairs*, predicted that the gap would actually close by 2007, at which time America's vaunted dominance in information technologies would be over.[118] According to the *IP Commission*

---

114 Salem M. Katsh and Michael P. Dierks, Globally, *Trade Secrets Are All Over the Map*, 7 JOURNAL OF PROPERTY RIGHTS (1995). For example, Canada, China, Germany, Italy, Japan, Korea, Mexico and the UK and U.S. have enacted statutory protections for trade secrets. *See* Nasheri, *supra* note 110 at 211 (citing Katsh and Dierks).

115 ONCIX 2004 Report at 1 ("Increasingly, foreign entities need not even come to the United States to acquire sensitive technology but instead, can work within their own borders."). As early as 1996 China had established a secret information warfare center that centralized the activities of the "theft of economic secrets" as well as offensive cyber attacks. *See* James Adams, THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS & THE FRONT LINE IS EVERYWHERE 251 (Simon & Schuster, 1998).

116 During the debate within the U.S. about whether to allow the U.S. intelligence agencies to conduct economic espionage, opponents to such a policy raised a number of concerns to include questions related to how the U.S. government would safeguard the sources and methods used in obtaining the information, with whom would the intelligence be shared (which companies constitute "U.S. companies"), which specific U.S. companies would the government provide the intelligence to, would there be a *quid pro quo* on the part of the government by giving the company the information? There were no satisfactory answers to these questions and debate on the topic during the 1990s concluded in a consensus that doing so would be a bad idea. LOWENTHAL, *supra* note 54, at 384-385.

117 *See* Fialka, *supra* note 86, at 5.

118 *See* Adams, *supra* note 115, at 255.

Report, "China is projected to pass the United States in total economic output between 2016 and 2030, depending on the source and methodology used."[119]

Economic espionage is about economic competition, the goal being to prevent the target from advancing economically. It is not about collecting information an adversary tried to keep secret in order to inform the making of policy; rather, it is about stealing property and information to provide domestic companies with an economic advantage, disadvantaging foreign companies, and eviscerating any competition. IP theft results in the loss of revenue for those who made the invention as well as of the jobs associated with those losses. It also undermines the means and the incentive to innovate, slowing the development of new inventions and industries that would otherwise expand the world economy and raise the prosperity and quality of life for everyone. The negative impact from IP theft on core values is global and staggering.

C. Treatment of Political/Military Espionage versus Economic Espionage Under International and Domestic Law

1. Intelligence Collection Under International law

Peacetime intelligence collection is effectively ignored by traditional international law.[120] With the single exception of the laws of war, there is no rule or body of rules in public international law that deals directly with the fundamental question of the legality (or illegality) of espionage.[121] Given the prominent role that espionage has played in international relations at all levels of decision-making, this omission is remarkable,[122] and it has

---

119 THE IP COMMISSION REPORT, *supra* note 22, at 15.

120 Richard A. Falk, *Foreword* to ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW (Roland J. Stanger ed., 1962) ("Traditional 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 in the event of capture.").

121 For a discussion of wartime espionage, *see* Baxter, *So-Called 'Unprivileged Belligerency'– Spies, Guerrillas, and Saboteurs,* 28 BRIT. YB. INT'L L. 323 (1951).

122 Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach,* 19 AM. U. INT'L L. REV. 1091, 1091 (2004) ("Espionage is . . . ill-defined under international law, even though all developed nations, as well as many lesser-developed ones, conduct spying and eavesdropping operations against their neighbors.").

contributed to the perception that espionage is extra-legal.[123] State practice has bolstered this view in that individual states have sought to deny, with rare exceptions, any systematic involvement in espionage and to conceal it in practice.[124] Indeed, however, as this Article noted earlier, despite the occasional outcries for its cessation,[125] states have long engaged in espionage and acknowledged it as a matter of practical reality. Arguably, the long history of espionage by states has given its practice the appearance of lawful activity, "grounded in the [states'] recognition that 'custom' serves as an authoritative source of international law."[126] And yet, "its very ubiquity seems to have obscured it from visibility to scholarly inquiry."[127]

The more traditional doctrinal view under international law has been that intelligence gathering within the territorial confines of another state, while not rising to the level of an "armed attack," constitutes an unlawful intervention.[128] Others have discussed espionage as lawful in that determining the intentions of other nations can constitute self-defense by allowing states to judge the potential threats more accurately.[129] It would seem that traditional

---

123 *Id*. at 1092 ("[I]nternational law neither endorses nor prohibits espionage, but rather preserves the practice as a tool by which to facilitate international cooperation.").

124 Baker, *supra* note 122, at 1094.

125 *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) (citing "sporadic demands for nonrepetition" of spying activities).

126 Baker, *supra* note 122, at 1094.

127 McDougal et al., *supra* note 4, at 365-448 (describing intelligence collection as existing in "an arena characterized by rudimentary normative demands").

128 *See, e.g.*, Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, 12 (Roland J. Stanger ed., 1962) [hereinafter Wright, *Doctrine of Non-Intervention*] ("[P]enetration 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.").

129 For a discussion of spying in support of a right to self-defense, *see, e.g.*, JOHANNES ERASMUS, THE INTELLIGENCE SERVICE 115, n. 120 (1952) (citing Heffter-Geffeken at 495); McDougal et al., *supra* note 4, at 368 ("Espionage becomes a functional method of sharing information for common purposes."); Glenn Sulmasy and John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. OF INT'L L. 625-38, 627 ("[I]ntelligence gathering can be "lawful" as a necessary means for nation-states defend themselves."). These assertions, however, are difficult to rectify with the doctrinal law of self-defense in the UN Charter related to the right of self-defense "against armed aggression." Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F.L. REV. 217, 224 (1999).

international law consigned espionage to a peculiar limbo under the law.[130]

In the practice of states, however, as the Cold War evolved, espionage became a systematic, publicly recognized form of state activity essential to the conduct of international relations, with almost all countries actively engaging in the practice.[131] While states continued to reserve the right to enforce national espionage statutes, they became increasingly candid about their own intelligence gathering activities.[132] Countries began to openly acknowledge that they were conducting intelligence collection, even identifying their intelligence officials in public.[133] Today, it is no longer surprising to hear in the news about a government official laying claim to a captured intelligence officer and participating in bartering arrangements for his release. In light of the actual volume of the spying activity, and the few formal protests lodged against it, this suggests states maintain a somewhat ambivalent perspective regarding such activities.[134] Although such practices cannot be interpreted as toleration of the penetration of the territorial integrity of a state, they are significant indicators of new perspectives by states regarding the collection of intelligence. This may indicate an admission of the lawfulness of intelligence

---

130 *See, e.g.,* OPPENHEIM, INTERNATIONAL LAW § 455 (3d ed., 1920) ("[A]lthough it is not considered wrong morally, politically or legally to [send spies abroad], such agents have no recognized position whatever according to international law[.]"); A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 605-606 (2007) ("[E]spionage is neither clearly condoned nor condemned under international law."); Sulmasy and Yoo, *supra* note 129, at 625 (arguing that international law "has had little impact on the practice of intelligence gathering").

131 *See* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. POL'Y 63, 71 (2010) (quoting Hays Parks: "No serious proposal has ever been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each.").

132 Chesterman, *supra* note 125, at 1072 ("Most domestic legal systems . . . seek to prohibit intelligence gathering by foreign agents while protecting the state's own capacity to conduct such activities abroad.").

133 James Adams, THE NEW SPIES: EXPLORING THE FRONTIERS OF ESPIONAGE, 88-89 (PIMLICO, London, U.K., 1994) (discussing how in October 1991, the head of the British intelligence service, Sir Patrick Walker, for the first time in history publicly acknowledged the existence of the British Security Service and his identity as the head of MI5 by stating at a public gala, "My name is Sir Patrick Walker. I am the director-general of the Security Service.").

134 McDougal et al., *supra* note 4, at 394.

gathering when conducted within some accepted normative limits.[135]

Like traditional espionage, there is no explicit legal prohibition for espionage in cyberspace.[136] Cyber espionage operations have been taking place since at least the 1990s, with the emergence of the Internet allowing governments to collect information more pervasively than traditional human methods of collecting information clandestinely.[137] Similar to traditional, political, or military espionage, cyber espionage, or cyber exploitation, constitutes the acquisition of information to inform policymakers about actual or potential threats, and does not rise to the level of a use of force or armed attack under international law.[138] Given that they are similar in their objectives, cybersecurity experts have argued that cyber espionage should have the same legal status as traditional, political, and military espionage.[139] In short, cyber espionage is another form of technology-enabled espionage or intelligence collection and as such is distinguishable from other intelligence functions that are more equivalent to low-intensity conflict.[140] Moreover, cyber espionage of this nature is

---

135 *See id.* at 395 ("The gathering of intelligence within the territorial confines of another states is not, in and of itself, contrary to international law unless it contravenes policies of the world constitutive process affording support to protected features of internal public order. Activities that seriously compromise the dignity of individual citizens, their privacy or personal security, or involve the destruction of property are, of course, unlawful no matter which decision function they attend. Such activities are, however, still widespread adjuncts of intelligence gathering.").

136 Daniel B. Silver (updated and revised by Frederick P. Hitz & J.E. Shreve Arial), *Intelligence and Counterintelligence*, *in* NATIONAL SECURITY LAW 935, 965 (John Norton Moore & Robert Turner eds., 2005) (describing the status of espionage in international law as "ambiguous").

137 *See* Bob Drogin, *Russians Seem to Be Hacking Into Pentagon*, LA TIMES, Oct. 7, 1999; *see also* Bradley Graham, *Hackers Attack Via Chinese Web Sites*, WASH POST, Aug. 25, 2005.

138 *See* Schmitt, *supra* note 6.

139 James A. Lewis, *The Cyber War Has Not Begun,* CSIS (Mar. 2010), *available at* http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf ("Nations should treat political and military espionage in cyberspace as they treat it in the physical world.").

140 Indeed, certain activities of intelligence agencies can involve activities that would constitute low-intensity conflict, indirect aggression, or indirect intervention such as the arming of rebels are other activities related to covert action, but this Article draws a distinction between intelligence collection, the focus of this Article, as opposed to such other intelligence activities involving covert action. And even though intelligence collected can be used to support such activities, including torture, it is only the collection

distinguishable from cyber economic espionage, as discussed earlier.

Some have speculated that the lawfulness of a particular act of spying may depend on the sponsor state's motivation.[141] If, for example, the information sought "contributes to defensive rather than aggressive policies of national defense," the act of espionage arguably would claim greater legitimacy under international law.[142] The acceptance of intelligence collection for the purposes of a global security system may be considered by some to be a radical trend away from traditional doctrinal notions of sovereignty under international law, but in light of ongoing state practice, it may also be seen as an indication of legality.[143] By extension, cyber espionage in line with the same objectives of traditional espionage may be seen as acceptable state practice under international law as long as such activities stay within the bounds of acceptable limits analogous to those rules of traditional espionage that have been accepted by states. There has been a marked difference, however, in state reactions to acts of economic espionage conducted through the physical realm of in cyberspace, as reflected by the U.S.' consistent objections to non-cyber economic espionage activities since at least the early 1990s and its most recent indictment of the PLA members for cyber economic espionage.[144]

2. Intelligence Collection as a Matter of Domestic Law

States typically do not come forward to defend spies caught by the techniques of counterespionage.[145] Rather, states engage in

---

of information through espionage that is within the scope of this Article. *See* McDougal et al., *supra* note 4, at 368 ("[T]he broader effect of gathering operations must . . . be considered in context and . . . in terms of disseminations and uses of intelligence products: data gathered innocuously may be used with brutal effects."); *see also* David P. Fidler, *Inter arma silent leges Redux? The Law of Armed Conflict and Cyber Conflict, in* CYBERSPACE AND NATIONAL SECURITY: THREATS, OPPORTUNITIES, AND POWER IN A VIRTUAL WORLD 71, 74 (Derek S. Reveron, ed., 2012) ("[S]uch activity constitutes high-intensity espionage as opposed to low-intensity conflict.").

141 Falk, *supra* note 120, at 58 ("[T]he test for the relative illegality of espionage rests to some degree upon one's judgment of the end being sought.").

142 *Id.*

143 *See* Lin, *supra* note 131.

144 *See* Nasheri, *supra* note 110, at 53.

145 For example, consider the silence of Soviet authorities during the long trial of Colonel Abel as well as the exchange of Abel for Powers. WEST, *supra* note 63, at 154-77.

mutual exchanges of captured spies, avoiding the politically embarrassing process of a prosecution, indicating that governments attach a great importance to spies as state agents and implicitly recognizing espionage as a systematic state activity that is to be expected in international relations.[146] The rules of the game allow a state to employ a spy and to prosecute spies that they catch, reflecting a relationship between the individual spy and the state, as opposed to a relationship between states at the international level.[147] For example, the legal authority according to which a state conducts intelligence operations, hiring and tasking and sending spies abroad, is based on a social contract between the people of the country and its government. Such rules also cover the state's use of electronic surveillance for intelligence collection purposes. Today, many states have open laws that provide explicit details about the authorities and limitations that have been granted to intelligence organizations within the state.[148] The same is true for laws that states enact prohibiting espionage activities within their own territories by outsiders, providing the government the authority to prosecute a spy for violating domestic laws.[149] These laws govern the relationship between the individual arrested for spying and the state prosecuting the individual.[150]

Throughout history, states often adopt new domestic laws restricting or prohibiting certain aspects of intelligence operations in the aftermath of controversial disclosures of government intelligence activities, whether domestically or internationally, that

---

146 *Id*.

147 The U.S. has criminalized the act of espionage under the Act of 1917, 18 U.S.C. 793(a)-(e) (prohibiting the collection, receipt, or transfer of "information respecting the national defense," where the individual acts "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").

148 In the U.S. the National Security Act of 1947 was enacted, establishing the authorities of the Director of Central Intelligence as the head of the CIA and in charge of foreign intelligence collection. *See* Adams, *supra* note 133, at 94 (discussing the 1989 Security Service Act that for the first time placed British MI5 on a statutory basis). In Germany, the Federal Intelligence Service (BND) is responsible for conducting foreign intelligence analysis and electronic surveillance of "threats to German interests" from abroad. *See* Directorate General for Internal Policies: Citizens Rights and Constitutional Affairs, *National Programmes for Mass Surveillance of Personal Data in EU Member States and their compatibility with EU law*, 68 (2013), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.

149 *See* Chesterman, *supra* note 125, at 1072.

150 *Id.*

are offensive from the perspective of the public.[151] From the public debates that took place in the 1970s over allegations of illegal activities of U.S. intelligence agencies to the current controversy over NSA's surveillance programs that recently came to light, these examples illustrate the tension that at times exists between a state's government and its people as related to intelligence activities.[152] But these discussions concern what a country's citizens are comfortable accepting as the role of the intelligence community and not about concerns of breaches of obligations owed to other states under international law. For example, if a American spy is found to violate U.S. law, the individual or a higher official within the U.S. intelligence community is held accountable under U.S. domestic law; the state itself is not held responsible. In the same sense, when a spy is caught abroad, there is no sense of legal culpability for the state from which the spy sent, instead, culpability extends only to the individual. When a state condemns the act of espionage directed against it, it does so as a matter of violation of its domestic laws and not under a belief that international law has been violated.[153]

Traditional espionage appears relegated to matters of domestic law.[154] While a comparative examination of all states' domestic legal systems related to espionage is beyond the scope of this Article, almost all states have enacted domestic laws that both restrict access to classified information as well as criminalize the act of an unauthorized taking of such information in order to deny intelligence gathering within their territories.[155] Actual or

---

[151] *See* Schmitt, *supra* note 6, at 276.

[152] *Id.*

[153] In response to the recent revelations of NSA's surveillance abroad by Edward Snowden, Brazilian President Dilma Rouseff, at a U.N. General Assembly meeting, publicly accused the U.S. of violating international law, yet failed to mention any specific source of law that was violated. *See* Julian Borger, *Brazilian President: US Surveillance a 'Breach of International Law'*, GUARDIAN, Sept. 24, 2013. Rouseff claimed that U.S. actions violated Brazil's sovereignty and its citizens' human rights and civil liberties. *See* Thalif Deen, *Breaking UN Protocol, Brazil Lambastes US Spying*, INTER PRESS SVC (Sept. 24, 2013), http://www.ipsnews.net/2013/09/breaking-u-n-protocol-brazil-lambastes-u-s-spying/; *see also* Schmitt, *supra* note 6, at 276 ("The ongoing Snowden affair, which revealed widespread monitoring of activities abroad by the U.S. National Security Agency, illustrates the international community's unease with cyber operations that target other states or their citizens even when nondestructive and, perhaps, lawful under current understandings of international law.").

[154] *See, e.g.,* Espionage Act, 18 U.S.C. § 37 (1917).

[155] *Id.*

threatened prosecution under these domestic laws takes the form of denial of information rather than an assertion by the state that the act is a *per se* in violation of international law, the legal issue is about individual criminal liability and not state responsibility.[156]

These domestic laws serve to prohibit foreign intelligence collection efforts within a state's territory without inhibiting the state's own efforts to collect intelligence about other states within their territories.[157] As mentioned above, there has been a trend since at least the early 1990s, and earlier for some states, toward increased openness about certain kinds of transnational intelligence activities.[158] Today, many states have acknowledged intelligence services and national laws that specifically identify and outline the authorities for their intelligence agencies to conduct intelligence gathering abroad.[159] Such legislative trends, coupled with the practice of state responses when spies are uncovered, may suggest a change in attitudes toward what is acceptable under international law. In this sense, the domestic laws that criminalize the act of espionage against a state, coupled with domestic laws that publicly acknowledge and empower agencies to conduct intelligence abroad, may be more reflective of a state's right to protect against espionage than indicative of a state's belief that espionage is a violation of international law.

3. Intelligence Collection as a Matter of International Law

The suggestion that intelligence collection is illegal under international law is often based on the reasoning that espionage is criminalized in the domestic legal systems of most states and therefore, there is a sense that states must then view such activities as unlawful under international law. This position is based on the

---

156 *See, e.g., United States Diplomatic and Consular Staff in Tehran* (U.S. v. Iran), 1980 I.C.J. 3, ¶¶ 85-87 (May 24).

157 *See* Espionage Act, *supra* note 154.

158 *See* discussion *infra* Part II of the existence of foreign intelligence services

159 *See Id*. Depending on the nature of the government of a nation, there will be more or less information available about the details of their domestic laws related to the intelligence agencies. *See* PSI HANDBOOK, *supra* note 55. For instance, with the enactment of the National Security Act, the U.S. has codified under domestic law the authorities of the intelligence community to conduct intelligence operations abroad. National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 (codified as amended in scattered sections of 50 U.S.C. § 15).

presumption that "[u]nder international law, if something were truly legal (or at least not illegal), no state should prosecute those who do it."[160] This position, however, misconstrues the concept of "principles of law recognized by civilized nations" as a source of international law.[161] "General principles of law" as a source of international law elevates domestic legal principles common to all domestic legal systems to the level of international law only if such principles are applicable to inter-state relations.[162] Of course, international law can and does regulate the means or methods utilized in intelligence collection, such as prohibiting the torture of individuals in order to obtain intelligence information. Furthermore, international law does impose some limitations on intelligence collection in specific circumstances. Such restrictions, however, cannot support any arguments for the general legality or illegality of peacetime espionage.[163] The criminalization of such methods, however, is distinct from intelligence collection per se being unlawful under international law.[164]

International law is fundamentally based on the principle of reciprocity.[165] States enter into agreements, promising to restrain

---

160 A. John Radsan, *The Unresolved Equation of Espionage and International Law* 28 MICH. J. OF INT'L L. 596, 604-05 (2006-2007).

161 UN Charter, Art. 38(1)(c) of the Statute of the International Court of Justice.

162 JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 23-30 (8th ed., Oxford Univ. Press 2012).

163 For example, limitations on intelligence collection are included in the Vienna Convention on Diplomatic Relations of 1961, the Vienna Convention on Consular Relations of 1963 and the Convention on Special Missions of 1969. Simon Chesterman, *The Spy Who Came in from the Cold War*, 27 Mich. J. of Int'l L. 1071, 1087-88 (2006). *See also* Law of the Sea Convention (UNCLOS), art. 19 (noting that states are obligated under UNCLOS not to conduct espionage while transiting the territorial sea of a coastal state under the innocent passage principle).

164 In 1980, Iran presented the issue of intelligence collection to the I.C.J., in the *Tehran Hostages* case, arguing that the seizure of the American embassy and its personnel was justified because U.S. personnel at the embassy had been conducting espionage in Iran Case Concerning United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, 15 (May 24, 1980) (Judgment). The Court rejected this as justification, noting the difficulty in determining when a diplomat's function of "ascertaining by all lawful means conditions and developments in the receiving State" constitutes interference in internal affairs. *Id.* at 39-40. The Court assessed that the lack of precision was overcome by permitting states to declare diplomats persona non grata based on their own domestic political and legal standards. *Id.*

165 *See* McDougal et al., *supra* note 4, at 380-81 (discussing the unwritten but reciprocal right of states to conduct intelligence activities out of their embassies located abroad: "Although they are not mentioned in the Vienna Convention or in the major

themselves in certain ways, because of the belief that states honor their promises and in doing so each side will receive reciprocal benefits.[166] Espionage as the collection of secret information offers reciprocal benefits to both sides.[167] Each side can seek to use intelligence gathering as a means to understand the capabilities and intentions of other nations that do not disclose freely such information. As long as states stay within the agreed redlines of espionage activities, states will allow each other to continue the practice without holding the state liable if a spy is detected.[168] In this way, espionage does not serve the divisive interests of each side against the other, but rather serves the common interest of both to know what the other side might be hiding.[169]

Intelligence collection supports the notion of reciprocity under international law by providing a pool of information that a state can share with other states, benefitting all states included in the sharing.[170] This sharing of intelligence can facilitate international

---

texts, these intelligence activities are accepted as a correlative purpose of diplomatic activity and are tolerated with a high degree of latitude.").

166 *Id.*

167 *Id.*

168 *Id.*

169 For a discussion of the various arms control treaties that establish a right for parties to collect intelligence for purposes of assessing other parties' compliance with the treaties see Chesterman, *supra* note 125, at 1090-92. In 1955, President Eisenhower proposed an "Open Skies" agreement with the Soviets, which called for an international aerial monitoring system that would prevent states from hiding stockpiles of nuclear weapons. The Soviets rejected the idea. When the U.S. aerial surveillance efforts over the Soviet Union were disclosed with the crash of Gary Powers in 1960, the State Department, in a press release, defending the U-2 flights, expressed the U.S. position that the collection of information about other countries' intentions and capabilities was an effective measure against surprise attack and aggression that enhances peace. The State Department noted President Eisenhower's proposed "Open Skies" agreement as an effort to establish peace through more available information. *See* Loch K. Johnson, *Spies*, FOREIGN POL'Y, Sept. 2000, at 24-25 (discussing the importance of the information that CIA collected relating to the activities of the Soviet Union in Cuba).

170 This practice of intelligence pooling is codified as one of the principles of the Proliferation Security Initiative (PSI) which represents the commitment of eleven states to counter the proliferation of weapons of mass destruction, pledging to exchange intelligence gathered by their individual intelligence agencies. *See* U.S. Department of State, White House Fact Sheet (Sept. 4, 2003) (noting that one of the PSI "interdiction principles" is to provide "the rapid exchange of relevant information" while "protecting the confidential character of classified information provided by other states . . ."). PSI illustrates the role of espionage in achieving cooperation on the mutual goal of counter-proliferation. This is in line with McDougal's criteria of "inclusiveness," acting not just

cooperation by solidifying the commitments states make to one another towards peaceful achievement of mutually shared interests and by providing decision-makers with necessary data to make informed decisions while building trust among states.[171]

Cases in which a state captures a spy within its territory and sends the spy back home instead of prosecuting would indicate that states accept the benefit of reciprocity in allowing spies within their country, so long as their spies will receive equal treatment by the other state.[172] In fact, the practice of swapping spies supports the notion of reciprocity. When a spy is prosecuted, the fact that the spy's employing state is not drawn formally into the espionage trial and there is no effort to impose legal responsibility on the state for the espionage indicates that states will not hold one another responsible for the act of espionage.[173] In a sense, there is a norm of reciprocally tolerated espionage as long as states follow the rules of the game.[174] If, however, a sending state diverges from the accepted rules, it may be vulnerable to charges of illegality.[175] If a state acknowledges a specific act of espionage publicly and defends it, it opens itself up to allegations of illegal actions under international law, as in the U.S.'s acknowledgement of the U-2 overflights of Soviet territory that led to the Soviets bringing allegations of U.S. "acts of aggression" before the U.N. Security Council.[176]

---

for the "self." This is different with economic espionage where there is no reciprocity; states stealing trade secrets are not planning on sharing the benefit of that information with other states in pursuit of mutual interests.

171 *See id.* at 375. *See also* Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. UNIV. INT'L L. REV. 1091, 1111-12 (2003-2004).

172 McDougal et al., *supra* note 4, at 365, 368 n.9 (1973) (recognizing that a normative demand of espionage as "reciprocal expectations of authority [that] may be generated between contending parties").

173 *See id.*

174 Julius Stone, *Legal Problems of Espionage in Conditions of Modern Conflict*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 29, 31 (Roland J. Stanger ed., 1962).

175 *See, e.g.,* Quincy Wright, *Legal Aspects of the U-2 Incident*, 54 AM. J. INT'L L. 836, 841-42 (1960) [hereinafter Wright, *Legal Aspects*].

176 In his memoirs, Nikita Khrushchev claimed that it was Eisenhower's admission of responsibility rather than the flight itself that caused him to scuttle the Paris "Big Four" summit meeting. *See* NIKITA S. KHRUSHCHEV, KHRUSHCHEV REMEMBERS: THE LAST TESTAMENT 447-48 (Strobe Talbott ed., trans., 1974). The U-2 flight was characterized by the United Nations Security Council as a violation of Soviet airspace,

Throughout the practice of states prosecuting spies, states have not engaged in any significant efforts to make the activity of spying an international crime, *delicta juris gentium*.[177] On the contrary, states have largely chosen to maintain silence about their espionage activities.[178] Lassa Oppenheim, the first international legal scholar to discuss peacetime espionage, stated that "[a]lthough all states constantly or occasionally send spies abroad, and although it is not considered wrong morally, politically, or legally to do so, such agents have, of course, no recognized position whatever according to international law, since they are not agents of states for their international relations."[179] As some contemporary international legal scholars have discussed the topic of espionage, "[i]ntelligence collection is the international norm . . . [and] as such[,] it does not violate international law."[180] Others have described espionage as possessing "the peculiar quality of being tolerated, but illegal," with most, if not all, states collecting intelligence against other countries.[181]

According to the voluntaristic theory of international

---

but not as an illegal use of force contrary to Article 2(4) of the UN Charter. *See* Wright, *supra* note 128, at 841-42. From the U-2 incident it can be argued that intelligence gathering by aircraft does not constitute per se a violation of international law by the originating state, but that the state whose airspace is penetrated may resort to reasonable use of force to defend its sovereignty against such entry. *See* Richard A. Falk, *Space Espionage and World Order: A Consideration of the Samos-Midas Program, in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, *supra* note 120, at 45; *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. V. U.S.), 1986 I.C.J. 14, ¶ 292 (June 27) [hereinafter *Nicaragua*].

177 McDougal et al., *supra* note 4, at 394; *see also* Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 347 (1996) ("While clandestine information gathering will continue to be considered an unfriendly act between nations, such activity does not violate international law.").

178 *See* Wright, *Legal Aspects*, *supra* note 175, at 837 n.3 (noting how the United States government broke this practice by explicitly defending its espionage in the case of the U-2 overflights of Soviet territory in 1960).

179 OPPENHEIM, *supra* note 58.

180 W. Hays Parks, *The International Law of Intelligence Collection*, *in* NATIONAL SECURITY LAW 433, 433 (John Norton Moore et al. eds., 1990); *see also* Kanuck, *supra* note 7, at 276 (discussing the nuances behind espionage's legality or illegality).

181 Falk, *supra* note 120, at 57; *see also* Radsan, *supra* note 130 (arguing thoroughly that espionage is illegal under international law); WINGFIELD, *supra* note 69, at 350 (arguing that peacetime espionage is one of many legitimate tools at a state's disposal); Chesterman, *supra* note 125 (noting how states conduct espionage despite their attempts to prohibit foreign agents from intelligence gathering).

obligations, as formulated in the *Lotus* case, those who assert the existence of a rule of law restricting state activity must specify a particular norm of international law proscribing such conduct.[182] Absent any specific prohibition, or lacking consensus as to whether a legal rule even exists within international law regarding espionage, it is useful to ask whether there are any principles, manifested in the practice of states, which evidence any existing restrictive rules or close analogies. On this point, some scholars have argued that espionage during peacetime is "a violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of other states," reasoning that "any act by an agent of one state committed in another state's territory, contrary to the laws of the latter, constitutes intervention, provided those laws are not contrary to the state's international obligations."[183]

Proponents of this position depict espionage as "indirect" or "subversive" intervention, base their claims on a much broader definition of "intervention" than is supported under international law. This overly broad definition fails to incorporate the required element of coercion as a necessary aspect of the prohibited intervention under international law.[184] Not all forms of interference into the domestic matters of a state would constitute unlawful coercive intervention. Under the principle of non-intervention in international law, the mere violation of the domestic laws of a state does not necessarily meet the threshold for prohibited coercive intervention.[185] To draw an example, the arming of rebels within the territory of another state in support of their goals to overthrow the government would certainly violate not only the state's domestic laws, but also the norm of non-intervention, while the intelligence gathering of information

---

182 *See S.S. Lotus* (Fr./Turk.), 1927 P.C.I.J. (ser. A) No.10, at 13 (Sept. 7).

183 Wright, *Doctrine of Non-Intervention*, *supra* note 128, at 13.

184 *See* discussion *infra* Part II.

185 *Legal Aspects of Reconnaissance in Airspace and Outer Space*, 61 COLUM. L. REV. 1074, 1074 (1961) ("Espionage of itself does not appear to constitute a violation of international law."); Stone, *supra* note 174, at 34 ("[T]here is no sufficient warrant for saying that international law does not permit state-authorized espionage in peacetime."); TALLINN MANUAL, *supra* note 6, at 180-81; Sean Watts, *Low-intensity Cyber Operations and the Principle of Non-intervention* 13 (May 5, 2014) (unpublished article) (on file with the Social Science Research Network), *available at* http://ssrn.com/abstract=2479609.

related to the actions of those same rebels or the government, with no other actions taken, while arguably violating the domestic espionage laws and sovereignty of the state, would not violate the norm of non-intervention since there would be no element of coercion involved in the intelligence collection activities alone.[186] The topic of coercion as an element of the norm of non-intervention will be addressed in more detail later in this Article as it relates to the theft of intellectual property as a form of coercive intervention.

Some observers have argued that espionage may be legal as a matter of customary international law.[187] The suggestion is that because of the long-standing practice by most states, sending spies clandestinely into another country is not legally wrong.[188] Under international law, this argument is based on the principle of customary international law that supports the existence of an international rule based on evidence of a "general practice accepted as law." As stated in Article 38(1)(b) of the ICJ Statute and supported by decisions of the ICJ,[189] a customary rule requires both generally uniform and consistent state practice and *opinio juris*, the belief by the state that the behavior is required or permitted under international law.

Scholars have suggested that the argument of customary law is a flawed offering as support the fact that when a state's spy is captured, the sending state typically does not intervene and

---

186 McDougal et al., *supra* note 4, at 368 n.7 ("We may, nonetheless, distinguish between gathering operations which constitute an intense intervention in some segment of social process and those whose degree of passive observation approaches social innocuousness. The degree of intervention of the gathering process has a number of important legal ramifications.").

187 *See* Smith, *supra* note 64, at 545 ("[B]ecause espionage is such a fixture in international affairs, it is fair to day that the practice of states recognizes espionage as a legitimate function of the states, and therefore it is legal as a matter of customary international law. Evidence of that is when intelligence officers are accused of operating under diplomatic cover in an embassy, they are nearly always declared personae non gratae and sent home. In exercising the right to 'PNG' a diplomat, the receiving state typically says their activities were inconsistent with diplomatic activities. I can recall no instance in which a receiving state has said that these activities violate international law.").

188 *Id.*

189 Statute of the International Court of Justice art. 38 para. 1b, June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993, *available at* http;//www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0; North Sea Continental Shelf Cases, 1969 I.C.J. 44, para. 77 (Judgment).

acknowledge that it has sent the spy. Rather, states typically try to deny knowledge of a spy's activities or quietly try to resolve the political flap with as little public attention as possible. This position that espionage must be illegal given the practice of denial by the sending states is based on the reasoning that the sending state does not intervene in defense of its spy because of a belief that what it is doing is legally wrong. Why else, the argument would flow, would the sending state stay silent in the face of their spy being arrested. Based on this reasoning, if espionage was legal, states would acknowledge their conduct when a spy is caught because the state believes what it is doing is completely legitimate under international law.[190] Based on the international legal principle of customary law, for state practice to have established a rule of law, the argument goes, the practice must be accompanied by a sense of right or legal authority and not by a sense of wrongdoing or illegality.[191]

This argument, however, is naive about the delicacies of international relations. In not acknowledging the spy, the sending state is not doing so necessarily because of a sense that its actions are illegal, but rather in order to put off what would be a very tense diplomatic conversation, but not necessarily a violation of international law.[192] The fact that spies are often given awards upon returning to their home country once PNGed from another state is reflective of the sending state's belief that there is nothing illegal or dishonorable in spying abroad.[193] In sum, given the fact

---

190 Wright, *Doctrine of Non-Intervention*, *supra* note 128, at 11.

191 *Id.*

192 Some sense of the delicacy in responding to cases of the expulsion of diplomats from a country for spying is found in L. TOBIASSEN, THE RELUCTANT DOOR: THE RIGHT OF ACCESS TO THE UNITED NATIONS 308 (1969). *See also* RICHARD HOLM, AMERICAN AGENT (St. Ermin's Press, ed., 2003) (discussing the case of the French dealing with the sensitive issue of disclosures of CIA agents working in Paris that lead to the French expelling the CIA officers from Paris. He discusses the fact that the U.S. Ambassador was originally told by the French minister that the CIA officers were being asked to leave the country "quietly" without any acknowledgement of what had occurred. However, for political reasons, in violations of the "rules of the game," the story was leaked to the press and the entire incident became public knowledge, which caused much embarrassment for both countries).

193 Russian President Dmitry Medvedev awarded 10 Russian spies who had been released and returned to Russia by the U.S., in exchange for prisoners being held by Russia in 2010, the highest honors at a ceremony upon their return to Russia. Ken Dilania, *Russian Spies Were Succeeding, FBI Official Says*, L. A. TIMES, Oct. 31, 2011.

that all states send spies to "clandestinely" collect information within other states, and that most states have passed domestic legislation establishing the some form of legal authority for such clandestine activities, it would seem that there exists *opinio juris* on the practice of espionage.[194]

4. Economic Espionage as a Matter of International Law

Some scholars have argued that economic espionage and traditional espionage exist in the same space under international law, with the absence of law regulating these activities tolerated by most states.[195] However, unlike traditional espionage, economic espionage has "no custom of reciprocity or cooperation that states should be concerned about preserving."[196] As has been suggested earlier, traditional espionage can serve to increase the security of states, helping to decrease the chances of surprise attacks and minimizing conflict, thereby preserving global security.[197] There is no equivalent benefit accruing from economic espionage because states that conduct economic cyber espionage do so in order to acquire technology and innovation they themselves have failed to develop.[198] These states will not reserve the reciprocal right to other states in conducting economic espionage; one side loses its economic competitiveness while the other side wins. Clearly, there are practical distinctions between traditional espionage and economic espionage. The question is whether there is a legal distinction under international law between traditional espionage and economic cyber espionage.

Domestically, many states have criminalized the act of economic espionage and protest against those states that conduct it, however, most states have never openly acknowledged or enacted domestic laws authorizing government agencies to steal

---

194 *Cf.* Wright, *Doctrine of Non-Intervention, supra* note 128*;* Chesterman, *supra* note 125, at 1072 (2006) (referencing argument that there is no support for a "customary" defense of peacetime espionage in international law).

195 Fidler, *supra* note 49 ("The desire to combat economic cyber espionage confronts a lack of international law on espionage and economic espionage.").

196 Skinner, *supra* note 13, at 1183.

197 McDougal et al., *supra* note 4, at 368 n.9 ("Normative demands do, of course, attend the collection of espionage; reciprocal expectations of authority may be generated . . . . [E]spionage becomes a functional method of sharing information for common purposes.").

198 SCHWEIZER, *supra* note 1, at 24.

trade secrets from another state's corporations in order to directly benefit its private sector.

The current trend seems to indicate that state practices in conducting and responding to economic espionage are distinct from those with respect to traditional espionage. In the case of the Chinese economic espionage, the U.S. did not quietly ask a few Chinese diplomats to leave the U.S., as is typical when foreign government officials are caught spying, but rather in a very public and embarrassing way for China, the U.S. government indicted five PLA officials.[199] There are even talks of the U.S. invoking a trade war with China through rough sanctions and potentially bringing a formal complaint to the WTO[200] As discussed earlier, the issue of the legality of acts of traditional espionage concerned the individual and the state. With the current discussions of sanctions and WTO claims related to economic espionage, it would seem that it is the states' actions, and not the individuals' acts, that are the target of legal dispute.

Another important distinction between traditional espionage and economic espionage is that unlike economic espionage, an important benefit of traditional espionage is that it allows states to determine and verify other states' intentions. This knowledge can build trust and cooperation, and therefore such espionage can serve as an instrument for stability and peace as long as the "rules of the game" are followed.[201] In contrast, economic espionage has the capacity to cripple states' economies and de-stabilize the global economic order at a rapid pace, potentially risking the peace and security of the international community.

If the test for legality is based on the motivation of the actor, one's judgment of the end being sought, it would seem that under international law one might also be able to draw another distinction between traditional espionage and economic

---

199 *See supra* text accompanying notes 25-48.

200 *Id.*

201 Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1097 (2004) (describing how espionage can be viewed as a "functional tool that enables international cooperation"); *see also* Kenneth W. Abbott, *"Trust But Verify": The Production of Information in Arms Control Treaties and Other International Agreements*, 26 CORNELL INT'L L.J. 1, 26 (1993) ("[S]tates seeking to convey assurances may find some foreign monitoring desirable as a way to channel information . . . .").

espionage.[202] A motivation-based analysis of the legality of espionage would have to distinguish between intelligence collection and its non-coercive purposes, as discussed earlier, and economic espionage, with its subversive influences that are coercive in nature. For instance, a clear distinction can be drawn between information gathering that aids policymakers in anticipating future trends and threats versus economic espionage utilized for the aggressive purposes of undermining the security regulations or economic policies of a sovereign state during peacetime. In the latter case, the acts of espionage can be seen to violate the independence of the target state. But in cases of surreptitious nondestructive information gathering, it may be that no harm is done to the target state, meaning there is no violation of international law *per se*.

The coercive practice of economic espionage, targeting the economic stability of a state, may implicate a number of international treaties prohibiting state actions that would be detrimental to international trade or economic development.[203] The Paris Convention was the first international agreement protecting intellectual property.[204] The Convention requires signatory nations to extend to foreign nationals the same intellectual property protections that are provided to their own citizens, and sets forth uniform rules by which member states must abide with respect to industrial property rights.[205] The treaty was designed to be flexible and allow signatory members to have some discretion in implementing national legislation.[206] In sum, the Convention does not specifically address economic espionage.[207] Article 10 on unfair competition only prohibits "any act of competition contrary to honest practices in industrial or commercial matters."[208]

---

202 *See* Falk, *supra* note 120, at 58.

203 *See, e.g.*, Paris Convention for the Protection of Industrial Property art. 1, Mar. 20, 1883, 21 U.S.T. 1583, 828 U.N.T.S. 305 [hereinafter Paris Convention] (amended most recently Sept. 28, 1979).

204 *Id.*

205 *See id.*

206 Rochelle Cooper Dreyfuss, *An Alert to the Intellectual Property Bar: The Hague Judgments Convention*, 2001 U. ILL. L. REV. 421, 423 (2001).

207 *See* Paris Convention, *supra* note 203.

208 *Id.* art. 10.

In 1967, the World Intellectual Property Organization ("WIPO") was established by a convention to administer international unions related to intellectual property, including the Paris Convention, and to protect the interests of intellectual property worldwide.[209] The WIPO defines intellectual property broadly to include rights related to any inventions or industrial property or designs, affording protection against unfair competition and "all other rights resulting from intellectual activity in the industrial, scientific, literary, or artistic fields."[210]

The Trade-Related Aspects of Intellectual Property Rights Agreement ("TRIPS"), a product of the Uruguay Round of GATT in 1994, requires member countries to protect against acquisition, disclosure, or use of a party's trade secrets "in a manner contrary to honest commercial practices."[211] "Honest commercial practices" are further specified in footnote 10 as including 'breach of confidence,' but the definition does not include the unlawful taking of proprietary information.[212] Although the TRIPS specifically refers to "confidential information" rather than trade secrets, it defines such information as having commercial value, not being in the public domain, and being subject to "reasonable steps under the circumstances" to maintain its secrecy.[213] Under Article 39, the protection of "undisclosed information" is mandated by the TRIPS Agreement in the framework of the discipline of "unfair competition."[214] The TRIPS agreement protects trade secrets, not as individual intellectual property, but as a prohibition against unfair competition.[215] Furthermore, it provides an enhanced enforcement mechanism through the WTO's Dispute Settlement Body ("DSB") as well as other remedies.[216]

---

209 Convention Establishing the World Intellectual Property Organization, July 14, 1967, 21 U.S.T. 1749, 828 U.N.T.S. 3 [hereinafter WIPO Convention].

210 *Id.*

211 Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 [hereinafter TRIPS Agreement].

212 *Id.* at fn 10.

213 *See* TRIPS Agreement, *supra* note 211, Annex 1C.

214 *See* TRIPS Agreement, *supra* note 211, art. 39.

215 Jacques Combeau, *Protection of Undisclosed Information*, *in* INTELLECTUAL PROPERTY & INTERNATIONAL TRADE: A GUIDE TO THE URUGUAY ROUND TRIPS AGREEMENT 58, 58 (Tania Saulnier et al. eds., 1996).

216 *See* TRIPS Agreement, *supra* note 211, arts. 41, 64.

TRIPS, however, provides members with a broad exception to its obligations, permitting members to adopt contrary national laws if necessary to protect "sectors of vital importance to their socio-economic and technological development, which may allow countries to avoid specific prohibitions against economic espionage."[217] There is no international consensus that TRIPS protects trade secrets against espionage conducted by a foreign state. The key issue for the application of Article 39.3 of TRIPS is to determine what is the nature and extent of the obligation to protect "against unfair commercial use."[218]

Without clarity about whether TRIPS covers economic espionage, the question is whether any international legal principles exist that would prohibit states from conducting such activities. The next section will focus on the norm of non-intervention, assessing whether that norm would prohibit economic espionage.

III. Intervention as an International Wrongful Act Under International Law

Legal scholarship to date has focused on interventions into the domestic affairs of states through *forcible* coercive influence and not on lesser intrusive forms of intervention, such as economic or political interference.[219] Yet the norm of non-intervention as applied to *non-forcible* efforts is assumed to be a legal obligation and not merely an aspirational goal.[220] Whether in defense of actions or in response to alleged interference in a state's internal affairs, this norm is often invoked by states. Despite this, how the norm actually applies to non-forcible conduct by states has been inadequately addressed by legal scholars and poorly understood by state decision-makers. Legal opinion diverges over the scope of the non-intervention rule, raising doubt over the parameters of the duty not to intervene and the alleged right under certain

---

217 *Id.* art. 8.

218 *See* TRIPS Agreement, *supra* note 211, art. 39.

219 Lori Fisler Damrosch, *Politics Across Borders: Non–intervention and Nonforcible Influence over Domestic Affairs*, 83 AM. J. INT'L L. 1, 3 (1989) ("Indeed, the prevailing viewpoint until well into the 20th century was that the international legal concept of intervention concerned itself only with the use or threat of force against another state and not with lesser techniques.").

220 *See* Fidler, *supra* note 49.

circumstances to intervene.[221] Drawing distinctions between which types of intervention by state actors might be acceptable under what particular circumstances has proven a daunting task for legal experts.[222]

Certainly, under the U.N. Charter, coercive acts that rise to the level of use of force, which includes acts that cause physical damage or injury, are irrefutably unlawful. However, under the traditional interpretation of the language of the Charter, those uses of forces that are prohibited exclude economic or political sanctions. In some situations, however, intervention in the form of economic coercion may entail conduct in breach of rules of customary international law, such as certain forms of expropriation or discrimination.[223] On the other hand, there are situations when specific treaty obligations or rules of customary international law cannot be invoked with necessary detail, requiring a vaguer concept of "economic coercion."[224] The challenge is to attach meaningful criteria to the concept of economic coercion so that states may better assess their legal obligations under the norm as well as their rights in response to wrongful interventions.

Particularly in the case of cyber economic espionage, or cyber-enabled theft of IP, there is a need to provide more context to the norm as it exists under international law in order for it to be effective as a legal principle to counter the present day threats in cyberspace. This Part of the Article seeks to provide more insight into the specific elements of the norm of non-intervention as it relates to economic espionage as a form of coercive economic interference.

A. Non-Intervention and the Nicaragua Case

In 1986, the International Court of Justice ("ICJ") provided much welcomed clarity to the norm of non-intervention in its decision in the *Nicaragua* case, drawing an explicit distinction between "uses of force" and "interventions."[225] The Court found that a "use of force" is a "particularly obvious example" of an unlawful intervention, but clearly not the only form of

---

[221] *See supra* note 18 and accompanying text.
[222] *Id.*
[223] MCDOUGAL & FELICIANO, *infra* note 255, at 266.
[224] *See* Lillich, *infra* note 308, at 234-40.
[225] Nicaragua, *supra* note 176, ¶ 205.

intervention.[226] The *Nicaragua* Court's decision has greatly contributed to the development of the principle of non-intervention by confirming non-intervention's customary status.[227] Drawn heavily from U.N. General Assembly declarations and the general prevalence of non-intervention provisions in other international agreements, this part of the Court's decision on the use of force and intervention provides an authoritative statement of the law in this area and is uncontroversial.[228] Indeed, the customary rules of international law relating to both forcible and non-forcible intervention are now recognized as existing alongside the general prohibition on the use of force, but remain separate from that prohibition codified in the U.N. Charter.[229]

Clearly, the U.N. Charter prohibits international intervention through the use of armed force in Article 2(4), but it "withholds comment on other, more subtle forms of 'subversive' coercion that do not involve, at the very least, a perceived threat of armed force."[230] Scholars assert that the Charter's framers failure to explicitly adopt language related to a duty of states not to intervene in any manner in the domestic affairs of other states was in no way intended to legitimize intervention by states, noting that key principles within the Charter reflect implicit rights of states to be free from intervention as well as correlative duties to refrain from intervention.[231] Indeed, the U.S. and other states have asserted the acceptance of this principle in the Montevideo

---

226 *Id.*

227 *See id.*

228 *Id.* paras. 202, 204.

229 ADDISON WESLEY LONGMAN INC., OPPENHEIM'S INTERNATIONAL LAW § 128 (Robert Jennings & Arthur Watts eds., 9th ed. 1996) ("While the customary rules of international law relating to intervention have now to a considerable extent to be considered alongside the more general prohibition of the use or threat of force, intervention is still a distinct concept.").

230 Joyner & Lotrionte, *supra* note 8, at 846.

231 *See* Damrosch, *supra* note 219, at 8 ("[S]everal key principles of the Charter reflect implicit rights of states to be free from intervention on the part of other states and correlative duties to refrain from intervention."); TALLINN MANUAL, *supra* note 6, at 44 ("Although not expressly set out in the United Nations Charter, the prohibition of intervention is implicit in the principle of the sovereign equality of States laid out in Article 2(1) of the United Nations Charter."). *See generally* HANS KELSEN, THE LAW OF THE UNITED NATIONS 770 (1950) ("An obligation of the members to refrain from intervention in domestic matters of other states is not expressly stipulated by the Charter but is implied in the obligation established by Article 2, paragraph 4.").

Convention of 1933 as well as other treaties.[232] The norm has also been endorsed by other groups of states.[233] The norm of non-intervention would therefore be accepted as customary international law, binding on all states.

In ruling on the issue of intervention, the *Nicaragua* Court examined both the prohibition on intervention and the scope of the prohibition of the use of force.[234] In elaborating on the content of these two sets of rules and the relationship between them, the Court relied on the principles codified in the Declaration on the Principles of International Law Concerning Friendly Relations and Cooperation Among States, which affirms a duty on states "not to intervene in matters within the domestic jurisdiction of any State, in accordance with the [U.N.] Charter."[235] As additional authority for the principle of non-intervention, the Court invoked the *Corfu Channel* case, other General Assembly resolutions, including the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, and inter-American practice.[236]

---

232 Convention on Rights and Duties of States (inter-American) art. 8, Dec. 26, 1933, 49 Stat. 3097, 165 L.N.T.S. 19 ("No state has the right to intervene in the internal or external affairs of another.") *See also* Charter of the Organization of American States art. 19, *opened for signature* Mar. 30, 1948, 2 U.S.T. 2394, 119 U.N.T.S. 3 (closed for signature May 2, 1948) ("No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. The foregoing principle prohibits not only armed force but also any other form of interference or attempted threat against the personality of the State or against its political, economic, and cultural elements.").

233 Conference on Security and Co-operation in Europe, Final Act part VI, Aug. 1, 1975, 14 I.L.M. 1292 ("[P]articipating States will refrain from any intervention, direct or indirect, individual or collective, in the internal or external affairs failing within the domestic jurisdiction of another participating State" including "any other act of military, or of political, economic or other coercion . . . ."). In China, the principle of mutual noninterference in internal affairs is one of the "Five Principles of Peaceful Coexistence" espoused by the Chinese government and codified in the Sino-Indian Trade Agreement of 1954. *See* JEROME ALAN COHEN & HUNGDAH CHIU, PEOPLE'S CHINA AND INTERNATIONAL LAW: A DOCUMENTARY STUDY 156-57 (1974).

234 Nicaragua, *supra* note 176, ¶ 192 (citing G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/8082, at 121 (Oct. 24, 1970)).

235 Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/8082, at 121 (Oct. 24, 1970).

236 Nicaragua, *supra* note 176, ¶ 203 (citing G.A. Res. 2131 (XX), at 12, U.N. Doc. A/RES/20/2131 (Dec. 21, 1965)). In the *Corfu Channel* case, the ICJ declared that "the

Notably, the ICJ insisted that the principle of non-intervention has a separate, independent identity as a norm of customary international law.[237] It follows therefore, that the principle of non-intervention may vary between treaty-based expressions and what is found in customary international law.[238] Thus, developments in interpretation and application to treaty-based understandings of non-intervention may not necessarily apply to customary understandings of the non-intervention norm. And, customary international law on the norm may be different in context from that norm as codified in the treaties. Certainly, those treaties that implicate a norm of non-intervention should be regarded as complementing and informing the context of the customary international norm, but they should not be viewed as displacing the customary non-intervention norm.

This Article argues that economic espionage, as a highly intrusive coercive act into the economic and political freedoms of a state, may constitute a wrongful act of intervention in violation of the customary norm. In addition to this customary norm, there are also independent treaty instruments that are also implicated by economic espionage, as noted earlier.[239] Those treaties should not be read to replace the fundamental norm of non-intervention when assessing the legality of coercive acts through whatever method is used, including economic instruments of theft of IP through cyberspace. Furthermore, as a matter of customary international law, it is questionable whether any treaty between parties, including the WTO Agreements and TRIPS, could "contract out" of customary international law, the international legal obligation not to intervene in the internal or external affairs of another state. This obligation exists side-by-side with the enumerated obligations within these treaties.

First, however, in order to assess whether a violation of the norm has taken place, a clearer understanding of the elements of the norm must be developed. Once we can assess what a non-forcible, wrongful intervention looks like in general, it may be

---

alleged right of intervention [was] the manifestation of a policy of force, such as has, in the past, given rise to most serious abuses and such as cannot . . . find a place in international law." *Corfu Channel* (U.K. v. Alb.), 1949 I.C.J. 4, 35 (Apr. 9).

237 *See Corfu Channel*, *supra* note 236.

238 *See supra* notes 223-224 and accompanying text.

239 *See* WIPO Convention, *supra* note 209.

possible to address the norm's applicability in the cyber context. The next section provides a further review of the legal elements of the norm as it has been understood through state practice.

B. Contents of the Rule of Non-Intervention as Applicable to Cyber Operations

1. Coercion

Under international law not all forms of intervention are prohibited, rather, "[i]ntervention is prohibited when it interferes in matters in which each state is permitted to decide freely by virtue of the principle of state sovereignty."[240] As a legal outgrowth of sovereignty and state territorial control, the norm of non-intervention prohibits states from coercively imposing their will on the internal and external matters of other states, whether in the physical realm or in cyberspace.[241] As the *Nicaragua* Court explained in discussing the content of the principles:

> [T]he principle forbids 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. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.[242]

Modern interpretation of customary international law also extends the principle to states' actions in cyberspace.[243]

Although this prohibition against intervention into other state's affairs has been central to the international legal framework that ensures international peace and security, the norm has often been violated and challenged as a norm of international law.[244] Although the fact of some variance from a norm does not

---

240 Joyner & Lotrionte, *supra* note 8, at 847.

241 Schmitt, *Cyber Operations*, *supra* note 8, ("Cyber operations into another State violate the principle of non-intervention, and accordingly qualify as internationally wrongful acts, when intended to coerce (as distinct from merely influence) the targeted State's government in matters reserved to that State.").

242 Nicaragua, *supra* note 176, ¶ 205.

243 Watts, *supra* note 185, at 5.

244 *See id.*

necessarily destroy the norm's legally binding character, this lack of complete compliance with the norm has made it particularly challenging to prove the content of the presumed rule of non-intervention and apply its delineations by testing it against states' known behavior.[245] Notably, however, when states have violated the norm, they have typically invoked arguments of legal exceptions to the prohibition and have not argued that the norm is no longer binding law.[246] Indeed, the presence of some violation of the rule is less troublesome if other states are actively protesting states that are violating the norm, imposing sanctions against the wrongdoing state, and not engaging in similar fashion of violating the norm.[247] Furthermore, legal scholars have recognized that although "cyberspace and cyber means present States with greater opportunities for intervention in other States' domestic and foreign affairs," the mere existence of a new medium through which states can conduct intervention "does not excuse violations of the principle in cyberspace."[248]

Just as a state's internationally wrongful physical act can constitute violations of the U.N. Charter, the laws of armed conflict, other obligations under international law based on treaties (e.g. Law of the Sea, WTO agreements), or customary international law (principles of sovereignty or non-intervention), so too can a state's actions in cyberspace constitute violations of various sources of international law.[249] Similarly, just as a state's physical interventions not rising to the level of a "use of force" can still be unlawful under international law, so too can a state's interventions through cyberspace, although not triggering Article 2(4) of the U.N. Charter, be unlawful.[250] As the *Tallinn Manual* noted, "[c]yber operations into another State violate the principle of non-intervention, and accordingly qualify as internationally wrongful acts, when intended to coerce (as opposed to merely

---

245 *Id.* paras. 106, 108-09 (addressing the existence of "established and substantial practice" in support of the principle of non-intervention and concluding that recent instances of conduct prima facie inconsistent with the principle of non-intervention did not change the legal character of the principle or its content).

246 *See infra* notes 451-458 and accompanying text.

247 *Id.* para. 210.

248 *Id.*

249 TALLINN MANUAL, *supra* note 6, at 29-30.

250 *Id.* at 44 ("In particular, a cyber operation may constitute a violation of the prohibition on intervention.").

influence) the targeted state's government in matters reserved to that State."[251] The assessment of the legality of such cyberspace interventions will depend on many circumstantial factors that need to be assessed on a case-by-case basis.

2. Level of Intensity of Coercive Acts

The principle of sovereignty is fundamental to understanding what actions constitute wrongful acts prohibited by the norm of non-intervention.[252] To constitute the types of intervention that is prohibited under international law, the acts must be coercive and must target those actions in which a state has a right of free choice.[253] In assessing the various ways in which a state's sovereignty can be violated under international law, including in cyberspace, it is useful to depict the different acts as existing on a spectrum of least intrusive to most intrusive into the affairs of a state.[254] In addressing state actions in the physical realm, scholars and commentators have elaborated on the notion of violations of sovereignty and acts of coercion in state relations as existing on a spectrum, focusing, at the most basic level, on the element of intrusiveness of the state actions in determining the legality of the actions.[255] At the highest end of the spectrum, the most intrusive

---

251 *Id.* at 30.

252 TALLINN MANUAL, *supra* note 6, at 15-18 (granting a state the right to regulate and maintain control over cyber activities and infrastructure within its own territory); CYBER CONFLICT STUDIES ASS'N, ADDRESSING CYBER INSTABILITY 16-17 (James C. Mulvenon & Gregory J. Rattray eds., 2012) ("Re-assertion of government sovereignty in cyberspace . . . derives from the realization that every switch, every router, every node in the network lies within the boundaries of a sovereign nation-state or travels over cable or satellite owned by a company governed by the laws of a sovereign nation-state.").

253 Rep. of the Int'l Law Comm'n, 53d Sess., Apr. 23-June 1, July 2-Aug. 10, 2001, U.N. Doc. A/56/10 at 180; GAOR, 56th Sess., Supp. No. 10 (Aug. 10, 2001) ("The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State . . . .").

254 *See* Gary D. Brown & Owen W. Tullos, *On the Spectrum of Cyberspace Operations*, SMALL WARS J. (Dec. 11, 2012, 5:30 AM), http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations.

255 *See, e.g.*, Rosalyn Higgins, *Intervention and International Law*, *in* INTERVENTION IN WORLD POLITICS 29, 30 (Hedley Bull ed., 1984) (arguing that factors beyond mere levels of intrusiveness are important in order to assess whether the act is sufficiently coercive to constitute intervention). McDougal and Feliciano incorporate a broader more complex analysis of the coercion involving multiple factors not only the accelerating or decelerating intensity of the actions but also the different objectives of the actions, different methods used to carry out the coercion, as well as the "changing conditions of a

actions, those deemed unlawful under international law, trigger the injured state's right to defend itself, thereby permitting the most intrusive measures against another state, namely force, in order to stop the violating state from taking these actions.

In the contest of kinetic force, for example, the use of military force to invade another state is at the highest end of the spectrum, usually referred to as "armed attacks." These clearly coercive actions against the rights of the target state are thus illegal under international law.[256] Under these circumstances, the state that has been invaded has the inherent, unilateral right to use force in self-defense.[257]

States can also violate another state's sovereignty by using less grave uses of force that would not necessarily constitute an armed attack.[258] For example, if, rather than sending in troops, a stare trains, arms, and equips rebels within another state, seeking to overthrow that state, such actions would constitute a use of force, even though they fall below the threshold of an armed attack on the spectrum, and would still be considered illegal.[259] In the context of cyber operations, the Stuxnet worm that destroyed centrifuges at the Iranian uranium enrichment facility at Natanz in Iran can be characterized as a use of force on such a spectrum, in violation of the UN Charter prohibition.[260] Although not an armed attack under the Charter, such an action would still be illegal, coercive, and in violation of the sovereignty of the state, but the level of intrusiveness is not as high as sending in armed troops with the requisite level of physical destruction, injury or death. Furthermore, according to the *Nicaragua* case, where a state

---

world arena." *See* Myres S. McDougal & Florentino P. Feliciano, *International Coercion and World Public Order: The General Principles of the Law of War*, 67 YALE L.J. 771, 779 (1958). In assessing the levels of coercion, McDougal & Feliciano suggested consideration of three factors: (1) the importance and number of values of the injured state affected, (2) the extent to which such values of the state were affected, and (3) the number of participants of the state whose values were affected. *Id.* at 783-84.

256 *Id.*

257 U.N. Charter art. 51.

258 *See* Nicaragua, *supra* note 176, ¶ 210.

259 *See id.*

260 TALLINN MANUAL, *supra* note 6, at 45; Catherine Lotrionte, *Cyber Operations: Conflict Under International Law*, Special Cyber Issue, GEO. J. INT'L AFF. (2012). State practice is not yet settled as to whether Stuxnet is considered a use of force or armed attack under international law. *See* David P. Fidler, *Was Stuxnet an Act of War? Decoding a Cyberattack*, IEEE SEC. & POL'Y 9, 56-58 (2011).

suffers a use of force that does not rise to the level of an armed attack, the injured state would not have the lawful right to use force in self-defense, even though other measures such as non-forcible countermeasures may be appropriate.[261]

As cyber scholars have contemplated, if cyber operations are assessed on a spectrum of actions ranging from least intrusive to most intrusive,[262] it is useful to think of state interventions in cyberspace as existing on a spectrum of coercive acts against one state where an offending state is in some way violating the rights of another state, particularly, the right to make certain decisions freely without being coerced.[263] Here, the spectrum can range from the least intrusive type of coercive intervention to the most intrusive type of cyber intervention.[264] Imagine the spectrum consisting, at the lowest level of intrusiveness, violations of a state's sovereignty, and at the highest level of intrusiveness, an armed attack against the state.[265] In between these two polar extremes are interventions and uses of force.[266] As in the physical realm, it is easy to assess the legality of cyber operations that are at the higher end of the spectrum as coercive and illegal under the

---

261 *See* Nicaragua, *supra* note 176, ¶¶ 187-201.

262 *See* Brown & Tullos, *supra* note 254. The authors discuss a potential spectrum of cyber operations to be used in assessing the legality of certain cyber operations and possible legal responses by states. At the lowest end of the spectrum are "access operations" that enable other cyber activities by providing unauthorized entry into a computer system. At the highest end are "cyber attacks" that have effects in the real world beyond the computer system, including damage, destruction, property, death, or injury to persons. In between these two extremes are "cyber disruptions" that would include the interruption of the flow of information or the function of information systems without causing physical damage or injury. *See id.*

263 McDougal & Feliciano, *supra* note 255, at 779 ("The factual process of coercion across state boundaries may be usefully described . . . in terms of certain participants applying to each other coercion of alternately accelerating and decelerating intensity, for a whole spectrum of objectives, by methods which include the employment of all available instruments of policy, and under all the continually changing conditions of a world arena."). Acknowledging the existence of a "broad spectrum of cyber operations," the *Tallinn Manual* discusses the assessment of cyber operations that range from the least intrusive types such as cyber exploitation that would not constitute per se a violation of the norm of non-intervention to those cyber operations such as Stuxnet that amount to a use of force. TALLINN MANUAL, *supra* note 6, at 45.

264 *Id.*

265 McDougal & Feliciano, *supra* note 255, at 796 ("The possible range is from the mildest to the most intense coercion, from minor damage to the prestige of the opponent state, for instance, to its permanent physical liquidation.").

266 *See* Brown & Tullos, *supra* note 254.

norm of non-intervention. For example, manipulating another state's election results through cyber means in order to dictate the winning party would be a coercive act impeding on that state's right to freely decide its own political system; a cyber operation equivalent to an armed attack would also lie on the higher end of the spectrum.[267] Cyber operations that fall below the use of force threshold, however, are more difficult to assess for legality under the criteria of "coercive" action for the norm of non-intervention.[268]

At times, the word "intervention" has been used generally to denote almost any act of economic interference by one state in the affairs of another; yet state practice in tolerating and encouraging transboundary economic activity shows that international law cannot be said to prohibit all external involvement in internal economic affairs, just as diplomatic engagement is not considered illegal interference.[269] The traditional formulation of intervention as "dictatorial interference" resulting in the "subordination of the will" of one sovereign to that of another is not sufficient in understanding the contours of prohibited interference.[270] Importantly, the *Nicaragua* Court employed a more specific standard than "dictatorial interference" in rendering its decision on what types of actions would rise to the level of prohibited intervention, noting that the specific target of the coercion must be that which the state has a right to decide freely; therefore, not all types of interferences are prohibited.[271] To illustrate, traditional espionage that entails the intrusion into the territory of another state to clandestinely collect information may constitute an "unfriendly act," but the mere collection of protected information does not constitute a coercive act in that it does not force the target state to change or forgo a policy on which it has the right to decide.[272]

---

267 TALLINN MANUAL, *supra* note 6, at 34.

268 *Id*. at 35 (discussing the relevance of context in assessing state cyber operations).

269 Quincy Wright, *Legality of Intervention under the UN Charter*, 51 Am. J. Int'l L. Proc. 79, 88 (1957) [hereinafter Wright, Legality of Intervention under the UN Charter].

270 OPPENHEIM, *supra* note 58, § 134 (formulating "dictatorial interference"); *see also* ELLERY C. STOWELL, INTERVENTION IN INTERNATIONAL LAW 317 (1921).

271 *See* Nicaragua, *supra* note 176, ¶ 205.

272 TALLINN MANUAL, *supra* note 6, at 44 ("It follows that cyber espionage and cyber exploitation operations lacking a coercive element do not per se violate the non-intervention principle. Mere intrusion into another State's systems does not violate the

In this way, economic espionage is distinguishable from traditional espionage in that economic espionage involves the theft of property of entities within a state that will disadvantage the state in the global trade market, negatively impacting the state's policies related to global trade.[273] Often, the resulting damage caused by the economic espionage will require the victim state to alter its domestic and international policies to stem the damage, thus making the economic espionage coercive in the manner intended by the *Nicaragua* Court, and therefore a wrongful act of intervention.[274] Although not all forms of cyber operations that involve political, economic, or ideological interference violate the non-intervention principle, coercive cyber economic espionage does.

To reiterate, lest one be misled into thinking that a state's use of economic instruments to carry out coercive acts against another may be lawful because of a lack military instruments, the *Nicaragua* Court clarified that the form of illegal intervention is not limited to military means but can take on different forms, since what makes the intervention unlawful is a coercive act "bearing on matters in which each state is permitted, by the principle of state sovereignty, to decide freely. One of these is the choice of a political, economic, social[,] and cultural system, and the formulation of foreign policy."[275] Any acts, whether in the physical realm or cyberspace, that are intended to eliminate or disadvantage another state's prerogatives in these matters, are prohibited by the norm of non-intervention.[276] In seeking to attack one of these elements and act coercively, a state may use different dimensions of its power to coerce, "the diplomatic, the ideological, the economic, and the military instruments."[277] Irrespective of what dimension of a state's power is used to coerce another state, such coercive acts are unlawful acts of intervention.

3. The Scale and Effects of the Coercive Acts

As discussed above, the violation of the principle of

---

non-intervention principle.").

[273] *See supra* notes 25-32 and accompanying text.

[274] *Id.*

[275] Nicaragua, *supra* note 176, ¶ 205.

[276] TALLINN MANUAL, *supra* note 6, at 45-47.

[277] McDougal & Feliciano, *supra* note 255, at 263-64.

intervention does not have to entail using force that would cause physical harm or damage.[278] Certainly, there must be an injury to the target state. But, it does not have to be the same type of injury a state would suffer from an armed attack, otherwise there would be no reason for the *Nicaragua* Court to distinguish between an intervention, a use of force, and an armed attack.[279] Furthermore, if the Court had meant that all prohibited interventions must entail physical harm, there would have been no need for the Court to distinguish between the different levels of recourse available to a state to respond to the wrongful actions.[280]

As the *Nicaragua* case made clear, there is considerable overlap between the rules on forcible intervention and the customary law codified in Article 2(4) on uses of force.[281] And while the Court in specific cases has equated a specific violation as both a use of force and an intervention, interventions can be actions that, while still illegal at times, fall short of reaching the gravity of constituting a use of force.[282] In short, although prohibited, not all interventions are uses of force. For example, in the *Nicaragua* case, the Court ruled that the U.S. indirect intervention into Nicaragua by "training, arming, equipping . . . military and paramilitary actions in and against Nicaragua" did not amount to an armed attack but was a use of force.[283] Furthermore, the Court ruled that the mere supply of funds to the contras by the U.S., while undoubtedly an act of intervention in the internal affairs of Nicaragua, did not in itself amount to a use of force.[284] The important implication, then, is that to violate the principle of non-intervention, the acts of a state need not involve physical coercion *or* force. Certainly, the easiest cases to identify as interventions and as such as violations of law are those cases of

---

278 TALLINN MANUAL, *supra* note 6, at 43-45 (finding that cyber operations into another state violates the principle of non-intervention, and qualify as internationally wrongful acts when intended to coerce the targeted state's government in matters reserved to that state even if damage does not occur). Other examples given of intervention by cyber operations would be manipulation of public opinion polls and bringing down the online services of a political party. *Id.* at 45.

279 *See* Nicaragua, *supra* note 176.

280 *Id.*

281 *Id.*

282 *See id.*

283 *Id.*

284 *Id.* ¶ 228.

uses of force such as the Stuxnet worm.[285] Such uses of force would also be an intervention. And since all uses of force are coercive *per se*, the intervention of Stuxnet was coercive and therefore in violation of the norm of non-intervention.[286]

If prohibited interventions can include acts not constituting uses of force, and not necessarily involving physical force, what then would constitute an act covered by the principle of non-intervention? In other words, what is the contour of those acts that are acts short of the threat or use of force involving a degree of coercion sufficient to trigger intervention? For example, the *Nicaragua* Court regarded the U.S. supply of funds to rebels who were conducting military and paramilitary activities against Nicaragua as "undoubtedly an act of intervention in the internal affairs of Nicaragua."[287] It follows then that there is a different level of coercion involved in acts in violation of the non-use of force norm as compared with acts in violation of the non-intervention norm, the former of greater scale and effects versus the latter of some lesser damaging scale and effect. For example, an illegal act of intervention could include impeding a state's sovereign authority by restricting the state's choice with respect to a course of action, or compelling a course of action, without involving any use of armed force.[288]

In the *Nicaragua* case, the Court's assessment of different levels of coercion distinguished between a use of force and armed attack based on the differing scales and effects of those actions.[289] In other words, the determination of what constitutes a use of force versus an armed attack goes beyond the mere intensity of the actions. Using the same method, based on scales and effects, to assess the difference between uses of force and interventions is also useful. Although a thorough review is beyond the scope of

---

285 There remains disagreement with the group of experts who wrote the TALLINN MANUAL on whether the Stuxnet cyber operation against the Iranian nuclear facility at Natanz qualified as an "armed attack" for purposes of Article 51 of the U.N. Charter. *See* TALLINN MANUAL, *supra* note 6, at 58.

286 *Id.* at 45 (addressing the issue of whether the Stuxnet-sponsoring state had a lawful right to use force in self-defense is beyond the scope of this article).

287 Nicaragua, *supra* note 176, ¶ 228.

288 *Id.* ("[T]he court considers that the mere supply of funds to the *contras*, while undoubtedly an act of intervention in the internal affairs of Nicaragua . . . does not in itself amount to a use of force.").

289 *See id.*

this Article, in assessing the scale and effects of espionage as coercive actions within a state, a variety of factors would be useful to consider: (1) the nature of state interests affected by the cyber intrusion; (2) the scale of effects the intrusion produces in the target state; and (3) the reach in terms of number of actors involuntarily affected by the cyber operation at issue.

If the law is clear in that prohibited intervention includes more than physical damage, then it is also true that a state's right to recourse is not limited to only instances when the injury suffered is physical damage. To conclude otherwise is to misinterpret the *Nicaragua* Court and the norm of non-intervention as it has developed under customary international law non–intervention.[290] Of course, what types of responses an injured state can lawfully carry out will vary depending upon the level of damage or intrusiveness into the affairs of the injured state. Such responses can also be viewed as existing on a spectrum.

4. Assessing the "Objective" of Coercive Acts

Understanding the purpose, motivation or objective of the intervening state may be one of the most important elements relevant in assessing the legality of a state's actions.[291] A state's objective in conducting coercive acts is centered on demanding that the target state accept certain terms with respect to specified policies, requiring it to alter its previous behavior.[292] Generally, the goal of coercive actions is to expand the values of the coercing state, its bases of power, and to weaken the bases of power or values of the target state.[293] This could include the demand to withdraw or abstain from a specific policy or the adoption of some

---

290 Some of the experts who wrote the TALLINN MANUAL took the position that sovereignty can be violated even when there is no damage caused, as in the case of the emplacement of malware designed to monitor a system's activities. TALLINN MANUAL, supra note 6, at 16.

291 McDougal & Feliciano, *supra* note 255, at 248-75. Bowett suggests focusing on the motive or purposes of the economic coercion, instead of the effect of economic coercion, in assessing its legality which would be more valuable. For instance, Bowett focuses on whether the accused state's acts were based on a purpose of causing injury to the target state versus advancing the economic interests of the acting state. Derek W. Bowett, *International Law and Economic Coercion*, 16 VA. J. INT'L L. 245, 248 (1975-1976).

292 *See* McDougal & Feliciano, *supra* note 255, at 248-75.

293 *See id.*

policy demanded by the coercive state. McDougal and Feliciano develop a number of relevant factors for evaluating these objectives, including: (1) the "consequences of the demands" ("the importance and number of the values affected, the extent to which such values are affected, and the number of participants whose values are affected"); (2) "the degree of participation in the sharing of the values demanded" (is it exclusive to only the state making the demands or are the demands inclusive, asserted on behalf of a greater number of other states?); (3) the extension or conservation of values (is the demanding state acting to defend its own values or to attack or acquire values of other state?); and (4) whether the actions are in support of or against international organizations (do the actions go against a decision made by an international organization or are they in support of decision from such a group?).[294]

To apply these factors in assessing the legality of state-sponsored theft of trade secrets, one might consider the nature of the injured state's interests affected by the economic espionage (e.g. the injured state's losses of jobs, innovation and denial of access to the global marketplace), the scale of the effects or impact the espionage produces in the injured state (e.g. staggering losses to injured state's economy in jobs and innovation), and the reach in terms of number of actors involuntarily affected by the economic espionage (e.g. in addition to the direct effect on the individuals whose ideas are stolen, and whose jobs are lost, the global impact on other countries that will lead to loss in development). For instance, it would be incumbent upon a state alleging economic coercion to prove that the measures complained of had produced substantial economic harm to its own economy.[295] All instruments of a state's power, including economic instruments, can be used to conduct coercion under the criteria.[296] Therefore, coercion sufficient to constitute intervention may occur not only in military cyber operations but also through states'

---

294 One aspect of intelligence gathering most in accord with inclusive common interests is reciprocal collection of intelligence for security purposes. *See* MCDOUGAL & FELICIANO, *supra* note 255, at 251-56.

295 McDougal & Feliciano, *supra* note 255, at 266 ("The employment of economics as an instrument of coercive policy may, in broad statement, be described as the management of access to a flow of goods, services and money, as well as to markets, with the end of denying the target-state such access while maintaining it for oneself.").

296 *Id.*

economic cyber operations.[297] An obvious example of an economic technique with a coercive element would include "the taking, expropriation or confiscation of enterprises and property of nationals of the target country."[298]

Both in the cyber context and physical context, a mere intrusion into another state's networks to gather information would not violate the norm of non-intervention without some indication that such collection was used to coercively influence the target state.[299] The element of analysis is the purpose or objective of the collection.[300] The element of "coercion, like all facets of [a] case, [has] a contextual and goal-sensitive relevance[.]"[301] Conclusions as to the legality of the actions will be drawn in terms of these factors rather than in terms of coercion alone.[302]

If the coercive element is lacking, the prohibition on intervention has not been violated.[303] For example, with traditional espionage, even when it involves the collection of economic intelligence, although such actions may violate the general territorial sovereignty of the target state, such actions do not violate the norm of non-intervention without the coercive element.[304] On the other hand, if such an intelligence collection operation was part of a campaign to assist a resistance or opposition movement's efforts to influence the political events in the target state similar to the U.S. financial assistance to the rebels in Nicaragua the collection (whether through cyber means or physical) would be a violation of the norm of non-intervention.[305] Additionally, an intelligence operation would be a violation of the norm of non-intervention if the theft of information was used to

---

297 *Id.*

298 *Id.* at 267.

299 TALLINN MANUAL, supra note 6, at 44 ("[C]yber espionage and cyber exploitation operations lacking a coercive element do not per se violate the non-intervention principle. Mere intrusion into another State's systems does not violate the non-intervention principle.").

300 *Id.* at 45.

301 McDougal et al., *supra* note 4, at 419.

302 *See id.*

303 *See* NILS MELZER, CYBER WARFARE AND INTERNATIONAL LAW (2011); Jason J. Jolley, *Article 2(4) and Cyber Warfare: How do Old Rules Control the Brave New World?*, 2 INT'L L. RES. 1 (2013).

304 *See* MELZER, *supra* note 303; Jolley, *supra* note 303.

305 *See* MELZER, *supra* note 303; Jolley, *supra* note 303.

destabilize the economy of the target state and preventing the state from regulating its own economy.[306]

5. Assessing the Legality of Coercive Economic Acts

There are types of economic coercion that exist that may be socially, economically, and politically undesirable given the current state of development of the international legal order.[307] This does not mean, however, that they necessarily violate international law. Indeed, economic competition has been a fact of international law for years.[308] Many have questioned whether certain state actions affecting trade may actually be illicit under international law "when directed against a particular country or countries for purposes of diplomatic pressure."[309] Courts and commentators have considered whether economic acts by states may constitute prohibited uses of force or intervention.[310] In drafting the U.N. Charter, only a small handful of states in the U.N. ever considered that Article 2(4) of the U.N. Charter was meant to cover economic coercion.[311] The consensus has been that Article 2(4) should not be interpreted to cover economic

---

306 Most commentators agree that espionage, whether through cyber or traditional means, would not constitute a use of force for purposes of U.N. Charter, Art. 2(4). Most commentators also do not assert that economic espionage would be equivalent to an armed attack under the U.N. Charter, unless the requisite scales and effects of the *Nicaragua* case would be met. *See* Nicaragua*, supra*. note 176; MELZER, *supra* note 303; Jolley, *supra* note 303.

307 *See* SCHWEIZER, *supra* note 1, at 15.

308 Richard B. Lillich, *Economic Coercion and the "New International Economic Order": A Second Look at Some First Impressions*, 16 VA. J. OF INT'L L. 233, 234 (1976) ("Economic competition – indeed, even economic warfare – between Sates has been a fact of international life at least since the Peace of Westphalia (1648).").

309 J. Dapray Muir, *The Boycott in International Law*, 9 J. INT'L L. & ECON. 187, 192 (1974).

310 Some commentators have contended that economic coercion may fall within the provisions of article 2(4). *See* Hartmut Brosche, *The Arab Oil Embargo and United States Pressure Against Chile: Economic and Political Coercion and the Charter of the United Nations*, 7 CASE W. RES. J. INT'L. L. 3, 23 (1974) ("[O]ne has to bear in mind that the United Nations Charter is no historical monument, but a living instrument which continues to expand due to the dynamic and progressive nature of our international society whose prime objectives [sic] is still the maintenance of peace and security.").

311 Rep. of the Special Comm. on Friendly Relations, 24 UN Doc. A/7619; GAOR, 24th Sess., Supp. No. 19, 12 (1969). A few writers have argued that article 2(4) of the UN Charter prohibiting the use of force should not be limited to armed force but should be read to include economic coercion as well. *See* Jordan J. Paust & Albert P. Blaustein, *The Arab Oil Weapon-A Threat to International Peace*, 68 AM. J. INT'L L. 410 (1974).

coercion.[312] However, this still leaves open the possibility that certain economic activities of a state may violate other Charter norms and customary principles. In fact, economic conduct was covered by two U.N. General Assembly declarations, providing support for regulating economic coercion under the duty of non-intervention.[313] Although not legally binding, these General Assembly resolutions are authoritative in that they reflect the expectations of the international community and therefore cannot be dismissed.[314]

In the *Nicaragua* case, Nicaragua alleged that the U.S. had ceased economic aid to Nicaragua in order to inflict economic damage and to weaken the Nicaragua political system.[315] Specifically, the U.S. had reduced a sugar import quota by ninety percent and later instituted a trade embargo.[316] In considering the allegations, the Court ruled that neither act constituted a breach of the customary law principle of non–intervention.[317] In assessing the decision based on the necessary element of coercion, it follows that a sugar quota reduction in these circumstances would not be an intervention, for it did not coerce Nicaragua in any significant

---

312 *See* D.W. BOWETT, SELF-DEFENSE IN INTERNATIONAL LAW 148 (1958) ("Taking the words in their plain, common-sense meaning, it is clear that, since the prohibition is of the use or threat of force, they will not apply to economic or political pressure, but only to physical, armed force."). Publicists support this position relying on the rejection at San Francisco in 1945 of a Brazilian proposal to extend the prohibition of article 2(4) to cover "economic measures" as well as the rebuffs in the UN of subsequent attempts to achieve this result by interpretation. *See* Brosche, *supra* note 310, at 19-23.

313 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, GA Res. 2131, UN Doc. A/6220, GAOR, 20th Sess., Supp. 14, 12, (Dec. 21, 1965) (stating the declaration condemns a state's "use of economic, political or any other types of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind"); s*ee also* Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States, GA Res. 2625, UN Doc. A/8028, 25th Sess., GAOR, Supp. 28, 121 (1970).

314 "Obviously, these formulations of the concept of economic coercion, resting as they do on resolutions of the General Assembly, lack the normative quality of a treaty provision. They are, however, indicative of the gradual acceptance of a concept whose influence cannot be ignored." Bowett, *International Law and Economic Coercion*, *supra* note 291, at 246.

315 *See* Nicaragua*, supra* note 176.

316 *Id.*

317 *Id.*

manner, but rather altered unilateral preferential treatment.[318] And while such preferential economic treatment on behalf of the U.S. toward Nicaragua could violate other trade treaty agreements, it would not involve the type or level of coercion anticipated by the norm of intervention.[319]

As Derek Bowett has noted, "various reformulations of the traditional concept of non–intervention over the past dozen years reflect the consensus that economic coercion actually is regulated by this duty."[320] International law does prohibit certain types of economic coercion.[321] For instance, acts of economic coercion are prohibited when used for political motives.[322] Examples of prohibited economic coercion could include sanctions so crippling as to undermine the economic foundations for the exercise of political freedoms, an economic blockade, or other forcible efforts to prevent a state's participation in global markets. In such cases, the acting state does not have the prerogative to deny the other state the ability to exercise political freedom or to trade in the international market place.[323] In line with the *Nicaragua* case, it is one thing for a state to distance itself economically from a regime that it dislikes, and another to inflict gratuitous economic harm on another state, whether through economic blockades or the systematic theft of intellectual property. Such economic coercion targets the independence of the states, and can produce a general deterioration in world trade and financial stability, and, in extreme cases, may create a threat to world peace.[324]

For example, in the case of China stealing the IP of U.S. companies, China's actions are depriving those companies of market access, thereby depriving the U.S. its right to lawfully and

---

[318] *Id.*

[319] *See* Nicaragua, *supra* note 176, at 126.

[320] Richard B. Lillich, *The Status of Economic Coercion Under International Law: United Nations Norms*, 12 TEXAS INT'L L. J. 17, 20 (1977).

[321] *See* Lillich, *Economic Coercion and the "New International Economic Order*," *supra* note 308. Derek Bowett suggested characterizing unlawful economic measures by their intent rather than their effect. *See* Bowett, *Economic Coercion and Reprisals by States*, 13 VA. J. INT'L L. 1, 5 (1972) ("In other words, measures not illegal per se may become illegal only upon proof of an improper motive or purpose.").

[322] Bowett, *International Law and Economic Coercion, supra* note 291, at 249 ("[I]t does not suggest that it is lawful to cause injury to another State by economic coercion when the motive is to further or protect the State's *political* interests.").

[323] *See* Conference on Security and Co-operation in Europe, *supra* note 233.

[324] *See supra* notes 25-32 and accompanying text.

fairly participate in global trade.[325] In modern society, a state's ability to secure its sovereignty depends on control of its economy and private sources of wealth. Such activity is unlawful because it interfers with the normal lawful user of the global trade market, and not because it is an act of intelligence gathering.[326] Intelligence gathering in general, as discussed earlier, is not unlawful. To illustrate, intelligence gathering operations on the high seas are accepted under international law as long as the means used do not interfere with other lawful uses of the oceans by others.[327] However, if for example a permanent tower were erected for intelligence collection purposes in a customary sea-lane for international passage, creating a disturbance of the normal lawful user of the seas, such an act would be delictual. This is not because intelligence gathering on the high seas is unlawful *per se*, but because of the interference with the normal lawful use of the seas.[328] In this way "a lawful act of intelligence gathering is transformed into a delictual deprivation of others' use of the high seas."[329] In the same way, cyber espionage is not *per se* unlawful under international law. However, if a state steals the wealth of another state by cyber espionage, depriving the target state of exclusive control of its economic space, interfering in the lawful function of a state to innovate and develop economically, and causing the state concrete harm, that state has deprived the target state of a right and has therefore conducted a wrongful act.

C. State Responsibility

Pursuant to the law of state responsibility, states bear "responsibility" for their actions that constitute an internationally wrongful act.[330] The law of state responsibility also extends to

---

325 *See* U.S. INT'L. TRADE COMM., CHINA: EFFECTS OF INTELLECTUAL PROPERTY INFRINGEMENT AND INDIGENOUS INNOVATION POLICIES ON THE U.S. ECONOMY, 1-1 (2011).

326 *See id.*

327 When states have objected to or acted against the intelligence collection ships of other states at sea it is usually on the basis of claims of territorial penetration or self-defense and not in terms of the unlawfulness of intelligence collection on the high seas. McDougal et al., *supra* note 4, at 393.

328 *Id.*

329 *Id.*

330 Gabcikovo-Nagymaros Project (Hung./Slovk.), 1997 I.C.J. 92, ¶ 47 (Sept. 25); Nicaragua, *supra* note 176; *Corfu Channel*, *supra* note 236, at 23.

states' actions in cyberspace.[331] For those wrongful acts that an "injured" state suffers, remedial countermeasures within the law of state responsibility are available to the injured state in order to compel or convince the state conducting the wrongful act to stop.[332] The *Tallinn Manual* recognized that "a victim state is entitled to take proportionate measures to end harmful ongoing cyber operations if the state of origin fails to meet its obligations to end them."[333] An injured state, and only the injured state,[334] can resort to countermeasures only if there has been a breach of an international obligation owed to the state and the wrongful act can be attributed to the state in question.[335]

Therefore, to establish state responsibility for certain acts of economic espionage as internationally wrongful acts of a state, it is not enough to qualify such actions as a breach of an international legal obligation; the action must also be attributable to the state under international law.[336] When the military or intelligence agencies of the government are conducting economic espionage activities, the actions of those agencies or departments of the state are automatically attributable to that state.[337] In the case of

---

331 TALLINN MANUAL, *supra* note 6, at 29 (explaining in rule six that, "[a] State bears international responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation").

332 Gabcikovo-Magymaros Project, *supra* note 330, ¶¶ 82-83; Nicaragua, *supra* note 176, ¶ 249; *Naulilaa Incident Arbitration* (Port. V. Ger.), 2 RIAA 1011, ¶¶ 1025-26 (1928).

333 Schmitt, *The Law of Cyber Warfare*, *supra* note 6, at 277 (referring to the TALLINN MANUAL).

334 Nicaragua, *supra* note 176, ¶ 249 ("[T]he acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate counter-measures on the part of the State which had been the victim of these acts . . . . They could not justify countermeasures taken by a third state . . . ."); Rep. of the Int'l Law Comm'n, 53rd Sess., Apr. 23–June 1 and July 2–Aug. 10, 2001, U.N. Doc. A/56/10; GAOR; 56th Sess., Supp. No. 10, ¶ 76 (2001).

335 Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334, ¶ 68 (focusing on "intervention" as the wrongful act that is being conducted by China's economic espionage. There may be a separate claim of wrongful act also triggering the right to use countermeasures, the failure of China to take feasible measures to terminate harmful cyber operations originating in its territory can also constitute an internationally wrongful omission by China.); *see* Skinner, *supra* note 13.

336 Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334, at art. 2(a).

337 *Id.* art. 2 commentary; TALLINN MANUAL, *supra* note 6, at 31 ("Any cyber activity undertaken by the intelligence, military, internal security, customs, or other State agencies will engage State responsibility under international law if it violates an

economic espionage amounting to a wrongful act of intervention by the Chinese PLA members, the PLA members' actions can be attributed to the Chinese government as wrongful acts.[338] Therefore, the law of state responsibility is certainly implicated.[339] Furthermore, as discussed in Part III, the law of countermeasures requires that the state taking the countermeasures provide the wrongdoing state with notice of the intent to carry out countermeasures.[340] This would allow any target state the opportunity to provide evidence that it in fact was not the responsible party for the wrongful acts.[341]

If economic espionage is understood as a wrongful act under international law, then a state which controls, directs, acknowledges, or supports cyber espionage against another state may be held responsible under the international legal doctrine of state responsibility. Under the law of countermeasures, a victim state would then have the right to evoke countermeasures in response to acts of economic espionage.

D. Justifications for Intervention

The *Nicaragua* Court set forth the principle that there is no general right of intervention.[342] However, where a victim state establishes that a violation of the non-intervention norm occurred, the commission of an internationally wrongful act confers upon the victim state the legal right to demand cessation of the unlawful act, assurances as to non-repetition, and, if appropriate, reparations.[343] If the unlawful act continues, the victim state can

---

international legal obligation applicable to that State.").

338 TALLINN MANUAL *supra* note 6, at 30 ("The law of State responsibility is not implicated when States engage in other acts that are either permitted or unregulated by international law. For instance, international law does not address espionage per se. Thus, a State's responsibility for an act of cyber espionage conducted by an organ of the State in cyberspace is not engaged as a matter of international law unless particular aspects of the espionage violate specific international legal prohibitions.").

339 *Id.*

340 ARSIWA, *supra* note 53, arts. 52(1)(b), 43.

341 The state cannot argue that its agents were acting beyond its instructions in order to avoid responsibility for even so-called *ultra vires* acts trigger a states international legal responsibility if the organs of the state in fact breached international obligations. Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334 at art. 7.

342 *See* Nicaragua, *supra* note 176, ¶ 209.

343 Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334, art. 30-31.

employ countermeasures under customary international law.[344]

Importantly, international law has imposed limits upon the justifications for intervention such as countermeasures.[345] Before an intervening state acts under a justification argument, traditionally, international law has held that the victim state must first exhaust or deem ineffective non-coercive measures such as diplomacy, negotiation, mediation, or arbitration.[346] Much debate remains, however, over the requirement for states to refrain from coercive countermeasures until dispute resolution has been exhausted. Some scholars have observed that, "[i]t seems untenable that international rules require a government that is being subjected to an electronic attack – the results of which may inflict catastrophic social and economic damage on its society – to delay responding until the factual predicate or the intent of the perpetrators are made clear."[347] With respect to invoking countermeasures in response to China's economic espionage, it remains unresolved whether the U.S. would be required to submit a claim and await a decision by a WTO panel on China's actions before invoking countermeasures, or whether the U.S. would have the legal right to invoke and continue countermeasures until China stops its economic espionage.

IV. Methods for Enforcing Rights Against Wrongful Interventions

A. Countermeasures

In terms of responses to cyber operations that constitute wrongful interventions, states enjoy the right pursuant to the law of state responsibility to respond with proportionate countermeasures, that would themselves otherwise be unlawful. Today, the modern conditions for countermeasures are built on the principles outlined in the *Naulilaa* case and have been more recently elaborated by the International Law Commission (ILC).[348]

---

344 *Id.*

345 Wright, *Legality of Intervention under the UN Charter*, *supra* note 269, at 88.

346 *Id.*

347 Joyner & Lotrionte, *supra* note 8, at 853.

348 *Naulilaa Incident Arbitration*, *supra* note 332. This decision is generally considered to be the most authoritative statement of the customary law of reprisals. In 1947, pursuant to the UNGA mandate under the U.N. Charter, Art. 13(1)(a), the UNGA created the ILC and charged it with "the promotion of the progressive development of

The ILC adopted the term countermeasure in its work on state responsibility.[349] In the resulting ILC Articles,[350] a culmination of a forty-plus year effort by the ILC, countermeasures are among the defenses to a claim of state responsibility as long as they are conducted according to the principles outlined in the ILC Articles.[351] In December 2001, the UNGA adopted Resolution 56/83, which "commend[ed the articles] to the attention of Governments without prejudice to the question of their future adoption or other appropriate action."[352] The ILC Articles include seven articles setting out the legal principles for countermeasures. More briefly, countermeasures must be (1) aimed at the state that violated its obligations towards the injured state,[353] (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,[354] (3) terminated when the wrongdoing state has complied with its obligations,[355] (4) commensurate with the injury suffered and have

---

international law and its codification." G.A. Res. 174(II), U.N. GAOR, 2nd Sess., U.N. Doc. A/RES/174(II) (Nov. 21, 1947).

349 *See* JAMES CRAWFORD ET AL. (EDS.), THE LAW OF INTERNATIONAL RESPONSIBILITY 1127–1214 (2010) (discussing the work of the ILC in this context).

350 Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334, ¶ 68. The final articles, commentaries, prior drafts and an informational introduction by the last special rapporteur on state responsibility, all appear in JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY (2002) and James Crawford, *International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts*, 96 AM. J. INT'L L. 874 (Oct. 2002). The ILC Articles, although written in the form of articles in a treaty, are not a "source" of law but rather they are evidence of a source of law. Although not legally binding, the articles have been referred to in arguments before international tribunals, in arbitral decisions, in state practice, in separate opinions of the ICJ, and by international legal scholars. David D. Caron, *The ILC Articles on State Responsibility: The Paradoxical Relationship Between Form and Authority*, 96 AM. J. INT'L L. 857, 865 (2002). Ultimately, the final test of acceptance of these articles will be based on state practice. Some critics have warned against the articles being accepted as law today, noting that "[t]he ILC's work on state responsibility will best serve the needs of the international community only if it is weighed, interpreted, and applied with much care." *Id.* at 873.

351 *See* Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334.

352 G.A. Res. 56/83, ¶ 2, U.N. GAOR, 56th Sess., U.N. Doc. A/Res/56/83 (Jan, 28, 2002) [hereinafter ARSIWA].

353 *See* Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334, art. 49.

354 *See id.* art. 30-31.

355 *Id.* art. 53.

as their purpose to induce the wrongdoing state to comply with its obligations under international law.[356] In short, the prevailing view is that countermeasures cannot involve the use of force[357] or affect peremptory norms, fundamental human rights obligations,[358] humanitarian obligations prohibiting reprisals,[359] or obligations to respect the inviolability of diplomatic and consular agents, premises, archives and documents.[360]

1. On Proportionality

Countermeasures must also be proportionate, meaning "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[361] This type of proportionality, however, is distinguished from the proportionality requirement for self-defense actions in response to armed attacks.[362] According to the self-defense proportionality requirement, states' actions after, or in anticipation of, an armed attack must not exceed the amount of force necessary in order to stop the threat.[363] Countermeasures taken against a state for a wrongful action, however, must be equivalent in effects to the injury suffered by the state taking the

---

356 *Id.* art. 51; s*ee also* Gabcikovo-Nagymaros Project, *supra* note 330, ¶ 85–87. Thomas Franck has suggested, "[i]n assessing the acceptability of a response, the principle of proportionality allows those affronted by unlawful conduct to respond by taking into account the level of response necessary to prevent recurrences*."* Thomas Franck, *On Proportionality of Countermeasures in International Law,* 102 AM. J. INT'L L. 715, 765-66 (2008).

357 The position that countermeasures cannot involve the use of force has been challenged by some scholars and at least one ICJ judge. ICJ Judge Simma, in a separate opinion, in the Oil Platforms case argued that under some circumstances a state could use forcible countermeasures. Oil Platforms Case (Iran v. U.S.), Separate Opinion of Judge Simma, 2001 I.C.J. 333 (Nov. 6).

358 *See* Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334, art. 50(1)(b).

359 *Id.* art. 50(1)(c).

360 ARSIWA, *supra* note 53, art. 50(2)(b).

361 *Id.* art. 51. *Naulilaa Incident Arbitration*, *supra* note 332, at 1028. Being commensurate does not require that the countermeasures be of the same nature as the wrongful act that gave rise to the countermeasures. For instance, non-cyber countermeasures can be imposed by the U.S. in response to China's wrongful cyber actions of economic espionage. Although there is a preference for countermeasures of like kind, making it easier in assessing proportionality. Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334, art. 51 commentary.

362 *See generally* Rep. of the Int'l Law Comm'n, 53rd Sess., *supra* note 334, art. 51.

363 *See* Schmitt, *Cyber Operations, supra* note 8, at 19.

countermeasures.[364] A somewhat broader approach was taken in the *Air Services* case, which incorporated into the assessment of proportionate countermeasures an evaluation of the right involved in the wrongful act, stating "it is essential in a dispute between States, to take into account not only the injuries suffered by the companies concerned but also the importance of the questions of principles arising from the alleged breach."[365] Under this approach, one does not only assess the losses incurred by the injured state in determining what level of countermeasures would be proportionate, but also the "positions of principle" which are involved in the wrongdoing state's actions.[366]

To illustrate how the proportionality of countermeasures may be assessed in the case against China's economic espionage, one would determine not only the losses incurred to the U.S. from the theft of American IP, but also the principles at stake in the theft of the IP. As mentioned previously, estimated economic loss to the U.S. in both revenue and jobs is quite large.[367] According to a 2011 report by the U.S. International Trade Commission ("USITC"), "firms in the U.S. IP-intensive economy . . . spent approximately $4.8 billion in 2009 to address possible Chinese IPR infringement."[368] However, more is at stake with IP theft, which must be taken into consideration when judging the proportionality of countermeasures.[369] Maybe even more important than the effect on jobs and revenue from this type of theft, is its effect on the general principle of fair competition in the global marketplace. For as recognized, IP theft undermines "both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and new industries

---

364 ARSIWA, *supra* note 53, art. 51.

365 *Air Services Agreement, infra* note 380, ¶ 83.

366 *Id.*

367 In 2012 a Department of Commerce study found that IP protection affects an estimated 27 million American jobs, roughly 19% of the U.S. workforce. *See* ESA & USPTO, INTELLECTUAL PROPERTY AND THE U.S. ECONOMY: INDUSTRIES IN FOCUS (March 2012). A 2011 report by the U.S. International Trade Commission found that in 2009 alone, the theft of U.S. IP from China alone was equivalent in value to $48.2 billion in lost sales, royalties and license fees." *See* China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy, Inv. No. 332-519, USITC Pub. 4226 (May 2011) (Final).

368 *Id.* at 2-7, 2-21.

369 *See e.g.*, Schmitt, *Cyber Operations, supra* note 8, at 20 (discussing the complexity of proportionality determinations).

that can further expand the world economy and continue to raise the prosperity of all."[370] At the root, IP theft incentivizes unfair competition and undermines the values of the global trade regime.[371] These are fundamental values that have been endorsed in the WTO regime and through state practice.

2. Role for Private Entities: Taking Countermeasures or Targets of Countermeasures

Scholars disagree over whether private entities may legally impose countermeasures on their own initiative based on injuries they suffered from another state.[372] While countermeasures can only be imposed by states under international law, an injured state does has the right to rely on private sector capabilities in order to effectively impose countermeasures on the wrongdoing state.[373] However, by 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.[374] In other words, the private entities would also be required to follow the limitations established under international law for conducting countermeasures. Some have advocated for permitting private American companies to "hackback" under a theory of "transboundary harm," arguing that this approach would be more effective in getting China to desist in its economic espionage efforts targeting American companies.[375] Both under

---

370 THE IP COMMISSION REPORT, *supra* note 22, at 10.

371 *See supra* notes 272-274 and accompanying text.

372 Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. OF TRANSNAT'L. L. 275, 276 (2013) ("[S]tates have an obligation of due diligence to prevent significant transboundary cyberharm to another state's intellectual property . . . . [A]ffected states may be entitled to reciprocate by . . . allowing their victimized nationals to hackback."); *see also* Schmitt, *supra* note 6, at 23.

373 Zach West, *Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119 (2012).

374 *See* TALLINN MANUAL, *supra* note 6, at 33 ("A state may not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.").

375 Messerschmidt, *supra* note 372, at 320 ("As much as a state may be well equipped to engage in one-off cyber attacks in response to transboundary attacks, the sheer scope of transboundary cyberharm makes responses by the government simply unrealistic. In contrast to the state, however, private actors are better positioned to

U.S. domestic legal restrictions and the principle of countermeasures under international law, there would be specific legal restrictions involving the private sector.

While the wrongdoing states must be the object of any countermeasures the injured state takes, the specific targets of the countermeasures do not have to be the wrongdoing state or its organs.[376] For example, if, in response to China's economic espionage, the U.S. imposes reciprocal cyber economic espionage countermeasures with the objective of putting an end to the Chinese government's wrongdoing, by targeting Chinese companies that have technology worth stealing or those Chinese companies that benefitted from the stolen U.S. trade secrets, this would be allowed as long as the other limitations of countermeasures were followed.

3. Dispute Settlement Controversy: When Can a State Engage in Countermeasures?

As mentioned above, the ILC Articles did much to provide clarity to the use of countermeasures under international law. However, determining whether to include specific dispute settlement machinery regarding countermeasures in the ILC Articles was highly controversial during the drafting process.[377] Today, ambiguity exists between customary law and the ILC Articles as to when an injured state's right to carry out countermeasures begins and ends. The proposed dispute settlement requirements under the ILC Articles are separated into those required before resorting to countermeasures and those required after countermeasures have been taken.[378] Those opposed to including a mandatory pre-countermeasure dispute settlement process argued that such a requirement would allow a wrongdoing state to appear to be open to negotiations as a way to thwart the

---

respond to cyberharm.").

[376] Schmitt, *Cyber Operations, supra* note 8, at 9.

[377] *See* Daniel Bodansky & John R. Crook, *Symposium – The ILC's State Responsibility Articles – Introduction and Overview*, 96 AM. J. INT'L L. 773, 787 (2002) ("The proposed linkage between resort to countermeasures and compulsory dispute settlement was high controversial, not least because it permitted a target state to thwart the good-faith use of countermeasures through sham recourse to settlement procedures.").

[378] *See supra* Part III; *see also* ARSIWA, *supra* note 53, arts. 52(1)(b), 43.

legitimate use of countermeasures against them.[379] Viewed this way, the proposed articles could provide the wrongdoing state with an avenue to avoid its responsibility. This approach was rejected in the *Air Services Agreement* case when the tribunal assessed the French intransigence prior to the U.S. application of countermeasures, rejecting the need to exhaust all procedures before resorting to countermeasures.[380]

In the end, the ILC omitted any voluntary or compulsory dispute settlement procedures from the final text.[381] Instead, the ILC Articles compromised, requiring an injured state to give notice to a wrongdoing state and offer to negotiate before resorting to countermeasures.[382] However, the ILC Articles do not require that parties enter into negotiations before countermeasures are initiated.[383] These requirements are consistent with the goals of countermeasures: to return an escalating situation back to a state of lawfulness and stop the wrongdoing party's harmful actions.

However, this leaves much confusion about the actual law regarding countermeasures and how they relate to dispute settlement. For example, as the ILC Articles note, the obligations of notice and an offer to negotiate may not apply if "urgent countermeasures" are necessary to preserve the injured state's rights.[384] In the cyber context, it may be necessary to take immediate action in cyberspace in order to stop the target state's injury.[385] Ultimately, the injured state must draw the distinction between "urgent" countermeasures, which do not require notice and an offer to negotiate, and normal countermeasures, for which the ILC Articles' requirements apply. The true challenge will be whether international arbitral panels will be able to draw such a

---

379 *See* Daniel Bodansky, John R. Crook & David J. Bederman, *Counterintuiting Countermeasures,* 96 AM. J. INT'L L. 817, 824 (2002).

380 *See* Air Services Agreement Award (Fr. v. U.S.), 18 R.I.A.A. 416, 445 (1978) [hereinafter Air Services Agreement Award] ("[T]he Arbitral Tribunal does not believe that it is possible, in the present state of international relations, to lay down a rule prohibiting the use of counter-measures during negotiations, especially where such counter-measures are accompanied by an offer for a procedure affording the possibility of accelerating the solution of the dispute.").

381 *See* Bodansky & Crook, *supra* note 377, at 787.

382 *See supra* note 378.

383 *See* ARSIWA, *supra* note 53, arts. 43, 52(1).

384 *Id.* art. 52(2).

385 Schmitt, *Cyber Operations, supra* note 8, at 14.

distinction if the matter comes before them.

4. Required Dispute Resolution

As acknowledged by the ILC Articles, states are allowed to take immediate countermeasures that may be necessary to preserve the injured state's rights.[386] However, the 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,"[387] a requirement that applies only once the case is *sub judice*.[388]

As the *Air Services Agreement* arbitral panel recognized, even given a tribunal's power to decide on interim measures of protection, the "power of the Parties to initiate or maintain counter-measures, too, may not disappear completely."[389] It is likely that under some circumstances the effects of the forfeited wrongdoing actions may constitute an obligation to provide reparation. The question then is whether the injured state would be required to cease its countermeasures before the wrongdoing state paid reparations. The ILC Articles do not directly address this issue, but they seem to create an absolute bar to the maintenance of countermeasures once the offending conduct has ceased.[390] This does not appear to be aligned, though, with the holding in the *Air Services Agreement* that once a dispute is submitted to a tribunal that has the "means to achieve the objectives justifying the counter-measures," the right to initiate countermeasures is vitiated and those already in force "may" be "eliminated," but only to the extent that the tribunal can provide equivalent "interim measures of protection."[391] The court or tribunal therefore must enjoy the authority to order "interim measures of protection, regardless of whether this power is expressly mentioned or implied in its governing statute (at least as

386 *See* ARSIWA, *supra* note 53, at art. 52(2).

387 *Id.* at art. 52(3)(a); *id. at* art. 52, cmt 7.

388 Air Services Agreement Award, *supra* note 380, ¶ 95; *see also* ARSIWA*, supra* note 53, art. 52, cmt. 8 ("Paragraph 3 is based on the assumption that the court or tribunal to which it refers has jurisdiction over the dispute and also the power to order provisional measures.").

389 Air Services Agreement Award, *supra* note 380, ¶ 96.

390 ARSIWA*, supra* note 53, art. 52.

391 Air Services Agreement Award, *supra* note 380, ¶ 96.

the power to formulate recommendations to this effect)."[392] If, however, the court lacks authority or its ability is severely restricted, the injured state may retain the right to initiate or continue countermeasures.[393]

The international arbitral tribunals have not yet provided sufficient certainty to states about their ability to enforce provisional measures effectively. It is not clear whether the tribunals have the power to enforce provisional measures as effectively as countermeasures taken by injured states. Quite probably, even given the ICJ's ruling in the *LaGrand* case on the binding effect of provisional measures, governments remain doubtful about whether a system of tribunal or court-imposed provisional measures can ever be as effective as vigorous countermeasures.[394]

It is unknown how this language will be interpreted in the context of treaties that provide that state parties will be obliged to take their dispute to a dispute settlement body, rather than engage in unilateral countermeasures.[395] Relevant to the focus of this article, for example, there are provisions to this effect in the WTO treaty.[396] How might a state lawfully seek recourse to countermeasures while still complying with its obligations to an applicable dispute settlement procedure within another treaty like the WTO? This will be the focus of the discussion below.

Indeed, 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."[397] On this issue, the ILC Articles appear to provide a broader reading of the limitation on countermeasures with respect to dispute settlement than the arbitral panel in the *Air Services Agreement* case did. Indeed, the arbitrator observed, "it is [not] possible, in the present state of international relations, to lay down a rule prohibiting the use of counter-measures during

---

392 *Id.*

393 *See id.* ("As the object and scope of the tribunal to decide on interim measures of protection may be defined quite narrowly, however, the power of the Parties to initiate or maintain countermeasures, too, may not disappear completely.").

394 LaGrand Case (Ger. v. U.S.), Judgment, 2001 I.C.J. 466 (June 27).

395 ARSIWA, *supra* note 53, art. 50(2)(a).

396 *Id.*

397 *Id*. art. 52, cmt. 8.

negotiations . . . ."[398] It will be up to an injured state to weigh the effects of issuing countermeasures against the potential judicial decisions of an international body.

There remains the unresolved issue of whether dispute resolution must be exhausted before countermeasures are pursued, including under the WTO. As a general matter, countermeasures may not be taken when the dispute is subject to a dispute settlement procedure.[399] This is so even when the dispute resolution mechanism is contained in the treaty that the responsible state has breached.[400] In this way, states are seen to have voluntarily decided to relinquish their right to countermeasures when they sign a treaty that includes a requisite dispute settlement procedure. What this means for whether and how a state may employ countermeasures in order to get a state to comply with its legal obligations not to conduct coercive intervention remains uncertain under international law.

While the dispute settlement provisions of the WTO may impose certain restrictions on the types of measures a state could take in response to economic espionage, this Article has proposed that the duty of a state not to intervene into another state to steal intellectual property has developed as a distinct international obligation outside of the treaties that states have signed under the WTO. This obligation stems from the norm of non–intervention and prohibition of coercive actions against the areas in which states have sovereign freedoms.[401] If a state breaches an international obligation, such as the norm of non–intervention, the target state may use unilateral countermeasures to enforce compliance with the law, to return the situation to a lawful position.[402] Even if a specific norm against economic espionage *per se* has not yet ripened into "hard law" through sufficient state practice, a state could use countermeasures to stop the intervening state because that is consistent with values the international community recognizes, and it does not intrude upon solely domestic matters. In other words, it would be acceptable for the

---

398 Air Services Agreement Award, *supra* note 380, ¶ 92.

399 ARSIWA, *supra* note 53, art. 50(2)(a).

400 Jurisdiction of the ICAO Council (India v. Pak.), Appeal, 1972 I.C.J. 46, ¶ 16 (Aug. 18).

401 *See supra* notes 320-324 and accompanying text.

402 *See* U.S.-Cotton Yarn, *infra* note 444, ¶ 120

U.S. to employ countermeasures to urge China to stop stealing trade secrets and comply with the fair trading principles that have been accepted by the international community.

V. The WTO Option- Bringing a Claim to the WTO for Espionage

This Part considers how the WTO rules of international trade may operate alongside the customary norm of non–intervention in providing an institutional mechanism for victim states in cases of economic espionage. In cases where one state can establish illegal economic conduct by another under the commitments of a signed treaty, such treaties afford a sounder basis for resolving disputes among states party to the treaty. Accordingly, the WTO appears to be an appropriate forum to consider disputes over economic espionage. Much of the success of the Uruguay Round negotiations is attributed to the States (WTO members) agreeing to construct a more rule-based international trading system primarily through the present dispute settlement system.[403] A qualified success, WTO dispute mechanisms have seen more than 339 settlement reports and arbitration awards issued by the organization's dispute body from 1995 through 2011.[404] The U.S. has participated in 140 of these disputes.[405]

As some have encouraged, it may be that given the level of damage to the U.S. from IP theft, the U.S. government is willing to take the next step, by bringing a complaint before the WTO under TRIPS. Some observers have proposed that the U.S. seek resort to the WTO, implying that economic espionage is outlawed under TRIPS.[406] If in fact the U.S. was to bring such a claim and the

---

403 *See* Faculty of Law, Univ. of Leicester, *Uruguay Round Results. A European Lawyer's Perspective*, 21(4) EUR. L. REV. 339, 339 (1996) ("The new dispute settlement understanding (DSU) is singled out . . . as the greatest innovation of the new trade order and as indicative of a shift from a power-oriented to a rule-oriented system.").

404 THE IP COMMISSION REPORT, *supra* note 22, at 19.

405 *Id.*

406 *See* Richard A. Clarke, *A Global Cyber Crisis in Waiting*, WASH. POST (Feb. 7, 2013), http://www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html ("[N]ations ought to be able to agree on something they all appear to practice already: forswearing cyberattacks that alter or destroy the networks of financial institutions."); JAMES A. LEWIS, CONFLICT AND NEGOTIATION IN CYBERSPACE 1 (CSIS, Feb. 2013) ("U.S. interests are best served by embedding cyberattack and cyber espionage in the existing framework of international law, and long-term U.S. interests are best served by winning international agreement to

issue is decided on the merits, there are two primary challenges the U.S. would face based on lack of clarity in the law. The first is whether the WTO agreements, such as TRIPS, cover economic espionage and thus prohibit WTO members from conducting economic espionage in the territory of another WTO member. The second is if in fact economic espionage is implicated by the WTO agreements, whether a complaining state is bound to use a WTO DSB mechanism in lieu of unilateral self-help mechanism of countermeasures, as previously outlined in this Article.[407]

As others have accurately pointed out, "WTO rules create obligations for WTO members to fulfill within their territories and do not generally impose duties that apply outside those limits."[408] Therefore, according to this interpretation of TRIPS, the principles incorporated into that treaty do not apply to extra-territorial espionage.[409] Although the U.S. has indicated some interest in pursuing a claim against China for economic cyber espionage through the WTO,[410] to date, no such claim has been brought.[411] Indeed, the central point is that it may prove difficult to establish noncompliance by China under the terms of the treaty and enforce the agreement for allegations of economic espionage, considering the lack of many decisions by the WTO on legal interpretations of the TRIPS agreement and existing ambiguity in many of the

---

this.").

407 *See infra* Part IV-C.

408 Fidler, *supra* note 49, at 3 ("The desire to combat economic cyber espionage confronts a lack of international law on espionage and economic espionage" and the general "participation in, and tolerance of, spying.").

409 David P. Fidler, *Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage*, ARMS CONTROL LAW (Feb. 11, 2013), http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/ (pointing out that TRIPS deals with a "WTO member's behavior within its own territory towards nationals of other WTO members doing business in that territory").

410 *See* Siobhan Gorman, Devlin Barrett & James T. Areddy, *U.S. to Rev Up Hacking Fight*, WALL ST. J. (May 23, 2014, 7:46 PM), http://online.wsj.com /news/articles/SB10001424052702303749904579580453314299412 ("If China doesn't begin to acknowledge and curb its corporate cyberespionage, the U.S. plans to start selecting from a range of retaliatory options . . . .").

411 The U.S. has brought one case against China before the WTO under TRIPS. However, this case did not involve cyber economic espionage. *See* Panel Report, *China – Measures Affecting the Protection and Enforcement of Intellectual Property Rights*, WT/DS362/R (Jan. 26, 2009).

TRIPS obligations.[412]

The goal of TRIPS was to "narrow the gaps in the way these rights are protected around the world, and to bring them under common international rules."[413] Most importantly, TRIPS enshrines important principles of fair play and honest dealing that are inconsistent with cross-border IP theft for commercial purposes.[414] Such information "must be protected against breach of confidence and other acts contrary to honest commercial practices."[415]

Even though there is no express economic espionage prohibition in the WTO rules or the TRIPS agreement, the letter and spirit of the agreements indicate that theft of trade secrets are prohibited.[416] Such theft undermines the purpose of these agreements—to create a fair trade regime among member states. China's actions can be characterized as "measures that comply with the letter of the agreement, but nevertheless frustrate one of its objectives or undermine trade commitments contained in the agreement,"[417] and arguably should be prohibited.

---

412 Fanshu Yang, Ping Yang & Kristie Thomas, *Recent WTO Disputes Involving the Protection and Enforcement of Intellectual Property Rights in China: Legal and Political Analysis*, 24 U. NOTTINGHAM: CHINA POL'Y INST. BRIEFING SER. (Aug. 2007), http://ssrn.com/abstract=1437642.

413 *Id.*

414 For example, Article 26(1) states that "[t]he owner of a protected industrial design shall have the right to prevent third parties not having the owner's consent from making, selling, or importing articles bearing or embodying a design which is a copy, or substantially a copy, of the protected design, when such acts are undertaken for commercial purposes." TRIPS Agreement, *supra* note 211, art. 26(1). Article 39(2) encompasses the principle of honest commercial practices, stating that "[n]atural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices . . . ." *Id.* art. 39(2).

415 *Intellectual Property: Protection and Enforcement*, WORLD TRADE ORG., http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm (last visited Oct. 6, 2014). Furthermore, as codified in the Paris Convention of 1883, TRIPS sets out a common rule that "[e]ach contracting State must provide for effective protection against unfair competition." Summary of the Paris Convention for the Protection of Industrial Property (1883), WORLD INTELL. PROP. ORG. [WIPO], http://www.wipo.int/treaties/en/ip/paris/summary_paris.html (last visited Sept. 14, 2014).

416 *Dispute Settlement Training Manual, Legal Basis for a Dispute, Types of Complaints and Required Allegations in GATT 1994*, WORLD TRADE ORG, http://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c4s2p2_e.htm (last visited Sept. 21, 2014).

417 *Id.*

A. Does the WTO have Jurisdiction over Economic Espionage?

As a general matter of law, IP rights are granted and protected on a territorial basis by national governments.[418] For example, China, under Article 3 of TRIPS, must provide IP within its territory, owned by citizens of other WTO members, certain minimum standards of treatment such as national treatment.[419] Nothing in the WTO or TRIPS rules explicitly mandates China or any WTO member to protect commercially valuable information found in the territories of other countries. Likewise, neither WTO nor TRIPS rules prohibit government-sponsored espionage within another country.

As courts of delegated and limited jurisdiction, WTO panels can only examine government measures for their consistency with so-called "WTO covered agreements."[420] As such, the WTO panels and the Appellate Body "cannot interpret and enforce non-WTO law other than to the extent necessary to interpret and apply WTO provisions."[421] They cannot examine claims of violation of, for example, human rights or environmental treaties, nor of customary international law.[422] In short, the mandate of panels and the Appellate Body is to determine whether provisions of the WTO 'covered agreements' alone have been violated. Pursuant to Article 1.1, the DSU applies to disputes brought under the covered agreements.[423] Finally, under Article 19.1 of the DSU, the standard recommendation is that the losing member "brings its measure into conformity with the covered agreements."[424] The limited jurisdiction of the WTO bodies, confirmed by the cautious jurisprudence of the Appellate Body, may prove to be a challenge

---

418 *See supra* notes 48-50 and accompanying text.

419 *See* TRIPS Agreement, *supra* note 211, at art. 3.

420 *Understanding on Rules and Procedures Governing the Settlement of Disputes*, art 1.1, WORLD TRADE ORG, http://www.wto.org/english/res_e/booksp_e/analytic_index_e/dsu_01_e.htm#article1A1 (last visited Sept. 21, 2014).

421 Gabrielle Marceau & Anastasios Tomazos, *Comments on Joost Pauwelyn's Paper: 'How to Win a WTO Dispute Based on Non-WTO Law?,' in* AT THE CROSSROADS: THE WORLD TRADING SYSTEM AND THE DOHA ROUND 55, 57 (Stefan Friller ed., 2008).

422 *Id.* at 71.

423 *Understanding on Rules and Procedures Governing the Settlement of Disputes*, *supra* note 420, art. 1.1.

424 *Id.* art. 19.1.

to any claim a state may bring before such bodies for acts of economic espionage constituting wrongful intervention.[425]

However, as has been noted by many international legal scholars and seemingly supported by the WTO decisions themselves, such limited jurisdiction does not mean that the WTO should be in isolation from the rest of international law. In its first report, *US-Gasoline*, the Appellate Body noted that the WTO agreements must not be interpreted in "clinical isolation" from public international law.[426] The Appellate Body cited Article 3.2 of the DSU, which requires panels and the Appellate Body to use "customary rules of interpretation" to interpret the provisions of the WTO agreements.[427] According to Article 31.3(c) of the Vienna Convention, when interpreting the ordinary meaning of treaty terms, an interpreter shall "take into account" any applicable rule of international law.[428]

It may be that while the WTO rules say nothing about economic espionage, the customary norm of non–intervention will lend interpretive value to the WTO rules to find that such state behavior is not acceptable under the WTO regime. In this way, Article 31.3(c) of the Vienna Convention promotes coherence so

---

425 *See* Appellate Body Report, *European Communities – Measures Affecting The Importation Of Certain Poultry Products*, WT/DS69/AB/R (July 13, 1998) (holding the Oilseeds Agreement was not "applicable law" and could not be enforced by the WTO dispute settlement mechanism when Brazil claimed that the European Communities had not provided it with the full allocations of a tariff quota on frozen chicken imports, contrary to their "Oilseeds Agreement" and EC schedules' obligations).

426 Appellate Body Report, *United States – Standards for Reformulated and Conventional Gasoline*, 17, WT/DS2/AB/R (May 20, 1996). One view is that WTO rules are part of general public international law and as such any non-WTO rules are "relevant to and may have an impact on WTO rules[,] and . . . have not been contracted out of, deviated from, or replaced by the WTO treaty." Joost Pauwelyn, *The Role of Public International Law in the WTO: How Far Can We Go?*, 95 AM. J. INT'L L. 535, 541 (2001); *see also* Panel Report, *United States – Continued Suspension of Obligations in the EC-Hormones Dispute*, ¶ 7.336, WT/DS320/R (Mar. 31, 2008) (*modified* and *adopted* Nov. 14, 2008) ("Customary international law applies generally to the economic relations between the WTO members. Such international law applies to the extent that the WTO agreements do not 'contract out' from it. To put it another way, to the extent there is no conflict or inconsistency, or an expression in a covered WTO agreement that implies differently, we are of the view that the customary rules of international law apply to the WTO treaties and to the process of treaty formation under the WTO.").

427 *Understanding on Rules and Procedures Governing the Settlement of Disputes*, *supra* note 420, at art. 3.2.

428 *See* Vienna Convention on Diplomatic Relations, *supra* note 62.

that the treaty being interpreted and other relevant international law rules are read in a mutually supportive way, thus avoiding conflicts with other treaties.

The U.S.'s challenge to bringing a claim before the WTO in the case of Chinese economic espionage therefore is that the U.S. would have to show that China violated an obligation that is specifically within the WTO or TRIPS rules. WTO members are only obliged to fulfill commitments that they have consented to within the "four corners" of the "covered agreements" of the WTO. It would seem clear, however, that the language of Article III of TRIPS requires as a general obligation under the "national treatment principle" that a country "shall accord to the nationals of other members treatment no less favorable then it accords to its own nationals . . . ."[429] China, in providing government-sponsored commercial intelligence based on stolen IP to its own firms, is giving its own nationals a more favorable treatment, arguably in violation of its obligation under TRIPS.

Ultimately, however, it will be up to those states that choose to litigate claims before the WTO panels, as well as the arbitrators, to determine whether and how the scope of the WTO agreements will include the customary international norm of non-intervention in economic affairs. The issue will revolve around whether the WTO agreements have contracted out of customary international norms like the norm of non-intervention whereby such rules would not be part of the WTO dispute settlement process. Certainly, no TRIPS provision explicitly and completely contracts out of the fundamental principles of sovereignty and state responsibility.[430]

If the U.S. ultimately decides to invoke legal countermeasures against China for its economic espionage, China may choose to bring a claim to the WTO against the U.S. for a violation of a WTO rule.[431] Types of the possible countermeasures the U.S. may consider that have been proposed against China to date include:

> denying products that contain stolen intellectual property access to the U.S. market; restricting use of the U.S. financial system to foreign companies that repeatedly steal intellectual property; and adding the correct, legal handling

---

429 TRIPS Agreement, *supra* note 211, at 299.

430 The DSU has arguably contracted out of some general rules on state responsibility. For a detailed discussion of this see Pauwelyn, *supra* note 426, at 539.

431 *See* Riley, *supra* note 41.

> of intellectual property to the criteria for both investment in the United States under Committee for Foreign Investment in the United States (CFIUS) approval and for foreign companies that are listed on U.S. stock exchanges.[432]

Since thousands of Chinese companies depend on the U.S. market and exposure to American companies in order to satisfy the growing Chinese consumer market, such countermeasures may likely succeed in getting China to desist in its economic espionage against American companies.[433] If China brings a claim against the U.S. based on such countermeasures, the U.S. may have to invoke the customary norm of countermeasures as a defense to China's claim. Then it will be up to the WTO panel to decide first, whether the panel has jurisdiction to hear the case (if the charges implicate WTO rules) and second, whether they will render a decision on the merits of the claim if the defense rests on claims of customary international law.[434]

Given the specific facts of the case of the Chinese PLA members, it may be likely that the U.S. seeks to use countermeasures to deter China. In invoking countermeasures, however, there may no option but to impose a countermeasure that links to trade issues, therefore potentially implicating the WTO process. Certainly, the allegations of Chinese economic espionage are intrinsically linked with trade issues.[435] Of those corporate victims in the U.S. indictment, four were in the midst of a trade dispute with China when they were hacked by the PLA officials.[436]

SolarWorld, one of the U.S. companies at issue in the PLA actions, has requested that the Commerce Department seek

---

[432] Dennis Blair & Jon Huntsman, Jr., *Protect U.S. Intellectual Property Rights*, WASH. POST, May 21, 2013, http://www.washingtonpost.com/opinions/dennis-blair-and-jon-hunts . . . rights/2013/05/21/b002e10e-c185-11e2-8bd8-2788030e6b44_story.html.

[433] Zachary Karabell, *Do American Politicians Even Care About the Rise of China Anymore?*, THE ATLANTIC, June 7, 2013, http://www.theatlantic.com/politics/archive/2013/06/do-american-politicians-even-care-about-the-rise-of-china-anymore/276663/.

[434] *See* Anastasio Gourgourinis, *'Lex Specialis' in WTO and Investment Protection Law*, 22 (Society of Int'l Econ. Law [SIEL] Working Paper No. 2010/37, July 2, 2010), *available at* http://ssrn.com/abstract=1634051; *see also* Joost Pauwelyn, *How to Win a World Trade Organization Dispute Based on Non-World Trade Organization Law? Questions of Jurisdiction and Merits*, 37 J. WORLD TRADE 997 (2003).

[435] *See* Riley, *supra* note 41.

[436] See Keith Bradsher, *Retalitory Attacks, Online*, N.Y. TIMES, May 20, 2014, http://www.nytimes.com/2014/05/21/business/international/firms-in-united-states-see-risk-in-challenges-to-beijing.html?_r=0.

information from Chinese officials, pertaining to the intrusions against the company as well as any information that links the government hackers to Chinese solar panel manufacturers.[437] This is the first case where a corporation has brought allegations of cyber espionage into a trade dispute.[438] Based on U.S. law, if the U.S. determines that the Chinese response is not satisfactory, it can impose high tariffs and import duties against Chinese solar goods, effectively blocking them from the U.S. market.[439] This would be the first time that the U.S. has imposed an economic penalty for activity stemming from cyber espionage.

B. The Applicable Law the WTO is to Use in Rendering Decisions

If China is found in violation of a WTO or TRIPS rule, and thus within WTO jurisdiction, the next question is what law the WTO should use in rendering its decision.[440] Unlike the ICJ, the WTO rules do not set out a list of the sources of law that are applicable to the decisions of the WTO panels.[441] However, there

---

437 *Id.*

438 As part of its complaint, SolarWorld alleges that Chinese solar companies receive large subsidies from the Chinese government, which allows the companies to sell their products for less than it costs to make them. According to the company, this has resulted in U.S. solar panel makers not being able to match the Chinese prices, forcing them to shut down factories, laying off thousands of workers. *See* Shane Harris, *Exclusive: U.S. Manufacturer Wants Commerce Dept. to Penalize China for Cyberattack*, FOREIGN POLICY, July 1, 2014, http://complex.foreignpolicy.com/posts/2014/07/01/us_manufacturer_wants_commerce_dept_to_penalize_china_for_cyberattack_0.

439 The U.S. mechanism to resolve trade disputes is through the USTR Special 301 Report. The annual report assesses foreign countries on their ability to protect intellectual property and identifies actions taken or anticipated by the U.S. government. Biman Mukherji, *U.S. Hits China Solar Firms*, WALL ST. J., Aug. 1, 2014, http://online.wsj.com/articles/u-s-hits-china-solar-firms-1406882738?mod=pls_whats_news_us_business_f.

440 *See* Lorand Bartels, *Applicable Law in WTO Dispute Settlement Proceedings*, 35 J. WORLD TRADE 499, 499 (2001) ("[I]nternational law from all sources is potentially applicable as WTO law, subject to a de facto restriction resulting from the limited jurisdiction of Panels and the Appellate Body to decide on only certain types of disputes, and subject also to a conflicts rule, stated in Articles 3.2, and 19.2 of the DSU, that Panels may not add to or diminish the rights and obligations of Members set out in the covered agreements.").

441 Statute of the International Court of Justice, art. 38, 1945 annex to the U.N. Charter.

have been a number of WTO decisions that have provided insight into what international law would be applicable. For example, WTO treaty terms have been interpreted with reference to: (1) other international agreements;[442] (2) general principles of international law such as good faith, due process or *abus de droit*;[443] and (3) general customary international law such as "the rules of general international law on state responsibility, which require that countermeasures in response to breaches by states of their international obligations be commensurate with injury suffered."[444]

Significantly, in the *Shrimp-Turtle* case, in confirming that the WTO operates as part of a living system of international law, the Appellate Body, opted for a so-called "evolutionary" approach to interpreting the WTO treaty provisions on "exhaustible natural resources."[445] The Appellate panel stated, "[t]hey must be read by a treaty interpreter in the light of contemporary concerns of the community of nations about the protection and conservation of the environment . . . . The generic term 'natural resources' in Article XX(g) is not 'static' in its content or reference but is rather 'by definition, evolutionary.'"[446] Certainly, however, interpretation with reference to other international law cannot lead to an interpretation *contra legem* and cannot overrule the unambiguous wording of a WTO provision.

One potential argument could be that because the WTO is part

---

442 Appellate Body Report, *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, ¶¶ 128-132, WT/DS58/AB/R (Nov. 6, 1998) (interpreting the words "exhaustible natural resources" in GATT Article XX(g)).

443 *E.g.,* Appellate Body Report, *European Communities – Measures Concerning Meat and Meat Products*, WT/DS26/28 (Apr. 14, 2014) [hereinafter EC-Hormones]; Appellate Body Report, *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R (Nov. 6, 1998); Appellate Body Report, *United States – Tax Treatment for 'Foreign Sales Corporations*,*'* WT/DS108/36 (Mar. 17, 2006).

444 Appellate Body Report, *United States – Transactional Safeguard Measure on Combed-Cotton Yarn from Pakistan*, WT/DS192/AB/R, ¶ 120 (Oct. 8, 2001) [hereinafter U.S.-Cotton Yarn]. So if the U.S. is brought before the WTO by China for any economic sanctions in response to the Chinese cyber economic espionage, the WTO panel would consider a U.S. defense argument based on customary international legal principles of state responsibility that its countermeasures were proportionate to the injury suffered from the Chinese actions. *See id.*

445 Appellate Body Report, *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, 48 WT/DS58/AB/R (Oct. 12, 1998).

446 *Id.*

of general international law, the customary international law of cyber economic non–intervention has altered the meaning of a WTO treaty provision. This would be a challenging argument to make before a WTO panel given the Appellate Body's extreme hesitation to address the issue of whether a rule of customary law ought to supplement the provisions of a WTO covered agreement.[447] It would be a real challenge for a WTO panel to rule that a new rule of custom has emerged that has supplanted a WTO treaty provision. Furthermore, even if customary law exists prohibiting cyber economic espionage intervention, and a genuine conflict exists because the WTO treaty does not prohibit such activity while under custom it is prohibited, the treaty is most likely to prevail as *lex specialis,* based on its often specific and explicit expression of state of will.[448] In sum, WTO members can only be held to customary international law if: (1) the strict rules for its emergence are met (long practice, majority of states and *opinio juris* with the persistent objector rule applicable); and (2) even if a custom was explicitly or tacitly consented to, it is unlikely to prevail over the WTO treaty.[449] However, even if WTO applicable law seems to exclude the direct application of some rules on state responsibility, these rules, to the extent that they are customary, bind WTO Members and remain a relevant benchmark for the interpretation of WTO law that is presumed to evolve consistently with other international law.[450]

In sum, the WTO panels and the Appellate Body cannot interpret or reach any conclusions about the legality of any actions with other treaties or custom in complete isolation from the WTO covered agreements.[451] However, if there is an interpretive link

---

447 EC-Hormones, *supra* note 443, pt. I, ¶ 35.

448 For a full discussion of this topic see JOOST PAUWELYN, CONFLICT OF NORMS IN PUBLIC INTERNATIONAL LAW: HOW WTO LAW RELATES TO OTHER RULES OF INTERNATIONAL LAW (2003).

449 *See* Pauwelyn, *supra* note 426 (discussing how the WTO would resolve the conflict between two norms).

450 *See* U.S.-Cotton Yarn, *supra* note 444, ¶ 120 ("Our view is supported further by the rules of general international law on state responsibility, which require that countermeasures in response to breaches by states of their international obligations be commensurate with the injury suffered.").

451 Marceau & Tomazos, *supra* note 421, at 77 ("There is no evidence whatsoever to even suggest that during the Uruguay Round the drafters of the WTO treaty ever wanted to provide non-WTO norms with direct effect into WTO law . . . .").

with customary international law and a provision of a WTO rule, then a WTO panel may apply the non-WTO law to interpret the provision of the WTO rule.[452] In that way, a claim related to economic espionage could be decided based on rules and the customary international norm of non–intervention. The norm can be used in order to assist in the interpretation of the TRIPS rule as well as other WTO rules of fair competition. However, the WTO dispute settlement process cannot allow non-WTO norms to have direct effect on WTO law and allow Members the benefit of free use of the WTO remedial mechanism to enforce non-WTO rights and obligations.[453]

If, however, the U.S. were to successfully argue that China has violated TRIPS, further obstacles await. First, it would need to prove that the Chinese government was responsible for conducting the wrongful act by attributing the intrusions to the government.[454] Second, the U.S. would have to be able to articulate the level of damage suffered by it as a result of China's conduct.[455]

Another option is for the U.S to impose trade sanctions against China by invoking national security exceptions found in WTO agreements.[456] Under WTO rules, a WTO member can invoke these exceptions without establishing any violation of WTO rules of the other party. Under Article 73 of TRIPS, the U.S. could claim it was taking such actions because it considers it "necessary for the protection of its essential security interests . . . taken in time of war or other emergency in international relations" caused by the Chinese economic espionage.[457] Most WTO experts argue that a WTO member's right to invoke such an exception is not challengeable by a WTO panel.[458] However, in the nearly seven

---

[452] *Id.*

[453] *See generally* Marceau & Tomazos, *supra* note 421.

[454] *See* TRIPS agreement, *supra* note 211, art. 41.

[455] *Id.*

[456] *Id.* art. 73.

[457] General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194, art. 21.

[458] The closest the trade regime has come to having to define the exception was in 1986 in the Nicaragua case. The U.S. argued that its imposing a trade embargo on Nicaragua was done for national security reasons and that the security exception left it to each country to judge for itself what action it considered necessary for the protection of its essential security interests. The GATT panel could not reach a binding result. Although this U.S. view of the self-judging nature of the national security exception is not accepted as an authoritative interpretation of international trade law, most WTO

decades since this security exception was written into the GATT, few have asked what this exception means, and how the breadth of the exception allows for potential abuse.[459] Furthermore, there is always the possibility that China would retaliate against the U.S. for imposing such sanctions.

C. WTO Dispute Settlement or Other Means

Ultimately, the WTO may inevitably have to deal with issues of cyber economic espionage. There are persuasive arguments in support of pursuing this avenue. First, international legal processes may actually produce positive results. Rooted in international law, the tools are girded with the legitimacy that only the law can confer. The legal process may be the best choice to achieve an equilibrium between nations that both encourages respect for the intellectual property rights of others and deters violations of international obligations. If the U.S. brought a complaint against China at the WTO, or even threatened to bring such a complaint, this may actually deter the Chinese, because their economy is reliant upon trust in the global marketplace.[460] A ruling against China by an internationally-recognized WTO panel could render China liable for billions of dollars in compensation, expose it to multinational economic sanctions, and cause it to be branded a scofflaw in global trade.[461]

It may not be wise, however, for states to use the international trade law and regimes as the instruments for addressing national security threats posed by espionage. In 1996, the U.S. took this position when it imposed unilateral trade restrictions against Cuba through the Helms-Burton Act. When the EU took the U.S. to the WTO challenging its actions, the U.S. informed the WTO that it would not participate in the WTO proceedings, saying the dispute was not fundamentally a trade matter and therefore not a WTO matter.[462] An important question is whether trade measures taken

---

members agree with this view.

459 *See Sweden – Import Restrictions on Certain Footwear*, GATT Doc. L/4250 (Nov. 17, 1975); *see also* Peter Lindsay, *The Ambiguity of GATT Article XXI: Subtle Access or Rampant Failure?*, 52 DUKE L.J. 1277, 1302 (2003).

460 *See* Donilon, *supra* note 24.

461 *Id.*

462 *See generally* David E. Sanger, *Europeans to Fight U.S. Sanctions Against Cuba in Trade Court*, N.Y. TIMES, Oct. 2, 1996, http://www.nytimes.com/1996/10/02/world/europeans-to-fight-us-sanctions-against-cuba-in-trade-court.html.

in the name of national security are ultimately justiciable? Are these trade disputes linked with security issues the types of disputes that the WTO panels can effectively and fairly judge? A more appropriate option for security issues related to espionage may be public international law and the use of countermeasures under customary international law as this Article has discussed. For settling disputes regarding economic espionage, the UN Security Council and the ICJ may be better alternatives than the WTO dispute mechanism.

Certainly, negotiations between states are always a possible mechanism. If negotiations fail, however, states still retain authority under rules of general public international law that encompass norms that are not necessarily incorporated within the WTO. Lawful unilateral countermeasures to enforce those norms, like the norm of non-intervention that prohibits a state from conducting economic espionage within another country, may be the most appropriate avenue for the U.S. to pursue with respect to Chinese cyber-enable IP theft.[463] A frontal assault on Chinese cyber espionage practices in general may be less likely to advance U.S. interests than putting pressure on specific Chinese policies, such as those that discriminate against foreign companies' economic competitiveness and those that work in favor of politically-connected Chinese companies, which may be most fruitful.

Understandably, in the absence of new agreements on economic espionage and an apparent lack of effective policy options to deter Chinese economic espionage, there is a temptation to seek satisfaction through the aggressive use of venues such as the WTO dispute settlement mechanism – litigation in lieu of negotiation.[464] Arguably, the actions by the Chinese government in conducting economic espionage violate the spirit, if not the letter, of our global trade agreements. Yet, if the U.S. decides to bring a complaint against China in the WTO for these actions, there may be serious long-term consequences for the viability of the WTO itself. The WTO is not a legislative body, and states, including the U.S., have generally objected when dispute settlement panels have taken an expansive view of their powers.[465]

---

463 *See supra* Sections II and III.

464 *See supra* notes 460-461 and accompanying text.

465 *See supra* note 462 and accompanying text.

If the dispute settlement mechanism is used to resolve fundamentally political or unsettled points, it will eventually lose credibility and countries will cease to abide by its decisions. For the sake of the future of the WTO itself, it may not be time yet to bring such claims to that forum. Importantly, international law still provides those states whose rights have been violated other avenues, such as countermeasures, to enforce those rights.

VI. Conclusion

Arguably, it would be a great boon to world security if traditional espionage were rendered obsolete. But as long as the world arena remains divided and latently hostile, individual states will adopt strategies intended to protect their own security secrets and discover the secrets of potential enemies in order to guard against surprise.[466] The development of an international norm prohibiting states from stealing IP in the cyber domain would contribute to a more stable international order.[467] First, the restriction tends to minimize the potential for escalating violence in the cyber domain. Second, it functions as a restraint against state actions in cyberspace based on misunderstanding and erroneous factual determinations that are pervasive in cyberspace.[468]

As discussed in this Article, the customary international law principle of non-intervention includes significant gaps and ambiguities as it pertains to cyber economic espionage. States have not reached consensus on rules for coercion in cyberspace to easily apply the term in the context of cyber-enabled IP theft. Furthermore, there seems to be a lack of a consensus by states on what are internal and external matters that would be protected by the principle in the context of economic matters.[469] There also appears to be significant disagreement among trade experts as to the extent the WTO regime contemplates the role of customary international principles such as non-intervention in its dispute mechanism.[470]

It may be that the current ambiguous state of the principle of

---

466 *See supra* Section I.

467 *See supra* note 5 and 201, and accompanying text.

468 *See* Cherne, *supra* note 95.

469 *See e.g.* Cohen & Chiu, *supra* note 233.

470 *See supra* Section IV(a).

non–intervention and the arguably limited, if not non-existent, role of the WTO dispute settlement regime in resolving the ambiguities, reflects the full extent to which states are willing to commit the issue to international law. It may be that the issue of cyber economic espionage will be resolved through political settlements rather than by international legal adjudication. Both the principle of non-intervention and the WTO dispute settlement process have played major roles in supporting a peaceful system of sovereign equals and international trade.[471] The rising threat from economic espionage may counsel for a focused interest in either addressing the ambiguities within these international legal mechanisms, or at least acknowledging that these issues will not be resolved under existing legal principles.

Today, uncertainty remains as to where the threshold for intervention lies. Over time, however, the reaction of states to cyber operations that fall below the use of force threshold as well as how states characterize their own cyber operations will inform the process of interpretation of the norm of non–intervention. Wherever the threshold for non–intervention lies today, in the future, that threshold will rise or fall with state practice depending on how states characterize the damage that IP theft can have on a state's economy.[472] States may recognize the value of well-defined red lines for economic espionage and seek to achieve consensus on a specific threshold for intervention.[473] Whatever may happen, as economic espionage persists, states will be forced by circumstances to take a position on whether a particular cyber operation has breached the non-intervention norm. These assessments will add to the context of the norm in the cyber context, providing much needed predictability and stability to the cyber domain.

Certainly, if law is to continue to be relevant, it must be responsive to the facts and circumstances of the times.[474] As cyber operations are not a passing fad, international law must be able to regulate state behavior in this new domain or risk being

---

471 *See supra* Sections III -, IV.

472 *See supra* notes 23-28 and accompanying text (discussing how the U.S. is beginning to characterize IP theft).

473 *Id.*

474 *See* Jensen, *supra* note 6.

irrelevant.[475] For cyber operations, the rules of modern international law must evolve to "define more sharply the criteria used to distinguish between which state actions are permissible as normal computer-generated transborder data flows for international communications, trade, and financial assistance"[476] from those cyber operations that may qualify as an unlawful intervention. As cyber activities become more central to the functioning of the modern society, and while a state's fundamental security rests on the ability of its companies to be competitive on the global market, the law, the norm of non–intervention, and the WTO rules, may need to evolve affording states and companies more security.[477] While economic competition is unavoidable in a globally connected world, international law as it evolves may contribute to avoiding economic conduct by states which causes serious harm to the economies of other states, creating destabilizing effects for the international community and increased potential for escalation of conflict.[478]

Indeed, whether and how the distinction can be drawn between permissible and impermissible economic conduct can be subjected to objective evaluation is a question of crucial importance. International law must be able to provide a means for delineating where proper economic pressure ends and improper economic coercion begins as well as an institutional mechanism capable of applying and enforcing delineations once they have been established. As this Article has suggested, the norm of non-intervention in conjunction with WTO rules may provide the necessary rules.[479] Furthermore, customary countermeasures as well as the potential for dispute settlement through the WTO may provide the needed institutional mechanisms for enforcing such rules. If, however, it is determined that the WTO regime currently

---

475 *Id.*

476 Joyner & Lotrionte, *supra* note 8, at 864.

477 International law responds and develops not only to the concerns of a nation-state, but also to the concerns of the many different players in the international order, including the private sector. W. MICHAEL REISMAN, THE QUEST FOR WORLD ORDER AND HUMAN DIGNITY IN THE TWENTY-FIRST CENTURY: CONSTITUTIVE PROCESS AND INDIVIDUAL COMMITMENT 137 (Hague Acad. of Int'l L., 2012) ("In both formal and informal arenas, non-official actors increasingly participate in direct or indirect fashion.").

478 *See supra* notes 272-274 and accompanying text.

479 *See supra* Section IV.

does not provide the necessary mechanism for evaluating the legality of measures of economic coercion in the case of theft of intellectual property, as it is restricted in the range of economic relations covered, consideration must be given to other arrangements to ensure that states refrain from economic coercion and adhere to fair trading practices.

It may be that until a comprehensive code of conduct regulating fair trading practice is developed that identifies practices which are coercive and thus not "fair," states will rely on their own determination of what constitutes "unfair" practices and rely on the use of legal countermeasures to protect their security in the economic realm. In that sense, this Article attempts to distinguish more clearly "economic coercion," which may be valuable to assessing what economic wrongful acts may trigger a state's right to invoke countermeasures. Certainly, the issue of economic coercion is only a minor facet of a much broader and much more important problem of securing fair trading practices. To date, it may be that the WTO regime has not been effective in covering all of the facets of securing such fair practices. In fact, the current controversy over China's cyber economic espionage[480] is illustrative of the fact that there has been a failure to establish institutional means that will ensure a system of fair trading. Until that time, states may be wise to contemplate countermeasures and the legal delineations for such self-help options.

---

[480] *See supra* notes 23-28 and accompanying text.