2014

An International Law Response to Economic Cyber Espionage

Christina Parajon Skinner

CONNECTICUT
LAW REVIEW

VOLUME 46 MAY 2014 NUMBER 4

Article

An International Law Response to Economic Cyber Espionage

CHRISTINA PARAJON SKINNER

Cyber threats have emerged as one of the most serious dangers to U.S. and global security. Increasingly, malicious actors—some private, but others that appear to be state-sponsored—seek to advance their strategic aims through violent or non-violent cyber-attacks. This Article considers the problem of non-violent, yet still destructive, economic cyber espionage, which targets the intellectual, industrial, and information property of major global powers like the United States.

The Article argues that the international community's reticence is owing to a stale set of international legal norms. The Article explains how existing principles of international law—such as state sovereignty, non-intervention, and state responsibility—should evolve to address the current threat of economic cyber espionage. The Article also discusses how norms against economic cyber espionage could also be interpreted to exist within the World Trade Organization (WTO) agreements that deal with intellectual property. These WTO rules together with the relevant (and modernized) customary norms arguably provide WTO member states recourse to the Dispute Settlement Body to assert their claims of economic cyber espionage. The Article urges victim states to channel their legal complaints through this economic body and its dispute resolution mechanism. It concludes with a realist perspective on why the WTO would be the most effective institution to ensure compliance with these norms.

ARTICLE CONTENTS

An International Law Response to Economic Cyber Espionage

CHRISTINA PARAJON SKINNER*

I. INTRODUCTION

Spying has re-emerged as a significant problem for national security. Today, in the Internet and information age, states have re-tooled their espionage techniques for use in cyberspace—and the United States is a prime target.[1] For the past several years, cyber espionage has been adversely impacting the nation's economic and national security.[2] Covert cyberintrusions, which target U.S. industry, research, and technology, are undermining the economy and its global competitiveness. But despite the damage that this spying has caused so far, these covert attacks continue, with no wholly effective legal or policy solution to date.

Cyber espionage, and economic-oriented cyber espionage in particular, poses a serious threat to the United States' national security. This type of economic espionage "affects the sources of American power,"[3] including its comparative advantage in scientific and technological innovation and development. According to a report from the Office of the National Counterintelligence Executive, cyberspace, "where most business activity and development of new ideas now takes place," allows "malicious" cyberspies "to quickly steal and transfer massive quantities of data while

---

* J.D. Yale Law School, 2010; A.B. Princeton University, 2006. Thank you to William Skinner, who helped me to develop this idea, and to Michael Reisman, BJ Ard, Pamela Foohey, Charlotte Garden, and Joshua Geltzer for their comments. I am also grateful to the editors of the *Connecticut Law Review* for their careful editing of this Article.

[1] *See, e.g.*, David E. Sanger & Mark Landler, *U.S. and China Will Hold Talks About Hacking*, N.Y. TIMES, June 2, 2013, at A1 (remarking that the growth of cyber-attacks is "a new enough phenomenon").

[2] In the context of a case involving an illegal export of U.S. military software, one federal agent recently explained that "[w]hile the thefts associated with economic espionage and illegal technology transfers may not capture the same level of attention as a terrorist incident, the costs to the U.S. economy and our national security are substantial." *Press Release: United Technologies Subsidiary Pleads Guilty to Criminal Charges for Helping China Develop New Attack Helicopter*, U.S. DEP'T JUST. (June 28, 2012), http://www.justice.gov/usao/ct/Press2012/20120628.html.

[3] JAMES A. LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, CONFLICT AND NEGOTIATION IN CYBERSPACE 50 (2013), *available at* http://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf; *see also id.* (noting that "[t]rade is a national security issue").

remaining anonymous and hard to detect."[4] The report also warned that "[c]yber tools have enhanced the economic espionage threat, and the Intelligence Community . . . judges the use of such tools is already a larger threat than more traditional espionage methods."[5] As commentators have noted, "[T]he hemorrhage of intellectual property (IP)—our most important international competitive advantage—is a national crisis. Nearly every U.S. business sector—advanced materials, electronics, pharmaceuticals and biotech, chemicals, aerospace, heavy equipment, autos, home products, software and defense systems—has experienced massive theft and illegal reproduction."[6] It comes as no surprise, then, that the *2010 National Security Strategy* assessed "[c]ybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[7]

Though there are no doubt other actors who have resorted to economic cyber espionage, Chinese actors appear to be at least one significant source of this activity.[8] In the past few years, China has reportedly attacked many

---

[4] 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, 2009–2011, at i (2011) [hereinafter FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS].

[5] *Id.*

[6] Dennis Blair & John Huntsman, Jr., *Safeguard U.S. Ingenuity*, WASH. POST, May 22, 2013, at A19. Private industry and government are not the only sectors affected; academia has also been the victim of serious cyberintrusions. According to the *New York Times*, "America's research universities . . . are increasingly coming under cyberattack, most of it thought to be from China, with millions of hacking attempts weekly. Campuses are being forced to tighten security, constrict their culture of openness and try to determine what has been stolen." Richard Pérez-Peña, *Campuses Face Rising Threat from Hackers*, N.Y. TIMES, July 17, 2013, at A1. The target, however, remains the same: intellectual property.

> Universities and their professors are awarded thousands of patents each year, some with vast potential value, in fields as disparate as prescription drugs, computer chips, fuel cells, aircraft and medical devices. . . . Like major corporations, universities develop intellectual property that can turn into valuable products like prescription drugs or computer chips. But university systems are harder to secure, with thousands of students and staff members logging in with their own computers.

Id.

[7] THE WHITE HOUSE, NATIONAL SECURITY STRATEGY 27 (2010), *cited in* THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 2 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

[8] The evidence that China sponsors cyber espionage includes detailed reports by the cybersecurity firm Mandiant. One report published in 2013 indicates that:

> APT1 [an advanced threat actor called "Advanced Persistent Threat"] has been stealing hundreds of terabytes of data from at least 141 organizations across a diverse set of industries beginning as early as 2006. . . . Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technological blueprints, proprietary manufacturing processes, test results, business

sectors of the U.S. economy and agencies critical to our national security, penetrating the online systems of the U.S. Departments of Homeland Security and State, Coca-Cola, Lockheed Martin, Dow Chemical, Adobe, Yahoo!, and Google, to name just a few.[9] According to General Keith B. Alexander, head of the United States Cyber Command and director of the National Security Agency, these cyber "attacks have resulted in the 'greatest transfer of wealth in history.'"[10]

The U.S. government has officially accused China of e-spying on American interests.[11] A Pentagon report released in May 2013 found that China's cyber espionage targeted industrial technology, as well as government policy information.[12] In February 2014, the *New York Times* reported, "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."[13] And on May 19, 2014, the U.S. Department of Justice announced that it was indicting five members of the

---

> plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership.

MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 20 (2013) [hereinafter MANDIANT REPORT], *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. It concludes "that APT1 is likely government sponsored." *Id.* at 2. More recently, Mandiant has inferred from the intelligence it has collected that "A.P.T. 1 is Unit 61398" of the Chinese Army, "the central element of Chinese computer espionage." David E. Sanger et al., *China's Army Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 19, 2014, at A1. It is from the location of this Unit that "an overwhelming percentage of the attacks on American corporations, organizations and government agencies" is believed to originate. *Id.* There are many other published accounts of China's participation in cyber espionage. *See, e.g.*, FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS, *supra* note 4, at i ("Chinese actors are the world's most active and persistent perpetrators of economic espionage."); Michael Riley, *Snowden's Leaks Cloud U.S. Plan to Curb Chinese Hacking*, BLOOMBERG (June 30, 2013), http://www.bloomberg.com/news/2013-07-01/snowden-s-leaks-cloud-u-s-plan-to-curb-chinese-hacking.html ("The U.S. already has privately provided China's leaders with evidence it gathered linking the hacks of commercial companies to China's intelligence agencies . . . ."); sources cited *infra* notes 9–12. However, this Article does not assume that China is the only country capable of or culpable for committing economic cyber espionage. Other countries reportedly engage in cyber espionage as well. *See, e.g.*, LEWIS, *supra* note 3, at 44–45 (describing Russia's cyber espionage efforts and noting that Israel and France have also been accused of maintaining state-led cyber espionage programs).

[9] Phillip Elmer-DeWitt, *Apple. China. Cyberwar.*, CNNMONEY (Mar. 31, 2013), http://tech.fortune.cnn.com/2013/03/31/apple-china-hackers-tradewar.

[10] Sanger & Landler, *supra* note 1.

[11] David E. Sanger, *China's Military Is Accused by U.S. in Cyberattacks*, N.Y. TIMES, May 7, 2013, at A1.

[12] *Id.* Although this Article is principally concerned with private sector thefts, according to the Pentagon report, "China is using its computer network exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs." Gopal Ratnam, *Pentagon Accuses China of Cyberspying on U.S. Government*, BLOOMBERG (May 7, 2013), http://www.bloomberg.com/news/2013-05-06/china-s-military-ambitions-growing-pentagon-report-finds.html.

[13] Sanger et al., *supra* note 8.

People's Liberation Army of China for the alleged economic cyber espionage activities of Unit 61398.[14] Surely, the United States has by now recognized that some meaningful action should be taken to address this problem.[15] For many years, however, these "[Chinese] intrusions . . . provoked little American response."[16] But economic cyber espionage is no longer on the back burner. While administration officials once felt that "the theft of intellectual property was an annoyance, resulting in the loss of billions of dollars of revenue," their recent actions indicate "something has changed."[17]

Yet economic cyber espionage is not only a domestic concern. Just as it harms the United States' economy, economic cyber espionage also threatens international trade and, over time, stands to have a destabilizing impact on the global economic order. For this reason, as a top Obama Administration official has stated, "the international community cannot tolerate such activity from any country."[18] The international community has not, however, formulated a coherent response. Although various factors could be blamed for this tepid response, the lack of clearly established law regarding economic cyber espionage or institutionalized mechanisms for regulating this activity very likely impedes further

---

[14] David E. Sanger, *With Spy Charges, U.S. Draws a Line that Few Others Recognize*, N.Y. TIMES, May 20, 2014, at A8.

[15] Others have recognized the need for firm policy action: "[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 consequence." Evan F. Kohlmann & Rodrigo Bijou, *Planning Responses and Defining Attacks in Cyberspace*, 126 HARV. L. REV. F. 173, 174 (2013). As U.S. Representative Mike Rogers underscored to the House Committee on Intelligence:

> 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.
>
> Beijing is waging a massive trade war on us all, and we should band together to pressure them to stop. Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this scourge.

MANDIANT REPORT, *supra* note 8, at 1 (quoting *Cyber Threats and Ongoing Efforts to Protect the Nation: Hearing Before the H. Permanent Select Comm. on Intelligence*, 112th Cong. (2011) (statement of Rep. Mike Rogers, Chairman, H. Permanent Select Comm. on Intelligence)).

[16] David Feith, *The Weekend Interview with Timothy L. Thomas: Why China Is Reading Your Email*, WALL ST. J., Mar. 30, 2013, at A11.

[17] Sanger et al., *supra* note 8. This *New York Times* article also notes the "mounting evidence of state sponsorship" and the fact that "[t]he United States government is planning to begin a more aggressive defense against Chinese hacking groups." *Id*. Until now, it seemed as though most attention had been focused on the threat of a large-scale kinetic cyberattack. In actuality, others have argued that "[t]he most severe threats lie in attacks against critical infrastructure" and the theft of valuable economic and strategic intellectual property or systems. Kohlmann & Bijou, *supra* note 15, at 173.

[18] Feith, *supra* note 16.

action.[19] This anormativity and lack of institutional arrangements for enforcing norms on the international level has created a moral hazard and legal vacuum. In this landscape, economic cyber espionage is arguably perceived by some states, like China and others that are similarly motivated, as a rational strategy for advancing an upward economic trajectory.

This Article urges the international community to respond to the normative and institutional gap in the law in order to treat the problem of economic cyber espionage. In so doing, the Article explains how certain norms of public international law can be said to apply to cyber espionage and should be incorporated into the existing treaty-based framework of the World Trade Organization (WTO). The Article also explains why pressing claims in the WTO would be effective against perpetrators of economic cyber espionage. Namely, this approach would both solidify customary norms against economic cyber espionage and leverage a credible source of authority to curb cyber-violations. To advance this thesis, the Article proceeds in three Parts.

Part II considers the problem of economic cyber espionage through the lens of China's conduct, using the country as a case study. It explores the connection between China's rise to superpower status and its acts of cyber espionage in the United States. Specifically, Part II discusses China's pressure to expand economically and its dependence on continued integration within the world economic order, including through membership in key multilateral economic institutions like the WTO. Part II suggests that states with these types of strategic motives may be more prone to succumb to the moral and institutional ambiguity surrounding economic cyber espionage.

Part III addresses the anormativity surrounding economic cyber espionage. It argues that economic cyber espionage violates well-established norms of customary international law, such as sovereignty, non-intervention, and state responsibility. It discusses how the existing principle of state sovereignty also provides a derivative right to economic sovereignty, which is directly violated by economic cyber espionage. Moreover, to the extent states sponsor the economic cyber-intervention of non-state actors—i.e., cyberspies—those states can be held accountable under the doctrines of state responsibility or non-intervention. In short, Part III argues that economic cyber espionage is illegal under customary principles of international law, even if traditional espionage is not.

---

[19] *See* Kohlmann & Bijou, *supra* note 15, at 173 ("A lack of established international legal procedures, a hazy public understanding of the mechanics of electronic intrusions, and cyberterrorists' exponentially faster operational tempo (all combined with the extreme challenges involved in definitively identifying perpetrators on the Internet) have allowed some lawless actors to operate with a surprising sense of impunity.").

Part IV suggests an institutional mechanism for enforcing these rights through the WTO. It first points out that the customary norm of economic sovereignty, as an aspect of the lex generalis, applies in conjunction with existing treaty-based rights under the WTO agreements, which is a lex specialis. By interpreting the WTO treaty rules in the context of the lex generalis of economic sovereignty and non-economic intervention, member states may arguably assert a claim under the WTO's Dispute Settlement Understanding ("DSU") against any member state that engages in or sponsors economic cyber espionage. On that basis, Part IV urges the United States to assert a claim in the WTO against member states that violate its economic sovereignty through economic cyber espionage. In the specific case of China, Part IV argues that the WTO—as the anchor of the international economic order and thus a necessary role-player in China's plan to obtain superpower status—has the ability to ensure Chinese compliance. And given the procedures of the WTO dispute resolution mechanism, China would be likely to engage cooperatively with the process, avoiding unnecessary confrontation between the United States and China or a deterioration in U.S.-Sino relations.

II. UNDERSTANDING THE THREAT: WHY STATES ENGAGE IN ECONOMIC CYBER ESPIONAGE

This Article begins by considering, from a political and international relations perspective,[20] the possible strategic motivations that drive states to engage in economic cyber espionage. In deconstructing the particular case of China, Part II suggests that economic cyber espionage may be state-driven and not purely private conduct, bringing it within the bounds of public international law. Moreover, it demonstrates that the motivation to engage in economic cyber espionage is two-fold: to achieve economic expansion and avoid global alienation. In this circumstance, the rules of law and dispute settlement mechanisms of a multilateral economic institution, like the WTO, would be effective in persuading such a state to abandon this activity. Part II concludes that other states with similar motives are also likely to take advantage of the normative and institutional vacuum that exists in the international law on economic cyber espionage.

A. *Power Transition in the Twenty-First Century World Order*

International relations scholars have studied the impact of states' efforts to advance their status in the global order. Power transition theory presents one particular approach to analyzing shifts in the global order that

[20] As President Barack Obama has noted, in many ways, the "old architecture" of international law is "buckling under the weight of new threats." Remarks on Accepting the Nobel Peace Prize in Oslo, Norway, 2009 DAILY COMP. PRES. DOC. 985, at 2 (Dec. 10, 2009).

accompany transitions of power between states.[21] According to the basic tenets of the theory, which was first developed by A.F.K. Organzski and later refined by Robert Gilpin, war is the likely consequence of power transitions in which the challenging state is both dissatisfied with its position and has or is near to parity with the dominant state.[22] War, however, is not an inevitable outcome of a power transition.[23] In fact, the post-World War II global order, largely built on multilateral institution and alliance, is conducive to peaceful power transitions, including China's rise to superpower status. By design, states transitioning to power in the contemporary world order require the support of these various legal institutions. In theory, then, would-be superpowers should want to be careful to avoid a disruption in their relationships with these institutions.

1. *The Factors that Influence China's Rise*

China faces intense pressure to expand economically. Theories that explain why states seek to expand territorially provide some insight into why aspiring superpower states, like China, seek to expand in the economic space.[24] For instance, according to the theory of "lateral pressure," developed by Nazli Choueri and Robert North, "States experiencing high rates of population growth and technological change require increasing stocks of resources to fuel further economic development. Over time, states find that they lack resources within their boundaries and thus face mounting 'lateral pressure' to expand abroad."[25] Although this theory has been applied in the context of physical resources,[26] economic expansion today also requires technology and intellectual property.[27] Consistent with this theory, as China's growth outstrips its technological resources, it may seek out these resources abroad.[28]

---

[21] Jack S. Levy, *Power Transition Theory and the Rise of China*, *in* CHINA'S ASCENT: POWER SECURITY AND THE FUTURE OF INTERNATIONAL POLITICS 11, 12 (Robert S. Ross & Zhu Feng eds., 2008) [hereinafter CHINA'S ASCENT].

[22] *Id.* at 12–14.

[23] *See* M. Taylor Fravel, *International Relations Theory and China's Rise: Assessing China's Potential for Territorial Expansion*, 12 INT'L STUDS. REV. 505, 506 (2010) ("[S]cholars . . . note that some transitions have been peaceful, such as the one between the United States and the United Kingdom in the late nineteenth century.").

[24] *See id.* at 513 ("China today appears to fit the criteria of an 'alpha' state prone to lateral pressure . . . . As China's economy has developed rapidly over the past two decades . . . its need for resources has grown dramatically.").

[25] *Id.*

[26] *See id.* (discussing China's need for various "products and commodities . . . such as petroleum or arable land").

[27] *See* Sanger & Landler, *supra* note 1 ("Chinese academics and industrialists say that if China is to maintain its annual economic growth . . . it needs a steady inflow of new technology.").

[28] *See* Fravel, *supra* note 23, at 513 (explaining that, under the theory of lateral pressure, states often "believe that . . . [resources] need to be captured or controlled through conquest").

China also faces internal pressure to expand economically. Its desire to be a "rich and strong country" is centuries old,[29] but has intensified during the last few decades.[30] Chinese leaders apparently maintain that the time is ripe for China to advance technologically and grow its economy.[31] These messages have cultivated an economically-oriented national mentality.[32]

A national expectation of growth and technological advancement has a powerful effect on Chinese foreign policy and strategy. International relations theory recognizes that "collective ideas . . . 'matter' in [shaping] foreign policy."[33] As one scholar explained, Chinese foreign policy is, in part, a function of the "expectations it generates in the domestic arena and the results that are experienced."[34] Thus, meeting the economic expectations they have created is a priority for Chinese leaders.[35] As such, China's aim to rise within the global order is arguably a means to an end of national economic development.

2. *China Depends on Integration Within the International Economic Order*

China's ability to expand economically depends on its integration within the world economic order.[36] As one China specialist has explained:

> China has benefitted tremendously from its participation in the existing international economic order. Indeed, China has risen precisely by deepening its engagement with existing institutions, not challenging them. To date, China's economic development has occurred through the relative openness of its economy to trade and foreign investment. In return, China has become increasingly dependent on such

---

[29] Jeffrey W. Legro, *What China Will Want: The Future Intentions of a Rising Power*, 5 PERSP. ON POL. 515, 517 (2007); *see also* Fravel, *supra* note 23, at 518–23 (discussing domestic pressures for expansion, which include nationalism).

[30] In 1997, Jiang Zemin reportedly reminded China that it "seeks 'the goal of being prosperous and strong'—an aim shared by Chinese leaders . . . throughout the ages." Legro, *supra* note 29, at 517 (quoting *Jiang Zemin's Report at the 15th National Congress of the Communist Party of China*, FED'N AM. SCIENTISTS, http://www.fas.org/news/china/1997/970912-prc.htm (last visited Apr. 15, 2014)).

[31] FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS, *supra* note 4, at 5.

[32] *See* Legro, *supra* note 29, at 525 (noting that China's leaders justify integration into the international order based on "economic development" and "bettering the living standards of Chinese citizens").

[33] *Id.* at 522.

[34] *Id.* at 524.

[35] *See id.* at 525 ("[T]he legitimacy and popular support of the government does not rest on socialist ideology, but instead on economic performance. 'Well-off Society' not 'Workers Unite' is the national mantra.").

[36] *See id.* ("The first, and most important, justification of [China's] current policy is that integration within the existing national order provides the best means for national economic development.").

openness for high rates of economic growth.[37]

China has thus sought to avoid instigating the creation of anti-China coalitions, which could threaten its "continued economic development" and ostracize it from the global economic community.[38]

For these reasons, China's relationship with the United States is strategically delicate. Although the world is becoming increasingly multipolar, the United States may still occupy the role of hegemon.[39] This power dynamic has made it difficult for China to balance the United States,[40] and China has chosen instead to "bandwagon" or cooperate with the United States.[41] Although internally China may desire to resist perceived U.S. dominance,[42] an outwardly aggressive policy would disserve its ultimate aim, as the United States has been a proponent of China's assimilation into the economic order that has supported its rise.[43] As the next Section argues, if China feels pressure to appear peaceful while at the same time amassing the resources it needs to propel itself toward superpower status,[44] economic cyber espionage may seem like the ideal strategy.

---

[37] Fravel, *supra* note 23, at 511 (citation omitted).

[38] *Id.* at 510.

[39] *See* Matthew Happold, *Introduction* to INTERNATIONAL LAW IN A MULTIPOLAR WORLD 1, 2 (Matthew Happold ed., 2012) ("[T]he international system appears to be experiencing a tendency toward multipolarity . . . ."); Zhu Feng, *China's Rise Will Be Peaceful*, *in* CHINA'S ASCENT, *supra* note 21, at 34, 36–37 (discussing U.S. hegemony dynamics in the face of a "rising China").

[40] *Id.* at 37. Just as China cannot internally balance U.S. power, it cannot persuade any partners to try to do so with it. *See id.* at 42–43 (noting that an attempt to balance would be "ineffective" and as a result there is "little incentive . . . to attempt to weaken U.S. power" through external measures and coalitions like "reordering either the global or regional alignments").

[41] *Id.* at 43, 44.

[42] *Id.* at 39. Resistance to U.S. power has become a matter of national pride as "Chinese blogs are full of national rhetoric accusing the United States of seeking to keep China bowed and humbled." Zachary Karabell, *Do American Politicians Even Care About the Rise of China Anymore?*, ATLANTIC, (June 7, 2013), http://www.theatlantic.com/politics/archive/2013/06/do-american-politicians-even-care-about-the-rise-of-china-anymore/276663.

[43] *See* Tom Johnson, *Clinton Pushes Open Trade*, CNNMONEY (Jan. 29, 2000), http://money.cnn.com/2000/01/29/economy/davos_clinton/ (describing how President Clinton supported China's entry to the WTO); Phillip C. Saunders, *The U.S. Isn't Trying to Contain China*, FOREIGN POL'Y (Aug. 23, 2013), www.foreignpolicy.com/articles/2013/08/23/the_united_states_is_not_trying_to_contain_china (arguing that the U.S. is "working to expand China's role in international organizations and increase U.S. access to China's market," rather than trying to contain China, and noting that trade between the United States and China increased during the first half of 2013 and reached $244 billion). As Ashley Tellis argues, from the U.S. perspective, a policy of economic containment could not be successful now in light of China's integration in the world economic order. ASHLEY J. TELLIS, BALANCING WITHOUT CONTAINMENT: AN AMERICAN STRATEGY FOR MANAGING CHINA 8–9 (2014); *see id.* at 19 (noting that "the American polity has not yet responded to the growth of Chinese power with the seriousness and urgency that it displayed . . . in regard to the Soviet threat").

[44] *See* Fravel, *supra* note 23, at 511 ("In the early 2000s, Chinese political elites began to frame China's foreign policy around the concept of 'peaceful rise.'").

B. *China's Grand Strategy for Rising*

These strategic considerations may explain why a state like China is not necessarily interested in expanding its power by physical force or other overtly antagonistic strategies.[45] As Gao Cheng argues, for some rising powers there appears to be a "deeper economic logic" behind the drive to expand.[46] This Section considers why economic espionage may appear to be a logical or rational strategy to Chinese decision-makers.

1. *China's Peaceful Rise*

An economic expansionist rising in the twenty-first century, such as China, is unlikely to aggress against the international economic community.[47] In China's case, its leaders no doubt recognize that a "confrontational and aggressive foreign policy" would harm China's economic development.[48] Aggressive foreign policies would "damage . . . decades of economic reforms in terms of lost trade, foreign investment, and technology, and, more generally, its participation in an international order that has facilitated greatly its rise."[49] China is therefore expected to pursue a strategy of "reassurance" vis-à-vis the international community.[50]

Likely for these reasons, in the early twenty-first century Chinese political elites began to characterize China's foreign policy "around the concept of 'peaceful rise.'"[51] The image of the peaceful riser was "strategic, designed to convey a benign and non-threatening image to other states, reassuring them about China's growing capabilities."[52] And China has taken various steps to solidify its image as a peaceful riser. For example, it has abided by Confucian values, endeavored to "conjure up a collective historical memory across East Asia," and spread Chinese

---

[45] *See* Gao Cheng, *Market Expansion and Grand Strategy of Rising Powers*, 4 CHINESE J. INT'L POL. 405, 412 (2011) (explaining that "the specific means through which [rising powers] choose to expand . . . depend primarily on a cost-benefit analysis" and that "using force to change the status quo is not necessarily the path that a rising power will follow").

[46] *Id.* at 411. Cheng argues, "[A]s a state rises in the industrial era . . . the basic goal of its grand strategy is to achieve economic development." *Id.* Cheng departs from traditional power transition theory (among others) and asserts that such arguments "fail to consider the strategy guiding China's rise as a choice based on industrial needs." *Id.* at 444. He contends that "[t]he strategies great powers follow in rising accord with an economic principle." *Id.*

[47] *See* Feng, *supra* note 39, at 36 ("Many scholars stress that China's extensive participation in globalization and normative economic diplomacy may mitigate its revisionist objectives and may socialize it into the existing order."); *see also* Fravel, *supra* note 23, at 506 (suggesting the utility of conducting a cost-benefit analysis to assess whether China's rise will be aggressive).

[48] Fravel, *supra* note 23, at 511.

[49] *Id.* at 506.

[50] *See id.* at 510 (arguing that China will pursue a grand strategy of "reassurance, which is keyed to participation in the existing international order and preventing the formation of a counter-balancing coalition that could block or limit China's continued economic development").

[51] *Id.* at 511.

[52] *Id.*

academic thinking on a more global scale.[53]

Yet China, which has been growing at a rapid pace in the past several decades,[54] naturally requires resources to sustain that growth. The inputs needed to fuel an expanding economy today are not only physical but also, importantly, technological and innovative.[55] Like other great powers before it, China is likely focused on "obtaining the necessary factors of production, resources, and markets" to propel its rise to superpower status.[56]

These economic pressures and constraints leave a state such as China in a difficult strategic situation. On the one hand, it must avoid outward displays of antagonism toward the international economic order. On the other, to maintain its progression to superpower status, it must continue to push its economy to the next level, feeding this expansion with what it perceives to be the necessary technological and scientific resource inputs.

2. *A Grand Strategy of Cyber Espionage*

A grand strategy of economic cyber espionage could, in theory, serve China's aim of maintaining a peaceful image while expanding economically at a rapid pace—particularly when targeted against the United States or another superpower that has made significant technological and innovative advancements.[57] The U.S. private sector, as a leader in technological development and a "central player in global financial and trade networks," is an especially attractive target for economic cyber espionage by a state that is eager to make rapid gains in its own technological and economic fields.[58] For an aspiring economic superpower, it may well seem that "economic espionage [is] an essential tool in achieving national security and economic prosperity," and China may continue to be one of the most "aggressive and capable collectors of sensitive US economic information and technologies . . . in cyberspace."[59]

---

[53] Gordon C.K. Cheung, *International Relations Theory in Flux in View of China's "Peaceful Rise,"* 26 COPENHAGEN J. ASIAN STUDS. 5, 12–13 (2008); *see id.* at 12–17 (describing China's use of soft power).

[54] *See* ZULIU HU & MOHSIN S. KHAN, INTERNATIONAL MONETARY FUND ECONOMIC ISSUES REPORT 8: WHY IS CHINA GROWING SO FAST? 1 (1997) (noting that since 1978 China has grown at more than nine percent per annum, with an almost four hundred percent rise in per capita income).

[55] *See supra* notes 25–28 and accompanying text; *see also* Levy, *supra* note 21, at 18–19 (suggesting that some predictions made under power transition theory may not sufficiently or precisely account for the impact of innovation).

[56] Cheng, *supra* note 45, at 412.

[57] *See* Sanger & Landler, *supra* note 1 ("Chinese academics and industrialists say that if China is to maintain its annual economic growth rate of 7 or 8 percent, it needs a steady inflow of new technology. That could make the Chinese reluctant to cut back on the systematic theft of intellectual property.").

[58] FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS, *supra* note 4, at i.

[59] *Id.* at ii, 4.

Cyber espionage also has the advantage of offering plausible deniability. To be sure, China has rigorously denied accusations of economic cyber espionage, calling it "unprofessional and groundless to accuse the Chinese military of launching cyberattacks without any conclusive evidence."[60] China's Defense Ministry maintains that "[t]he Chinese military has never supported any hack attacks" and suggests that the cyberattacks have been perpetrated by transnational actors with "anonymous characteristics."[61] On balance, a program of economic cyber espionage may seem, from the perspective of a state like China, to have several benefits and few drawbacks. Cyber espionage fuels technological growth while, at the same time, "soft balancing" the United States.[62] Moreover, due to its covert nature, China may preserve its image as a peaceful riser and represent to the United States that it is not responsible for these intrusions. And ultimately there is, as of yet, no tangible legal repercussion.

Yet a firmer response from the international community, grounded in principles of international law, may alter this perspective and reduce the appeal of economic cyber espionage.[63] As the next two Parts will show, a legal response is not only appropriate and potentially effective, but it also sends a broader message that is conducive to global stability: in the twenty-first century, superpowers may rise in the global order provided they do so within the rule of law. To that end, Part III argues that certain norms of public international law already provide a basis for asserting this conduct as unlawful.

---

[60] Craig Timberg & Ellen Nakashima, *Chinese Suspected in Attack on Post's Computers*, WASH. POST., Feb. 2, 2013, at A1; *see also* Sanger, *supra* note 11 (quoting Hua Chunying, a spokeswoman for the Chinese Ministry of Foreign Affairs, as saying "China . . . resolutely oppose[s] all forms of hacker attacks").

[61] Timberg & Nakashima, *supra* note 60. The Chinese have continued to deny these allegations in the face of a U.S. criminal indictment charging economic cyber espionage and theft of trade secrets. *E.g.*, Timothy M. Phelps & Julie Makinen, *U.S.-China Cyber Battle Grows; Five Chinese Military Officials Are Accused of Stealing U.S. Corporate Secrets. Beijing Calls Charges "Fabricated."*, L.A. TIMES, May 19, 2014, at A1.

[62] *See* Feng, *supra* note 39, at 50 (describing soft balancing as engaging in "measures [that] do not directly challenge a unipolar state's military preponderance, but rather seek to delay, complicate, or increase the costs of that state's exercise of its power").

[63] Others believe that the rules of law on warfare justify a counter-attack in certain cyber-attack situations. *See, e.g.*, Michael N. Schmitt, *Cyberspace and International Law: The Penumbral Mist of Uncertainty*, 126 HARV. L. REV. F. 176, 177 (2013) ("At a certain level of severity, cyberoperations cross the 'armed attack' threshold, thereby allowing states to defend themselves with force, including cyberforce, pursuant to Article 51 of the U.N. Charter and customary international law. The concept of armed attacks at least includes cyberoperations causing death, injury, or significant damage."); *see also* Jan E. Messerschmidt, Note, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275, 279 (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 hack*back*." (emphasis added)).

III. CUSTOMARY NORMS AND ECONOMIC CYBER ESPIONAGE

This Part argues that the international community should recognize economic cyber espionage as prohibited under established principles of customary international law. Section A first explains why economic cyber espionage may seem to fall within a gap in the law. Though prosecutable as a domestic crime, China's state-sponsored cyberactions may be effectively outside the United States' reach, even if personal jurisdiction could be said to apply.[64] More importantly, this conduct seems untouchable by international law. Historically, espionage has existed in the hinterlands—neither expressly condoned nor condemned. Yet with the capacity to cripple states' economies and de-stabilize the global economic order at a rapid and uncontrollable pace, economic cyber espionage should be treated differently.

Section B next argues in favor of a modernized interpretation of existing principles of international law. Specifically, it considers how existing norms—first recognized decades ago—should be interpreted today to fit the contemporary threat of economic cyber espionage. Although existing norms of state sovereignty and non-intervention have customarily been applied to safeguard the territorial integrity of states, today serious threats to security are mounted from cyberspace. These invasions are aimed to alter states' economic powers and relationships, not their borders. Accordingly, Section B argues that the principles of state sovereignty and non-intervention, which provide derivative rights to economic sovereignty and non-economic intervention, also prohibit economic cyber espionage. By extension, states may be held accountable for violating these principles either directly or through their sponsorship of these cyber actions.

A. *The Espionage Lacuna in the Law*

This Section explains the various bodies of domestic and international law that could regulate economic cyber espionage but, for various reasons, cannot effectively do so or simply do not yet recognize this conduct as illegal. The result is a perceived lacuna in the law surrounding economic cyber espionage. Subsection 1 discusses this lacuna and Subsection 2 explains why it is an illusion and why existing international law norms could, in fact, fill this space.

1. *U.S. Domestic Law and Economic Cyber Espionage*

The covert theft of U.S. intellectual property and industrial secrets is well covered by domestic criminal law. For one, the Economic Espionage

---

[64] For a discussion of the extraterritorial application of the criminal law, see Sara A. Solow, *Prosecuting Terrorists as Criminals and the Limits of Extraterritorial Jurisdiction*, 85 ST. JOHN'S L. REV. 1483, 1508–16 (2011).

Act of 1996 directly criminalizes this behavior.[65] The statute provides that economic espionage occurs when an actor knowingly or intentionally commits an offense that "will benefit any foreign government, foreign instrumentality, or foreign agent," and "knowingly": (1) steals or obtains a trade secret by "fraud, artifice, or deception" or by other unauthorized means; (2) "conveys a trade secret" by various methods of copying (without authorization); or (3) "receives, buys, or possesses a trade secret knowing" it was stolen or otherwise taken without authorization.[66] Given the breadth of this statute, it is surely intended to capture economic espionage that is perpetrated in cyberspace and with cybertools.[67] In fact, the United States has recently used this statute to charge five Chinese military hackers for acts of economic cyber espionage, among other crimes, against U.S. companies.[68]

In reality, however, a U.S. prosecution for economic cyber espionage likely does not loom large for foreign actors such as these.[69] It has been noted that "[e]spionage is nothing but the violation of someone else's laws."[70] Thus, for U.S. law to serve as a meaningful deterrent to foreign actors, the United States must be able to apprehend and punish these actors within the four corners of its domestic law. Yet, as a practical matter, cyberspies can indefinitely evade prosecution if their host state refuses to cooperate. In the case of China, for example, under the terms of the U.S.-Hong Kong Extradition Treaty, China can refuse to extradite a person within its borders if "surrender implicates the 'defense, foreign affairs or essential public interest or policy' of the People's Republic of China."[71] Thus the efficacy of the United States' criminal action will depend on

---

[65] 18 U.S.C. §§ 1831–39 (2012).

[66] *Id.* § 1831.

[67] Of the seven cases brought under the Economic Espionage Act in 2010, six related to China. COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., THE IP COMMISSION REPORT 42 (2013).

[68] Indictment, United States v. Wang Dong, No. 14-118 (W.D. Pa. May 1, 2014), *available at* http://www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf.

[69] *See* COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., *supra* note 67, at 41 (observing that it is "notoriously difficult" to curb trade-secret theft and economic espionage under the current U.S. legal framework—with the latter offense being particularly problematic to prove because it "requires that the act be done with intent to benefit a foreign nation"); *id.* at 42 (noting that the extraterritorial reach of the Economic Espionage Act "remains limited"). For an account of how narrow judicial readings have constrained the Economic Espionage Act's efficacy, see generally Robin L. Kuntz, *How Not to Catch a Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets*, 28 BERKELEY TECH. L.J. 901 (2013).

[70] Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1077 (2006) (quoting *U.S. Intelligence Agencies and Activities: Risks and Control of Foreign Intelligence: Hearings Before the H. Permanent Select Comm. on Intelligence, Part 5*, 94th Cong. 1767 (1975) (statement of Mitchell Rogovin, Special Counsel to CIA Director)).

[71] *Treaty Gives Hong Kong Option to Reject Snowden Extradition to the U.S.*, S. CHINA MORNING POST (June 10, 2013), http://www.scmp.com/news/hong-kong/article/1257639/treaty-gives-hong-kong-option-reject-snowden-extradition-us. For the text of the treaty, see Agreement for the Surrender of Fugitive Offenders, U.S.–H.K., Dec. 20, 1996, T.I.A.S. No. 98-121.

China's cooperation and the "hope[] that Beijing will 'respect our criminal justice system and let justice take its course.'"[72] But given Chinese officials' denials of economic cyber espionage activities,[73] it seems unlikely that its government will submit the accused to U.S. courts.

U.S. law also addresses the problem of economic cyber espionage indirectly through the Arms Export Control Act of 1976.[74] It gives the Executive the "authority to control the export of defense articles and services."[75] However, as a practical matter, the Arms Export Control Act is similarly limited in its application to the problem of economic cyber espionage. On its face, it reaches bad actors within the United States who export prohibited items abroad.[76] Thus while the U.S. may be effective at prosecuting the U.S.-based conduits of technology and trade secrets, hackers and spies operating abroad may continue to act with legal impunity for jurisdictional reasons.

In sum, these domestic prohibitions—though forceful to the extent they apply—provide little deterrent to the continued perpetration of economic cyber espionage from outside actors. Criminal charges may ultimately be more symbolic than punitive. Another strategy, which works outside the U.S. criminal justice system and more directly implicates the cyber-hacking country's standing and success in the international economic arena, is needed to effectively curtail this conduct.

Moreover, the problem of economic cyber espionage is not one for the United States to solve alone. Economic cyber espionage is a threat that is international in nature, as it has the potential to upset the global economic order by destabilizing trade and distorting competition. As a threat to international security that is shared collectively by all members of the international community, this is a problem that international law can and should address.

2. *International Law and Espionage*

Currently, however, international law seems to tolerate espionage and,

---

[72] Ellen Nakashima & William Wan, *Chinese Military Unit Charged with Cyber-Espionage Against U.S. Firms*, WASH. POST (May 19, 2014), http://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html.

[73] *See China Denounces US Cyber-Theft Charges*, BBC NEWS (May 20, 2014), http://www.bbc.com/news/world-us-canada-27477601.

[74] 22 U.S.C. §§ 2751–2799aa-2 (2012).

[75] *The Arms Export Control Act*, U.S. DEP'T ST., DIRECTORATE DEF. TRADE CONTROLS, https://www.pmddtc.state.gov/regulations_laws/aeca.html (last visited Apr. 15, 2014).

[76] *See* 22 U.S.C. § 2778 (explaining that the Act applies to "persons of the United States involved in the export and import of such articles and services").

by extension, economic cyber espionage.[77] While some bodies of international law might be relevant to spying, none adequately address this particular threat.[78] Indeed, there is no clear consensus among states on the legal nature of espionage or whether states enjoy a right at international law to complain of it.[79] Oddly, espionage remains "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."[80] Although no international agreement expressly condones espionage, "states do not reject it as a violation of international law."[81] This historical acceptance has given espionage the appearance of lawful activity, "grounded in the [states'] recognition that 'custom' serves as an authoritative source of international law."[82] To the extent states are concerned with espionage at all, it is espionage at wartime that vexes them most.[83] Meanwhile, international espionage at peacetime is virtually ignored.[84] The academic literature has been equally silent.[85] Indeed, "[l]eading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate in the event of capture."[86] Thus there appears to be a lacuna in the international law on espionage.

States may perceive that economic cyber espionage exists in the same grey area as peacetime espionage, which is considered "an unfriendly act"

---

[77] *See* David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies*, 17 ASIL INSIGHTS, no. 10, 2013, at 1, 2, *available at* http://www.asil.org/sites/default/files/insight130320.pdf (noting that "[t]he 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").

[78] *See id.* ("[R]ules on armed conflict and on diplomatic relations in peacetime[] do not prohibit or seriously constrain . . . economic espionage.").

[79] *See* A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 602 (2007) (using a three way split in existing literature as support for a "thesis that espionage is beyond international consensus").

[80] Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1091 (2004).

[81] *Id.* at 1094.

[82] *Id.*

[83] *See* Chesterman, *supra* note 70, at 1078 (noting that spies caught during wartime have historically been subject to severe treatment, "reflect[ing] the danger posed by espionage and the difficulty of guarding against it"). That said, according to Grotius, sending spies in war is "beyond doubt permitted by the law of nations." *Id.* (quoting HUGO GROTIUS, DE JURE BELLI AC PACIS LIBRI TRES 655 (James Brown Scott ed., Francis W. Kelsey trans., 1925) (1646)) (internal quotation marks omitted).

[84] *See* Radsan, *supra* note 79, at 603 ("[A]ttention in the law to peacetime espionage has lagged behind the development of other international norms concerning intelligence gathering." (quoting Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 321 (1996)) (internal quotation marks omitted)).

[85] *Id.* at 602 (quoting Richard A. Falk, *Foreword* to ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at v (Roland J. Stanger ed., 1962)).

[86] *Id.* (quoting Falk, *supra* note 85, at v) (internal quotation marks omitted).

but not a violation of international law.[87] Even if they do not view peacetime espionage as legal, per se, states may nonetheless tolerate this form of espionage because they perceive it to be in their self-interest.[88] By this account, countries are likely "realistic" about the fact that they will commit espionage in other countries and want to safeguard their own option for continuing this practice.[89] In any state's estimation, endorsing norms against the practice of peacetime espionage would hinder its security as much as—if not more than—it enhances it. As one scholar has argued, in this way states "preserve[] the practice [of espionage] as a tool by which to facilitate international cooperation."[90] On this view, the "rules" of espionage are not prescribed by law, but rather "are situational."[91]

However, it would be a mistake to afford the same legal treatment to economic cyber espionage.[92] For one, unlike traditional espionage, economic cyber espionage takes place on a much larger scale. The volume of information stolen via cyberspace, using cybertools, is much more significant and happens at a quicker pace than traditional human or technical intelligence gathering.[93] Moreover, the penetration of computer systems and databases is far more difficult to detect and stop than traditional human espionage.[94] Finally, with economic espionage, there is no custom of reciprocity or cooperation that states should be concerned about preserving. With traditional espionage, which focuses on state-strategy and military capacity, one can assume that state spying ensures the collective security of all nations. A state's knowledge about its neighbors' military capabilities allows it to hedge against or prevent a threat. This, in turn, might decrease the likelihood of any successful or surprise attack. In this way, traditional espionage functions as a structural constraint against

---

[87] *Id.* at 603 (quoting Demarest, *supra* note 84, at 347) (internal quotation marks omitted). Radsan also points to scholars who view peacetime espionage as illegal. *Id.* at 604–05.

[88] *Id.* at 605–06; *see* Chesterman, *supra* note 70, at 1090 ("One of the reasons for the unusual treatment of espionage in diplomatic relations is the principle of reciprocity—the recognition that what one does to another state's spies will affect that state's treatment of one's own agents. The underlying assumption of this arrangement is that intelligence collection is an important or at least an unavoidable component of diplomatic relations.").

[89] Radsan, *supra* note 79, at 606.

[90] Baker, *supra* note 80, at 1092.

[91] Radsan, *supra* note 79, at 606.

[92] *See generally* Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389 (2006) (describing how the nature of economic espionage has changed significantly due to the proliferation of information in cyberspace).

[93] *See id.* at 395–97 (comparing traditional approaches to economic espionage to those used in the Internet age).

[94] *See id.* at 397 ("A victimized government, corporation, or individual today will have an exceptionally challenging task [of] merely identifying the cyber collector who has targeted their information. This is, of course, assuming the victim is even aware of the fact that he or she has been subject to an attack!").

open conflict and preserves global stability. Yet there is no such corresponding benefit to global security that accrues from economic cyber espionage. In the most likely scenario, the states that perpetrate this economic spying are motivated to do so because they are still developing and lack desirable technology, innovation, or best practices.[95] Therefore, no state would be incentivized to preserve its option to return the favor. The spying state merely harms the victim state's incentive to innovate, natural comparative advantages, and robustness as a trading partner.[96]

For these reasons, it is a mistake not to draw any legal distinction between traditional espionage and economic cyber espionage. Section B urges the international community to take seriously a state's claim that such conduct violates well-established norms of international law as they are interpreted to apply to this modern problem.

B. *The International Law Norms Against Economic Cyber Espionage*

The international community has begun to appreciate that the "old architecture" of international law is "buckling under the weight of new threats."[97] This realization and desire to move forward presents a key moment in which international law can evolve to address the growing threat of economic cyber espionage. This Section first considers why the time is ripe for this normative evolution and then considers which norms must evolve.

1. *A "Constitutive Process" for Normative Evolution*[98]

First, one might ask, how is international law made or evolved? The answer to this question is important to any argument for a new prescription—after all, there is no definitive "central legislator" for

---

[95] *See* LEWIS, *supra* note 3, at 44–45 (describing the experience of China, where political leaders identified "an immense lag" in technology in the post-Mao era and "made the illicit acquisition of technology a central element of China's economic opening to the West").

[96] *See id.* at 45 ("The theft of IP and confidential business information . . . appears to cost developed countries much more . . . by damaging economic competitiveness.").

[97] *See supra* note 20.

[98] Professors McDougal, Lasswell, and Reisman originated this theory by which they "refer to authoritative decision as process." Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, *The World Constitutive Process of Authoritative Decision*, 19 J. LEGAL EDUC. 253, 258 (1967). By this theory:

> An examination of the world community context corroborates the view that, within limits, a global system of public order has come into existence that comprises a constitutive process in which authoritative decision institutions have taken form and which utilizes these institutions to protect and extend itself and also to contribute to the shaping and sharing of values other than power.

Id. at 257.

international law,[99] and the prospect of new law depends, in large part, on whether international law's processes of generating norms are properly activated and engaged.[100] This is equally true with respect to economic cyber espionage. Even though existing norms can be interpreted to prohibit it, deploying these norms in a new way requires some normative evolution.

As Professor Michael Reisman has theorized, international law in the contemporary global order is made pursuant to a multi-dimensional, "constitutive process."[101] This process is "the context which produces international law."[102] By this account, today there are various dimensions of the world community that play a role in the shaping of international law, including "[t]he economic, environmental and resource dimension of the world community."[103] The economic dimension ushers into the international law-making process the voices and concerns of various players in the transnational market,[104] including business entities, corporations, and research engines from academia and the non-profit sector. In this modern-day world order, these interests can and do serve to generate "new principles and governance structures" to regulate international activity,[105] as these participants recognize the "utility of maintaining and enhancing a stable transnational economic environment that enables their various enterprises to flourish."[106] On this theory, 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 those in the private economic sector.[107]

This has led to a "contemporary open process of lawmaking" that is

---

[99] Joost Pauwelyn, *The Role of Public International Law in the WTO: How Far Can We Go?*, 95 AM. J. INT'L L. 535, 536 (2001).

[100] *See* McDougal et al., *supra* note 98, at 255 (discussing "[a] world constitutive process of authoritative decision [which] includes the establishment of an authoritative decision process in the world community, and its subsequent maintenance, modification, or even termination").

[101] *See generally* W. MICHAEL REISMAN, THE QUEST FOR WORLD ORDER AND HUMAN DIGNITY IN THE TWENTY-FIRST CENTURY: CONSTITUTIVE PROCESS AND INDIVIDUAL COMMITMENT 101–17 (2012) (discussing "the world constitutive process and its decision functions"); *see also* McDougal et al., *supra* note 98, at 279–80 (observing that "[t]he outcomes that flow from the constitutive process are the decisions that delimit authoritative and controlling participation in the world arena," including "prescriptions" regarding, inter alia, "constitutive norms").

[102] REISMAN, *supra* note 101, at 46.

[103] *Id.* at 58. "That process is, in the broadest sense, the context which produces international law, within which international law and those practising it have to operate, and which, in turn, they are trying, in various ways, to direct and regulate." *Id.* at 46.

[104] *Id.* at 60–61.

[105] *Id.* at 61.

[106] *Id.* at 60.

[107] *See id.* at 137 ("This dynamic and open process of communication involves a wide range of non-State actors who play critical roles in the shaping and sustaining of expectations of right behaviour.").

"more dynamic and fluid" than before and "often respond[s] to perceptions of crisis."[108] A fluid, democratic, and reactive system of international law should mean that norms, as they exist, are constantly subject to change and growth, responding to the popular concerns of international law's economic participants.[109] No longer is international law solely the product of lex scripta, that is, the usual state-driven methods of lawmaking such as treaties and other international agreements; it may also develop more organically.[110]

All this is to say that the creation of norms regarding economic cyber espionage does not depend on the formal machinery of international lawmaking. Instead, they can evolve immediately, in response to the concerns of those affected—business, industry, the media, and the non-profit world—as states and powerful economic multilateral institutions are influenced to reach consensus that such conduct is unlawful.[111]

That consensus already has a rallying point in existing principles of customary international law. As derived from the fundamental principle of state sovereignty, the following Subsection argues that states enjoy a right to economic sovereignty[112] that accrues to the state both for its benefit and for that of the private economic actors that exist under its aegis. It also argues that states should be held responsible for the cyber espionage that they sponsor.

2. *Economic Sovereignty and the Right to Non-Economic Intervention*

Since the Peace of Westphalia ended the Thirty Years War in 1648, the global community has ordered itself around a state-based system.[113] This

---

[108] *Id.*

[109] *See* REISMAN, *supra* note 101, at 136–37 ("Thus the modalities through which international law is being prescribed now range over a wide spectrum."); McDougal et al., *supra* note 98, at 261 ("All participants in world social process act in the constitutive process of authoritative decision.").

[110] REISMAN, *supra* note 101, at 136–37; *see also* Myres S. McDougal & W. Michael Reisman, *The Prescribing Function in World Constitutive Process: How International Law Is Made*, 6 YALE STUDS. WORLD PUB. ORD. 249, 250 (1980) ("The making of law is a decision function which may be conveniently described as prescription.").

[111] This Article considers the problem from the perspective of the United States. To the extent other nations and economies are threatened by economic cyber espionage, their interests will also build pressure for a change in the normative outlook.

[112] The general idea of economic sovereignty has existed in the academic literature for some time. *See, e.g.*, Alan M. Simon & Spencer Weber Waller, *A Theory of Economic Sovereignty: An Alternative to Extraterritorial Jurisdictional Disputes*, 22 STAN. J. INT'L L. 337, 348 (1986) ("Economic sovereignty encompasses the right to continue and preserve economic activities closely linked to the existence of the state.").

[113] *See* JOHN KISH, INTERNATIONAL LAW AND ESPIONAGE 83 (David Turns ed., 1995) ("The general principle of exclusive sovereignty over national territory is firmly established in customary international law. Each State exercises control over its national territory to the exclusion of all other States, and any limitation of this authority is subject to the consent of the territorial State.").

Westphalian system places the state and its "sovereignty at its core."[114] According to international relations scholars, "Westphalian" is "an 'institutional arrangement for organizing political life that is based on two principles: territoriality and the exclusion of external actors from domestic authority structures.'"[115] At base, "Westphalian sovereignty is violated when external actors influence or determine domestic authority structures."[116]

Though the Westphalian version of sovereignty has historically been linked to territorial control, the conceptual underpinnings of sovereignty are not necessarily limited to land or physical spaces. Instead, sovereignty is a principle that is mainly concerned with protecting national power bases and a state's exclusive right to control them.[117] It thus requires that "any limitation of this authority is subject to the consent of the . . . State."[118] Today, a state's ability to safeguard its sovereignty—the essential aspects of its statehood—depends not only on control of its borders, but also on control of its economy and private sources of wealth. Threats to these economic aspects of a state's integrity are increasingly mounted through cyberspace. It follows then that sovereignty also proscribes external attempts to manipulate or infringe on a state's national economic spaces (as defined to include the private sector), including those launched in cyberspace, even if such acts fall below a conventional threshold of force.[119]

Customary international law[120] also supports an expanded notion of

---

[114] Andreas Osiander, *Sovereignty, International Relations, and the Westphalian Myth*, 55 INT'L ORG. 251, 251 (2001); *see* Benjamin Straumann, *The Peace of Westphalia as a Secular Constitution*, 15 CONSTELLATIONS 173, 173 (2008) (noting that Westphalia is perceived as the "origin" of the principle of state sovereignty).

[115] Straumann, *supra* note 114, at 173 (quoting STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 20 (1999)).

[116] *Id.*

[117] *See* KISH, *supra* note 113, at 84 ("As general rules of international law safeguard the sovereignty of every State over its national territory, any limitation of territorial sovereignty depends on agreement between the territorial State and other States.").

[118] *Id.* at 83.

[119] Others have made the point that sovereignty applies in cyberspace. *See, e.g.*, Schmitt, *supra* note 63, at 177 ("States have a sovereign right to exercise control over cyberinfrastructure and activities on their territory as well as to protect them from harmful actions."); *cf.* Chesterman, *supra* note 70, at 1081 (noting that sovereignty suggests legal limits on espionage even when it falls below the threshold standard defining certain uses of force).

[120] According to Professor Michael Paulsen:

> [Customary international law] refers to the norms and practices of nations, apart from treaties or other written agreements. Within the regime of international law, it is "law" inferred from "a general and consistent practice of states followed by them from a sense of legal obligation." It is, in effect, a body of unwritten international "common law" principles.

sovereignty, which includes a concept of economic sovereignty that protects private sector actors that contribute to the nation's economic security. As the following discussion shows, international courts and tribunals have interpreted state sovereignty and the related principles of non-intervention and state responsibility quite broadly, without limiting them to the physical domain.[121] Particularly where, as here, a global threat is new and states have not yet had an opportunity to address it through practice, these legal precedents can "influenc[e] the subsequent practice of States and international organizations"[122] to apply the principle of economic sovereignty to prohibit economic cyber espionage.

a. A Broad Understanding of Non-Intervention

A state's sovereignty confers on it a right to be free from the unwanted intervention of another state.[123] The International Court of Justice (ICJ) considers this principle of non-intervention part of customary international law.[124]

In expounding on it, the ICJ expressed a broad view of sovereignty in *Nicaragua v. United States*.[125] There, the court considered whether the United States' support to the Nicaraguan *contras* was justified by the fact—if proven—that the Sandinista Government of Nicaragua was supplying arms to insurgents in El Salvador.[126] To evaluate the United States' justifications, the court considered the "principle of non-intervention in customary international law."[127] The ICJ found that "the support given by the United States, up to the end of September 1984, to the military and paramilitary activities of the *contras* in Nicaragua, by

---

Michael Stokes Paulsen, *The Constitutional Power to Interpret International Law*, 118 YALE L.J. 1762, 1800 (2009) (quoting RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 102(2) (1987)). According to the Statute of the International Court of Justice (ICJ), customary international law is "a general practice accepted as law." Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1055, 1060.

[121] The authors of the *Tallinn Manual* have made this point in their thorough and expert analysis of international law in cyberspace. Specifically, they explain that, based on their conclusion that "general principles of international law appl[y] to cyberspace," it follows that "legal concepts [such] as sovereignty, jurisdiction, and State responsibility" are part of "international cyber security law." TALLINN MANUAL, *supra* note 7, at 14. They refer to "the hostile use of cyberspace" and these principles' relationship to *jus in bello*. *Id.*; *see also* Schmitt, *supra* note 63, at 177 ("[A] thick web of international norms suffuses cyberspace."); *infra* Parts III.B.3.a–c.

[122] ICRC, *Assessment of Customary International Law*, http://www.icrc.org/customary-ihl/eng/docs/v1_rul_in_asofcuin (last visited Apr. 15, 2014); *see id.* ("[A] finding by an international court that a rule of customary international law exists constitutes persuasive evidence to that effect.").

[123] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 202 (June 27).

[124] KIMBERLEY N. TRAPP, STATE RESPONSIBILITY FOR INTERNATIONAL TERRORISM 30 (2011).

[125] *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. ¶ 201.

[126] *Id.* ¶¶ 93, 126, 128.

[127] *Id.* ¶ 201.

financial support, training, supply of weapons, intelligence and logistic support, constitute[d] a clear breach of the principle of non-intervention."[128] The court held:

> [I]n international law, if one State, with a view to coercion of another State, supports and assists armed bands in that State whose purpose is to overthrow the government of that State, that amounts to an intervention by the one State in the internal affairs of the other, whether or not the political objective of the State giving such support and assistance is equally far-reaching.[129]

In reviewing state practice on non-intervention, the court's concept of sovereignty was broader than physical territory principles:

> As regards . . . the content of the principle of non-intervention . . . in view of the generally accepted formulations, the 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.[130]

This ICJ holding confirms that coercion need not be by military force, but can result from any impediment to a state's ability to "decide freely" in matters that touch on any aspect of that state's sovereignty.[131] "[C]oercion," after all, was held to "define[], and indeed form[] the very essence of, prohibited intervention."[132] Arguably, the spying and stealing of economic property in cyber space can be seen as a form of coercion that impermissibly interferes with both the internal and external affairs of a state.[133]

---

[128] *Id.* ¶ 242.

[129] *Id.* ¶ 241.

[130] *Id.* ¶ 205. The *Tallinn Manual* experts reference the ICJ's *Nicaragua* holding during their articulations of various cyber security law principles. *E.g.*, TALLINN MANUAL, *supra* note 7, at 26, 44–47, 55, 58.

[131] *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. ¶ 205; TRAPP, *supra* note 124, at 31.

[132] *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. ¶ 205.

[133] As others have observed:

The *Nicaragua* decision thus supports an expansive customary norm that a state is sovereign in its economic—not only territorial—spaces, and that the principle of non-intervention gives rise to prohibitions on a state's interference in that economic space. The rigorous right to exclusive control over a state's economic affairs should also extend to protect the private-sector actors that comprise a critical component of the state's proprietary economic space. Economic sovereignty, as derived from the court's holding in *Nicaragua*, therefore imposes obligations on states to refrain from interfering with private-sector economic actors through the use of coercive tactics like economic cyber espionage.[134] As the following discussion shows, it also prohibits states from sponsoring or supporting such activity.

b. State Responsibility Based on Knowledge and Control

The *Corfu Channel* case holds that states may be held accountable for unlawful activity committed from within its territory if the circumstances suggest the state had knowledge of it.[135] *Corfu Channel* involved a dispute between the United Kingdom and Albania that was brought before the ICJ in 1947.[136] The case involved whether, among other things, Albania was responsible for laying mines that were struck by British ships while crossing the Corfu Channel in 1946.[137] The Channel had been declared free of mines in 1944, and so Britain argued that the mines had been recently laid, either by Albania or "with its connivance or knowledge."[138]

On April 9, 1949, the ICJ rendered its decision as to whether Albania could be held responsible for the mines.[139] Since there was no direct

---

> [T]he ICJ held that US financing of the *contras* did not amount to a breach of the prohibition of the use of force, although it was an illegal intervention in the domestic affairs of Nicaragua. By analogy, assistance with diplomatic assets or providing transportation or intelligence, none of which, by themselves, imply a use of force, could amount to a breach of the principle of non-intervention, but not the prohibition of the use of force.

TRAPP, *supra* note 124, at 31–32 (footnote omitted).

[134] *Cf.* Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 43 (Apr. 9) (separate opinion of Judge Alvarez) ("Sovereignty confers rights upon States and imposes obligations on them.").

[135] *See id.* at 18, 22–23 (majority opinion) (finding that Albania must have had knowledge of the mines that were in Albanian waters and that they were therefore responsible for their explosion). The *Tallinn Manual* interprets this opinion to mean that "[t]he obligation to respect the sovereignty of another State . . . implies that a State may not 'allow knowingly its territory to be used for acts contrary to the rights of other States.'" TALLINN MANUAL, *supra* note 7, at 26 (quoting *Corfu Channel*, 1949 I.C.J. at 22).

[136] Application Instituting Proceedings in Corfu Channel, 1949 I.C.J. Pleadings 8, 8 (May 22, 1947).

[137] *Corfu Channel*, 1949 I.C.J. at 27–28.

[138] Memorial of United Kingdom, Corfu Channel (U.K. v. Alb.), 1949 I.C.J. Pleadings 19, ¶¶ 73, 76 (Sept. 30, 1947).

[139] *Corfu Channel*, 1949 I.C.J. at 23.

evidence that Albania had known about the mines, the court considered circumstantial evidence.[140] The court found it "clearly established that the Albanian Government constantly kept a close watch" over the Channel, as evidenced by certain diplomatic notes protesting the passage of ships through the Channel as well as earlier firings on British ships.[141] This evidence persuaded the court that "whoever the authors of the minelaying were, it could not have been done without the Albanian Government's knowledge."[142] The court's holding in this regard confirmed that circumstantial evidence of a state's knowledge of an unlawful act committed within its territory can, in certain circumstances, be sufficient for holding that state responsible for it.

The principle of state responsibility evolved with the ICJ's decision in *Nicaragua v. United States*.[143] There, the court further refined the parameters of state responsibility and established an "effective control" test for attributing acts of non-state actors to the state.[144] But perhaps more important for economic cyber espionage was the International Criminal Tribunal for the former Yugoslavia's critical analysis of the *Nicaragua* test in *Prosecutor v. Tadic*.[145] In that case, the Appeals Chamber concluded that, with respect to organized groups, "overall control" should be the operative test, that is, whether the "state . . . has a role in organizing, coordinating or planning the military actions of the . . . group."[146] After *Nicaragua* and *Tadic*, a state may be held responsible for the unlawful actions of those putative non-state actors on its territory where the state has knowledge of this activity and some role in its orchestration. Precisely as Michael Schmitt points out, "international law . . . obligates states to ensure that cyberinfrastructure on their territory is not used for acts that unlawfully affect other states."[147]

---

[140] *Id.* at 18.

[141] *Id.* at 18–19. It also considered expert evidence that any minelayers would have been seen by Albanian lookouts. *Id.* at 20–22.

[142] *Id.* at 17. The U.K. advanced this theory, *id.*, and following an examination of the facts, the court agreed, *id.* at 22.

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

[144] *Id.* ¶ 20.

[145] Case No IT-94-1-A, Judgment (July 15, 1999).

[146] *Id.* ¶¶ 120, 137. With respect to individuals, the Appeals Chamber stated:

> [I]f it is proved that individuals who are not regarded as organs of a State by its legislation nevertheless do in fact act on behalf of that State, their acts are attributable to the State. The rationale behind this rule is to prevent States from escaping international responsibility by having private individuals carry out tasks that may not or should not be performed by State officials.

Id. ¶ 117. Such individuals, however, must have "specific instructions or directives" to commit unlawful acts if the state is to be held responsible. *Id.* ¶ 132.

[147] Schmitt, *supra* note 63, at 177.

A robust notion of state responsibility, derived from this case law, is necessary to bring economic cyber espionage within the bounds of the law—as this conduct is typically shrouded in state denial and therefore difficult to attribute directly to a state.

c. The Law of Armed Conflict

International law scholars and military specialists have begun to consider how the law of armed conflict applies to large-scale, kinetic-level cyber attacks.[148] One leading result of this effort is the *Tallinn Manual*, published by law-of-war scholars in 2013.[149] The *Tallinn Manual* considers "[t]he legality of cyber intelligence activities . . . as they relate to the *jus ad bellum* notions of 'use of force' and 'armed attack', or as relevant in the context of an armed conflict governed by the *jus in bello*."[150] The *Tallinn Manual* is not, however, addressed to "[c]yber activities that occur below the level of a 'use of force,' . . . like cyber criminality."[151] Nevertheless, several of the underlying principles discussed in the *Tallinn Manual* indirectly suggest a basis for holding states accountable for economic cyber espionage.

For example, according to Rule 1 of the *Tallinn Manual*, "A cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty."[152] The experts note that, although the traditional "violation of sovereignty was limited to actions by, or attributable to States . . . there is an embryonic view proffered by some

---

[148] For examples of recent commentary on this subject, see generally Michael Gervais, *Cyber Attacks and the Law of War*, 30 BERKELEY J. INT'L L. 525 (2012), Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1 (2010), and Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421 (2011).

[149] TALLINN MANUAL, *supra* note 7. The *Tallinn Manual* "results from an expert-driven process designed to produce a non-binding document applying existing law to cyber warfare" and "examines the international law governing 'cyber warfare.'" *Id.* at 1, 3. The *Tallinn Manual* also speaks generally to how traditional principles or rules of international law apply to cyberspace. *Id*. pt. I.

[150] *Id.* at 3–4. This Article agrees that a counter-response of force would not be an appropriate response to economic cyber espionage, and argues that this threat should be contained with a rule of law response. Others have suggested differently. *See, e.g.*, Schmitt, *supra* note 63, at 178 ("[I]t is questionable whether the historic exclusion of economic warfare should be interpreted as extending to cyberoperations that generate dramatic economic consequences."). NATO has also issued an advisory manual that discusses "how international law applies to online attacks by the state, and warns that online attacks could lead to full-blown military conflicts." Hayley Dixon, *Rules of Cyberwar Set Out for First Time in NATO Manual*, TELEGRAPH (Mar. 19, 2013), http://www.telegraph.co.uk/technology/9939401/Rules-of-cyberwar-set-out-for-first-time-in-Nato-manual.html. The manual was authored by NATO's Co-operative Cyber Defence Centre of Excellence and "defines a cyber attack as one that is reasonably expected to cause injury or death to persons or damage or destruction to objects." *Id.* (internal quotation marks omitted).

[151] TALLINN MANUAL, *supra* note 7, at 3–4.

[152] *Id.* at 16.

scholars that cyber operations conducted by non-State actors may also violate a State's sovereignty."[153] Also, pursuant to Rule 6, "[a] State bears international responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."[154] And "persons or entities" that are "specifically empowered" by the state are, for purposes of international law, "equated to State organs," including private entities "granted the authority . . . to engage in cyber intelligence gathering."[155]

Again, the *Tallinn Manual* stops short of applying the law of state responsibility to economic cyber espionage, noting "international law does not address espionage *per se*" and it therefore cannot "amount to an 'internationally wrongful act.'"[156] However, to the extent this Article argues that economic cyber espionage is distinct from traditional espionage and violates a state's economic sovereignty in a more coercive way, the *Tallinn Manual*'s rules may be relevant to those acts.

* * *

The foregoing Part demonstrated that, although international law is not often mobilized to combat instances of traditional espionage, economic cyber espionage should be treated differently. It is more coercive than traditional espionage insofar as it deprives a state of exclusive control of its economic space (a key source of power), and therefore directly violates the right to economic sovereignty and causes concrete harm to the state. From this it follows that a state which controls, directs, acknowledges, or supports cyber espionage against another state may be held responsible under the international law doctrine of state responsibility, provided there is knowledge and some appropriate level of control over the groups or entities (or even individuals) that engage in it.

Applying these customary norms to economic espionage, however, is not enough. In order to make a norm against economic cyber espionage meaningful, it must truly become state practice. And in order for that state recognition to take hold, there must be an institutional mechanism available for states to assert a claim for economic cyber espionage. That mechanism must also have the ability to ensure compliance through a credible means of rendering a decision and enforcing it. The next Part argues that the WTO is the proper institutional mechanism for channeling these norms into state practice.

---

[153] *Id.* at 18.
[154] *Id.* at 29.
[155] *Id.* at 31.
[156] *Id.* at 30.

IV. DEVELOPING STATE PRACTICE AGAINST ECONOMIC ESPIONAGE: ASSERTING CLAIMS IN THE WTO

A norm is of little value without a legal mechanism to enforce it. Where Part III considered the problem of anormativity in the area of economic cyber espionage, this Part considers and proposes a solution to the lack of institutional implementation arrangements. Focusing on recognition and enforcement of the norm against economic cyber espionage, it considers how a victim state might assert a claim for the violation of its economic sovereignty caused by the continued use of economic cyber espionage. This Part argues that an international economic institution like the WTO is the most appropriate and effective forum for regulating economic cyber espionage, particularly when perpetrated by states motivated by the simultaneous desire for economic expansion and economic integration, such as China. The WTO provides a legal framework already dedicated to fair trade and competition, and it has the power and authority necessary to ensure compliance with its judgments.

This Part first considers how the WTO rules of law fit together with the customary principles developed in Part III. It argues that certain WTO rules, when considered through the lens of a contemporary right to economic sovereignty, protect member states against economic cyber espionage. This Part also argues that the right to economic sovereignty—and a state's corresponding obligation to refrain from economic cyber espionage—can be asserted within the WTO's existing dispute settlement framework. Finally, this Part details how a trade-based system would be effective in halting and deterring illegal cyber conduct in the case of China.

A. *WTO Law and the Norm of Economic Sovereignty*

1. *WTO Treaty-Based Protections of Intellectual Property*

The WTO is a multilateral economic institution[157] that provides for, among other trade-related rights, rigorous protection of intellectual and industrial property rights between member states through its treaties and various agreements.[158] The WTO's Agreement on Trade-Related Aspects

---

[157] *See What Is the World Trade Organization*?, WORLD TRADE ORG., http://www.wto.org/english/thewto_e/whatis_e/tif_e/fact1_e.htm (last visited Apr. 15, 2014) ("Most nations—including almost all the main trading nations—are members of the system. But some are not, so 'multilateral' is used to describe the system instead of 'global' or 'world.'").

[158] The United States and China are both member states. For a full list of membership, see *Members and Observers*, WORLD TRADE ORG., http://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm (last visited Apr. 15, 2014). For a very basic overview of the treatment of intellectual property in the WTO, see WORLD TRADE ORG., UNDERSTANDING THE WTO 39–43 (2011) [hereinafter UNDERSTANDING THE WTO], *available at* http://www.wto.org/english/thewto_e/whatis_e/tif_e/understanding_e.pdf.

of Intellectual Property Rights (TRIPS) was negotiated during the 1986–1994 Uruguay Round of trade talks.[159] TRIPS "introduced intellectual property rules into the multilateral trading system for the first time."[160] The goal of the Agreement is to "narrow the gaps in the way these rights are protected around the world, and to bring them under common international rules."[161] Importantly, the Agreement "establishes *minimum* levels of protection that each government has to give the intellectual property of fellow WTO members."[162] Specifically, the second part of the TRIPS Agreement considers exactly how to protect certain kinds of intellectual property rights and takes as its "starting point" the obligations set out in the main international agreements of the World Intellectual Property Organization (WIPO).[163]

The TRIPS Agreement and the conventions it incorporates protect several substantive rights related to economic cyber espionage. For example, it protects "[t]rade secrets and other types of 'undisclosed information' which have commercial value."[164] This information "must be protected against breach of confidence and other acts contrary to honest commercial practices."[165] The TRIPS Agreement also protects industrial designs[166] and provides for national treatment regarding industrial property by incorporating the Paris Convention of 1883, which states "each contracting State must grant the same protection to nationals of the other contracting States as it grants to its own nationals."[167] Through that Convention, TRIPS also sets out a common rule that "[e]ach contracting State must provide for effective protection against unfair competition."[168] And TRIPS protects copyrights, including computer programs and

---

[159] UNDERSTANDING THE WTO, *supra* note 158, at 39. For a general description of the Uruguay Round, see *The Uruguay Round*, WORLD TRADE ORG., http://www.wto.org/english/thewto_e/whatis_e/tif_e/fact5_e.htm (last visited Apr. 15, 2014).

[160] *Intellectual Property: Protection and Enforcement*, WORLD TRADE ORG., http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm (last visited Apr. 15, 2014) [hereinafter *WTO IP Protection and Enforcement*].

[161] *Id.*

[162] *Id.* (emphasis added).

[163] *Id.* The first part of the Agreement deals with basic principles. Those principles include national treatment ("treating one's own nationals and foreigners equally"), and most-favored-nation treatment ("equal treatment for nationals of all trading partners in the WTO"). *Id.*

[164] *Id.*; *see* Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 108 Stat. 4809, 1869 U.N.T.S. 299 [hereinafter TRIPS Agreement] (pronouncing that member states have a duty to protect undisclosed information).

[165] *WTO IP Protection and Enforcement*, *supra* note 160.

[166] TRIPS Agreement, *supra* note 164, arts. 25–26.

[167] *Summary of the Paris Convention for the Protection of Industrial Property (1883)*, WORLD INTELL. PROP. ORG., http://www.wipo.int/treaties/en/ip/paris/summary_paris.html (last visited Apr. 15, 2014).

[168] *Id.*

databases within the scope of protection.[169] Patent protection is likewise broad: "[p]atent protection must be available for both products and processes, in almost all fields of technology."[170]

Together, these rights and enforcement principles suggest two things relevant to economic cyber espionage. First, the rules require member states to protect innovative economic activity that is not necessarily developed or owned by the state itself, but rather by private economic actors.[171] Second, member states are bound to protect one another's intellectual property and refrain from any activity that impedes those rights.[172] At first blush, the WTO thus appears an obvious forum for asserting complaints about economic cyber espionage. Indeed, some experts already "have argued that the United States should use international trade law's protections for intellectual property against countries engaged in economic cyber espionage."[173]

However, WTO members have apparently "shown no interest" in pursuing this path, "despite mounting worries about this practice."[174] And the United States has not yet pursued any claim against China for economic cyber espionage through the WTO.[175] This reluctance appears to stem, in part, from an overly narrow interpretation of the TRIPS rules. As David Fidler points out, WTO members would likely agree that to "covertly obtain intellectual property of nationals of other WTO members operating in their territories could violate WTO obligations to protect such property."[176] But whether members would also consider WTO rules violated where a member state obtained such "information from private sector entities located *outside* their territories" remains an open question.[177] Member states may thus assume that there is no basis for claiming

---

[169] TRIPS Agreement, *supra* note 164, arts. 9–10.

[170] UNDERSTANDING THE WTO, *supra* note 158, at 41; *see* TRIPS Agreement, *supra* note 164, arts. 27–34 (outlining the patent-related rights of member states).

[171] *Cf.* Geoffrey D. Antell, Book Note, 46 HARV. INT'L L.J. 527, 527 (2005) (reviewing GREGORY SHAFFER, DEFENDING INTERESTS: PUBLIC-PRIVATE PARTNERSHIPS IN WTO LITIGATION (2003)) ("[A]lthough only WTO Member States can bring litigation before the WTO, private actors such as corporations and activists play an important role in states' decisions about which cases to bring.").

[172] *WTO IP Protection and Enforcement*, *supra* note 160.

[173] Fidler, *supra* note 77, at 3; *see also* LEWIS, *supra* note 3, at 49 (suggesting that the United States should pursue cyber espionage and intellectual property theft claims against China in the WTO).

[174] Fidler, *supra* note 77, at 3.

[175] The *Wall Street Journal* recently reported that some U.S. officials may consider WTO action as one of several options. Siobhan Gorman et al., *U.S. to Rev Up Hacking Fight*, WALL ST. J., May 23, 2014, at A1. To date, however, the United States has brought only one case directly against China in the WTO under TRIPS and it did not pertain to cyber espionage. *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 Apr. 15, 2014).

[176] Fidler, *supra* note 77, at 3.

[177] *Id.* (emphasis added); *see id.* (stating that WTO cases have not involved "accusations against government-sponsored espionage").

economic cyber espionage violates the TRIPS Agreement because "WTO rules create obligations for WTO members to fulfill within their territories and do not generally impose duties that apply outside those limits."[178]

This assumption may prove too much. If a member state's actions taken from within its territory infringe on another member state's intellectual property rights, should not the WTO rules apply? That the harm is done in cyber space seems a poor reason to limit application of the TRIPS Agreement, which was, in any event, negotiated before the rise of cyber threats to trade and intellectual property rights. After all, the general goals of the TRIPS Agreement, found in its preamble, are to "reduce distortions and impediments to international trade . . . [and] promote effective and adequate protection of intellectual property rights."[179] In short, to remain relevant, the WTO Agreements must consider the possibility of cyber violations.

Further, the fact that the WTO rules are silent as to economic cyber espionage is not an indication that those rules do not apply. The next Subsection explains why the scope of the WTO agreements should be determined by reference to modernized norms of economic sovereignty and non-intervention in economic affairs[180] and argues that the TRIPS Agreement should, in fact, be recognized to protect member states against the economic cyber espionage of other member states.

2. *Customary International Law and WTO Treaty-Based Rules*

Though TRIPS may not address economic cyber espionage explicitly, its rules may nevertheless be interpreted to prohibit that conduct, particularly when general international law suggests that they should. A prevailing view is that "[g]eneral international law fills the gaps left by treaties," unless there is a conflict between the provisions or an express exclusion of the customary principle.[181] Otherwise, "[e]very international convention must be deemed tacitly to refer to general principles of international law for all questions which it does not itself resolve in express terms and in a different way."[182]

More specifically, it is well-accepted that general international law applies in the WTO. Joost Pauwelyn explains that "WTO rules are part of

---

[178] *Id.*

[179] TRIPS Agreement, *supra* note 164, pmbl.

[180] *See supra* Part III.B (discussing states' rights to economic sovereignty, rights to non-economic intervention, and responsibility for the sponsorship of non-state cyber espionage).

[181] Pauwelyn, *supra* note 99, at 536; *see id.* at 542 ("In international law, there is . . . a presumption in favor of continuity or against conflict, in the sense that if a treaty does not contract out of a preexisting rule, that rule (being of the same inherent value as the new one) continues to exist." (footnote omitted)).

[182] *Id.* at 541 (quoting Pinson v. United Mexican States, 5 R.I.A.A. 327, 422 (Perm. Ct. Arb. 1928)) (internal quotation marks omitted).

the wider corpus of public international law" and are properly considered "rules of international law that . . . constitute *lex specialis* vis-à-vis certain rules of general international law."[183] Accordingly, those non-WTO rules that existed before the WTO treaty was signed on April 15, 1994, and 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" continue to apply.[184] The same is true for "non-WTO rules that are created subsequently to the WTO treaty . . . and . . . are relevant to and may have an impact on WTO rules" and "add to or confirm existing WTO rules."[185] All of these non-WTO rules, which "consist mainly of general international law,"[186] would therefore include customary norms of economic sovereignty and non-intervention in economic affairs as interpreted to proscribe economic cyber espionage. This gap-filling function of non-conflicting customary norms is explicitly confirmed in Article 3.2 of the DSU.[187] It states "that WTO covered agreements must be clarified 'in accordance with customary rules of interpretation of public international law.'"[188]

The WTO case law has followed this approach and resorted to customary international law for interpretive supplementation. As the panel in *Korea—"Government Procurement"* generally explained:

> Customary international law applies generally to the economic relations between the WTO members. . . . [T]o 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.[189]

This statement mirrored the view expressed by the panel in *United States—"Gasoline"* that WTO agreements should "not . . . be read in clinical isolation from public international law."[190]

WTO cases have thus accepted that the customary principle of good faith is useful in interpreting member states' performance of their treaty

---

[183] *Id.* at 538, 539.

[184] *Id.* at 540.

[185] *Id.* at 541.

[186] *Id.* at 540.

[187] Understanding on Rules and Procedures Governing the Settlement of Disputes art. 3.2, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 2, 1869 U.N.T.S. 401 [hereinafter DSU].

[188] Pauwelyn, *supra* note 99, at 542 (quoting DSU, *supra* note 187, art. 3.2).

[189] Panel Report, *Korea—Measures Affecting Government Procurement*, ¶ 7.96, WT/DS163/R (May 1, 2000).

[190] Appellate Body Report, *United States—Standards for Reformulated and Conventional Gasoline*, ¶ 17, WT/DS2/R (Apr. 29, 1996).

obligations. For example, the *United States—"EC Hormones"* panel explained that "[g]ood faith is a general principle of international law that governs all reciprocal actions of States," and therefore "agree[d] with the European Communities that every party to an international agreement must be presumed to be performing its obligation under that agreement in good faith."[191] The appellate body in *United States—"Hot-Rolled Steel"* also relied on the principle of good faith in interpreting the Anti-Dumping Agreement.[192] In examining paragraph 2 of Annex II in light of a good faith obligation, the appellate body found that a state's investigating authority was prevented from imposing unreasonable burdens on exporters.[193]

WTO panels have referred to other customary principles as well, including notions of state responsibility. For example, the panel in *Turkey—"Textiles"* considered whether Turkey was responsible for certain quantitative restrictive import measures taken by the Turkey-EC customs union.[194] Among other reasons for holding Turkey responsible, the panel concluded that "in public international law, in the absence of any contrary treaty provision, Turkey could reasonably be held responsible for the measures taken by the Turkey EC customs union."[195] Similarly, the *Australia—"Salmon"* panel referred both to general international law and WTO law to determine that certain import measures taken by Tasmania were to be "regarded as a measure taken by Australia."[196] The WTO case law thus supports Pauwelyn's thesis that "[t]he WTO is not a secluded island but part of the territorial domain of international law" and that "public international law . . . is enriching and continues to enrich WTO law."[197]

The WTO agreements' silence on the issue of cyber trade violations presents a classic situation in which customary principles should be

---

[191] Panel Report, *United States—Continued Suspension of Obligations in the EC-Hormones Dispute*, ¶ 7.317, WT/DS320/R, *modified by* Appellate Body Report WT/DS320/AB/R (Nov. 14, 2008); *see also* Anastasios Gourgourinis, Lex Specialis *in WTO and Investment Protection Law* 24 (Soc'y of Int'l Econ. Law, Working Paper No. 2010/37, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1634051 (discussing *the EC-Hormones* case).

[192] Appellate Body Report, *United States—Anti-Dumping Measures on Certain Hot-Rolled Steel Products from Japan*, ¶ 101, WT/DS184/AB/R (July 21, 2001).

[193] *Id.* ¶ 102.

[194] Panel Report, *Turkey—Restrictions on Imports of Textile and Clothing Products*, ¶¶ 8.3, 9.33-9.35, WT/DS34/R, *modified by* Appellate Body Report, WT/DS34/AB/R (Nov. 19, 1999).

[195] *Id.* ¶ 9.42; *see* Gourgourinis, *supra* note 191, at 23 (describing how the panel resorted to customary international law because the agreements did not specifically address the issue); *see also* HELMUT PHILIPP AUST, COMPLICITY AND THE LAW OF STATE RESPONSIBILITY 152 (2011) (noting that this case could suggest "that complicit State action could potentially also lead to findings of non-compliance with GATT obligations by the WTO dispute settlement mechanism").

[196] Panel Report, *Australia—Measures Affecting Importation of Salmon—Recourse to Article 21.5 by Canada*, ¶ 7.12, WT DS184/AB/R (Feb. 18, 2000).

[197] Pauwelyn, *supra* note 99, at 552.

consulted to interpret the agreements' scope and applicability in this domain. No TRIPS provision has explicitly (and entirely) contracted out of the fundamental tenants of state sovereignty and state responsibility.[198] Nor is TRIPS inconsistent with these general principles. The economic corollaries of sovereignty and non-intervention—in addition to the well-recognized requirement to comply with one's treaty obligations in good faith—should therefore give rise to a cognizable claim that economic cyber espionage violates TRIPS.[199] On this view, the WTO agreements would not exclude a claim of economic cyber espionage simply because the conduct "involves governments obtaining information from private-sector companies located outside their territories."[200] Arguably, it would be contrary to both the letter and spirit of the WTO agreements to fail to recognize such a claim.

3. *The WTO Mechanisms for Enforcement*

As a global matter, the TRIPS Agreement takes the existence of intellectual property rights seriously, and duly recognizes the need for enforcement, as "[h]aving intellectual property laws is not enough. They have to be enforced."[201] Part III of the TRIPS Agreement is thus specifically dedicated to enforcement and imposes a requirement upon governments "to ensure that intellectual property rights can be enforced under their laws, and that penalties for infringement are tough enough to deter . . . violations."[202] Consistent with the spirit of rigorous enforcement, the DSU has broad jurisdiction in construing what constitutes a claim: "WTO rules have an 'all-affecting' character, which means that even

---

[198] The DSU has apparently contracted out of some general rules on state responsibility. Pauwelyn, *supra* note 99, at 539. However, at least some scholars believe that the principles of state responsibility remain relevant to WTO claims. *See id.* at 542 & n.51 (positing, as a matter of treaty interpretation, that it is "not so clear" that the DSU completely contracted out of state responsibility rules). In addition to those WTO cases discussed above, others have considered this customary principle in their decisions. For example, the Appellate Body referred to customary principles of state responsibility, as set out by the ILC, to interpret the definition of a "public body" in the context of the Agreement on Subsidies and Countervailing Measures. *See WTO Analytical Index: Dispute Settlement Understanding*, WORLD TRADE ORG., http://www.wto.org/english/res_e/booksp_e/analytic_index_e/dsu_10_e.htm#1683 (last visited Mar. 15, 2014) (discussing the *US—Anti-Dumping and Countervailing Duties* case); *see also id.* (discussing the *Canada—Dairy* case in which the Panel also resorted to the ILC's Draft Articles on State Responsibility to determine whether a particular entity had acted pursuant to delegated government authority and could therefore be considered an "agency" of the Canadian government).

[199] *See* Gourgourinis, *supra* note 191, at 22 (referring to the customary countermeasure defense and arguing that to "the extent that WTO treaties do not explicitly . . . contract-out" from a particular aspect of customary law, these norms remain available "to raise in WTO adjudication so as to justify WTO violations").

[200] Fidler, *supra* note 77, at 3.

[201] *WTO IP Protection and Enforcement*, *supra* note 160.

[202] *Id.*

disputes with a relatively limited trade aspect can be brought before the WTO."[203] Arguably, with such a broad enforcement prerogative, the principles of economic sovereignty and non-economic intervention would be proper parts of a member state's claim that TRIPS rules have been violated by economic cyber espionage.

However, even if economic cyber espionage was not recognized as a direct violation of the TRIPS Agreement, the behavior should be actionable as a non-violation complaint. Non-violation complaints allow a member state to appeal to the Dispute Settlement Body in certain circumstances where an agreement has not been directly violated.[204] They are "allowed if one government can show that it has been deprived of an expected benefit because of another government's action, or because of any other situation that exists. The aim [of the non-violation complaint] is to help preserve the balance of benefits struck during multilateral negotiations."[205] The provision allowing for such claims is found in Article XXIII of the General Agreement on Tariffs and Trade (GATT), which provides, in relevant part:

> If any contracting party should consider that any benefit accruing to it directly or indirectly under this Agreement is being nullified or impaired or that the attainment of any objective of the Agreement is being impeded as the result of (a) the failure of another contracting party to carry out its obligations under this Agreement, or (b) the application by another contracting party of any measure, whether or not it conflicts with the provisions of this Agreement, or (c) the existence of any other situation, the contracting party may, with a view to the satisfactory adjustment of the matter, make written representations or proposals to the other contracting party or parties which it considers to be concerned. Any contracting party thus approached shall give sympathetic consideration to the representations or proposals made to it.[206]

Article 64 of the TRIPS Agreement, which deals with dispute settlement, refers to Article XXIII(1) of GATT,[207] suggesting non-violation complaints

---

[203] Pauwelyn, *supra* note 99, at 553.

[204] *TRIPS: "Non-Violation" Complaints (Article 64.2)*, *Background and the Current Situation*, WORLD TRADE ORG., http://www.wto.org/english/tratop_e/trips_e/nonviolation_background_e.htm (last visited Apr. 15, 2014) [hereinafter *TRIPS: Non-Violation Complaints*].

[205] *Id.*

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

[207] TRIPS Agreement, *supra* note 164, art. 64.1.

are in theory possible under TRIPS.[208]

However, there is currently a moratorium on the use of non-violation complaints in connection with TRIPS set out under Article 64.2 of TRIPS.[209] The moratorium was most recently extended to December 2015 at the Ministerial Conference held in December 2013.[210] When the issue is revisited, there are several reasons why the TRIPS Council should recommend that TRIPS-related non-violation complaints be allowed in the limited circumstance of economic cyber espionage.[211]

For one, non-violation complaints are designed to handle trade disputes and disruptions of precisely the type posed by economic cyber espionage. Consider the text of Article XXIII. A member state that is a victim of economic cyber espionage of the magnitude described above[212] can undoubtedly "consider" that a benefit under the TRIPS Agreement—namely, the rigorous protection of its intellectual property and trade secrets—is being "nullified or impaired" by that conduct.[213] Such claims would also be consistent with the purpose of the non-violation complaint, which was initially envisioned by members to provide a "remedy against actions that are not inconsistent with [WTO] rights and obligations" but which actions constitute "measures that comply with the letter of the agreement, but nevertheless frustrate one of its objectives or undermine trade commitments contained in the agreement."[214] If economic cyber espionage may evade censure as a violation of a TRIPS rule merely because the intellectual property harm occurs outside the violator's physical territory, that activity nonetheless frustrates a core objective of the TRIPS Agreement—to safeguard the "minimum levels of protection that each government has to give to the intellectual property of fellow WTO members."[215]

---

[208] *Legal Basis for a Dispute: Types of Dispute in the TRIPS Agreement*, WORLD TRADE ORG., http://www.wto.org/English/tratop_E/dispu_e/disp_settlement_cbt_e/c4s5p1_e.htm (last visited Apr. 15, 2014).

[209] *See* TRIPS Agreement, *supra* note 164, art. 64.2 (outlining a five year moratorium); *see also TRIPS: Non-Violation Complaints*, *supra* note 204 ("[F]or the time being, members have agreed not to use [non-violation complaints] under the TRIPS Agreement.").

[210] *Ministerial Decision of 7 December 2013*, WORLD TRADE ORG., http://wto.org/english/thewto_e/minist_e/mc9_e/desci31_e.htm (last visited Apr. 15, 2014).

[211] In past discussions, the TRIPS Council considered four options: "(1) banning non-violation complaints in TRIPS completely, (2) allowing the complaints to be handled under the WTO's dispute settlement rules as applied to goods and services cases, (3) allowing non-violation complaints but subject to special 'modalities' (i.e., ways of dealing with them), and (4) extending the moratorium." *TRIPS: Non-Violation Complaints*, *supra* note 204.

[212] *See supra* Part I.

[213] GATT, *supra* note 206, art. XXIII.

[214] *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 Apr. 15, 2014) [hereinafter *Legal Basis for a Dispute: Types of Complaints*].

[215] *WTO IP Protection and Enforcement*, *supra* note 160.

Moreover, given the rigorous requirements for asserting a non-violation complaint,[216] there is little reason to fear that allowing a limited exception to the moratorium for complaints of economic cyber espionage would open up a Pandora's Box of attempted claims. Article 26.1 of the DSU requires the complainant in a non-violation case to "present a detailed justification in support of any complaint relating to a measure which does not conflict with the relevant covered agreement;"[217] this complaint must satisfy the criteria set out in Article XXIII.[218]

The United States' hypothetical claim against China is instructive. Per the doctrine of state responsibility, there appears to be circumstantial (if not direct) evidence of China's knowledge and overall control[219] of certain cyber espionage measures taken against the United States' intellectual property interests.[220] With respect to a relevant right or "benefit accruing" under the TRIPS Agreement, the United States could argue that it has a legitimate expectation to every possible market opportunity flowing from any innovation or industrial design originating in its private sector.[221] That benefit is "nullified or impaired" when economic cyber espionage "has the effect of upsetting the competitive relationship" of the parties.[222] Lastly, the United States might claim that it "was not able to reasonably anticipate the application of [economic cyber espionage] when it was negotiating"

---

[216] *See generally* GATT, *supra* note 206, art. XXIII (outlining the requisite procedures for making a non-violation complaint). The requirements can be summarized as follows:

> The text of Article XXIII:1(b), combined with the concept of nullification or impairment of a benefit gives rise to three conditions whose existence a complainant must establish, in order to be successful with a non-violation complaint. These three conditions are: (1) the application of a measure by a Member of the WTO; (2) the existence of a benefit accruing under the applicable agreement; and (3) the nullification or impairment of a benefit as a result of the application of the measure.

Legal Basis for a Dispute: Types of Complaints, *supra* note 214.

[217] DSU, *supra* note 187, art. 26.1(a).

[218] *See supra* note 216.

[219] As Fidler points out, "Even if a WTO member could construct a claim that economic cyber espionage violates a WTO rule, it would have to establish that another WTO member's government is responsible for the infringing acts." Fidler, *supra* note 77, at 3.

[220] *See supra* notes 8–9, 68 and accompanying text. This is key because "[p]urely private conduct, taken by itself, would not satisfy this condition. If a government simply tolerates private restrictive conduct, this also could not be challenged with the non-violation complaint." *Legal Basis for a Dispute: Types of Complaints*, *supra* note 214. However, "[a] different situation is that where the government actively supports or encourages such private actions." *Id.* The recent criminal indictment against Chinese military actors alleges a direct link with China, but it remains to be seen whether the United States will be able to prove this link. Furthermore, in the future, such direct links may not be provable and thus the ability to prove state responsibility through circumstantial evidence remains important.

[221] *Cf. Legal Basis for a Dispute: Types of Complaints*, *supra* note 214 (noting that complaining parties have been able to point to "the legitimate expectation of improved market access opportunities resulting from the relevant tariff concessions" as a relevant benefit).

[222] *Id.*

any aspect of its trade relationship with China.[223] It would be difficult, however, for member states to credibly make similar claims in cases of less serious, low-grade cyber-related trade conduct. Therefore, although large-scale economic cyber espionage would meet the criteria for a non-violation complaint, most other conduct that was simply nettlesome to trade would not. In this way, non-violation complaints for economic cyber espionage would remain an "exceptional remedy."[224]

The possibility of violation or non-violation complaints under TRIPS makes the WTO an appropriate legal framework for asserting claims against members that engage in economic cyber espionage. The next Section argues why the WTO is also the most effective multilateral institution to manage this process. Although the Article uses the case of China as an example, the point remains equally true with respect to other states that have conducted economic cyber espionage in the current normative and institutional fogginess that exists in international law and may be driven by similar strategic needs for domestic economic expansion and global economic integration.

B. *The WTO as a Credible Source of Power and Authority*[225]

As conceptualized above, the WTO treaty-based framework is designed to protect intellectual property and trade secrets. This framework is compatible with and reinforces the norms of economic sovereignty and non-economic intervention, as well as the principle that states should be held responsible for the unlawful economic acts that they sponsor. But equally important to the existence of these norms under international law is the ability of the WTO to command compliance. This Section argues that the WTO members should recognize claims asserted for economic cyber espionage not only because the WTO agreements allow it, but also because the WTO is the most effective institution to vindicate these rights as a matter of credibility, power, and authority.[226]

---

[223] *Id.*

[224] *Id.* (quoting Panel Report, *Japan—Measures Affecting Consumer Photographic Film and Paper*, ¶ 10.37, WT/DS44/R (Apr. 22, 1998)).

[225] I am indebted to Professor Michael Reisman who taught me to think about the policy dimension of international law along these lines.

[226] Other solutions have been proposed. For example, Dennis Blair and John Huntsman have recommended:

> [I]mmediately: 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 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.

Blair & Huntsman, *supra* note 6 (emphasis omitted).

1. *The WTO Has Power and Authority that Aspiring Superpower States Will Respect*

To be effective, rules of law must be backed by the perceived authority to decide that those rules apply and the power to command compliance.[227] There are several reasons why the WTO holds this power and authority and, as such, is the most effective multilateral institution to decide disputes over economic cyber espionage.

In the case of China, for example, the WTO is a necessary and critical element of its rise to superpower status—China's rise, which is predicated on economic expansion, depends on the continued embrace of the world economic community.[228] Its inability to participate in the WTO and trade with its members—especially the United States—would be deleterious to that goal.[229] Although China aspires to "leap from a poor isolated nation to a global economic superpower," if it "fails to evolve toward more responsible behavior both abroad and at home, a backlash that is already forming in the United States and among its neighbors will swell."[230] Because China needs the WTO's support, that institution holds real power over China and stands as a source of authoritative decisionmaking.

The WTO also holds symbolic power and authority over China.[231] Participation in this club is an important sign of China's acceptance by the world's most powerful trading states and, by proxy, its own rising economic status. For these reasons, the WTO's approbation of economic cyber espionage would serve to mark such norm or rule as "legally meaningful and effective."[232]

Finally, the WTO is also a credible source of authority. To be effective, "[l]egal arrangements must also include credible commitments to apply the resources necessary to make them effective, as the expectation that there are such commitments and that they will be applied in the event of deviance from the arrangement is an important factor in compliance."[233] Once WTO members recognize economic cyber espionage as a violation of

---

[227] *See* REISMAN, *supra* note 101, at 95–100 (discussing authoritative power as a requirement for "any effective legal arrangement" in the context of international law and politics).

[228] *See supra* Part II.A (discussing China's pressures to rise and dependence on integration within the international economic order).

[229] *See* Karabell, *supra* note 42 (noting that "[t]housands of Chinese companies depend on the U.S. market, and on continued exposure to American businesses as they turn to serve a burgeoning domestic Chinese consumer market").

[230] *The China Moment*, WASH. POST, June 6, 2013, at A14.

[231] *See* REISMAN, *supra* note 101, at 77 ("Symbols of authority are a factor that contributes toward compliance.").

[232] *See id.* ("Legal communications are distinguished from the daily bombardment of 'you shoulds' and 'you-oughts' by the fact that they are accompanied by (i) symbols of authority and (ii) commitments of control. Together the signals of authority and control serve to mark the communications they attend as legally meaningful and effective.").

[233] *Id.*

the covered agreements, through the application and incorporation of customary norms, then the full weight of the DSU mechanisms become available.[234] The dispute resolution mechanism—and its ability to require a violating state to bring its law and policy into conformance—represents a credible commitment of resources to enforcing a legal proscription against economic cyber espionage. In fact, with the WTO's power and authority looming large, even the threat of a claim against China could go far in deterring its conduct.[235]

2. *The WTO Presents a Palatable Solution*

Efforts to secure compliance and to deter unwanted conduct are also well-served by presenting a solution that the violator perceives to be in its interest or, at least, palatable. Providing such a face-saving solution that is considered acceptable, from an appearances perspective, is often critical in resolving or mediating a conflict.[236] This is especially important where a party to the conflict faces internal, domestic pressure to maintain a strong façade or present a successful image.[237] China may fit this paradigm. It faces domestic pressure to sustain its economic progress,[238] and would therefore likely resist cooperation with any rules of law perceived to be destructive of that image. WTO sanctions could frustrate its citizens' expectations of improved economic conditions,[239] which "would be a deeply disillusioning experience if China's government is somehow implicated."[240]

Importantly, the WTO dispute settlement mechanism provides a palatable solution by which China's leaders could avoid a difficult trade-off between compliance with the WTO's prescriptions and internal political strength. A canonical principle of the Dispute Settlement Body is "to settle disputes, not to pass judgment."[241] Accordingly, after it has been decided that a "country has done something wrong, it should swiftly

---

[234] *See WTO IP Protection and Enforcement*, *supra* note 160 (stating that the dispute settlement system is "available" for "trade disputes over intellectual property rights").

[235] *See* LEWIS, *supra* note 3, at 49 ("Even a credible hint that the United States is considering [going to the WTO] would have an immediate effect on Chinese decisionmaking."); *see also* Robert F. Turner, *Cyberdeterrenece*, 126 HARV. L. REV. F. 181, 181 (2013) ("[T]he most effective responses will focus on affecting the perceptions of decisionmakers on the other side.").

[236] *See* Christina Parajon, *War-Stopping Techniques in the Falklands*, *in* STOPPING WARS AND MAKING PEACE: STUDIES IN INTERNATIONAL INTERVENTION 1, 38, 45–46 (Kristen Eichensehr & W. Michael Reisman eds., 2009) (discussing the importance of politically palatable solutions in war-stopping or mediation efforts in the context of the Falklands dispute).

[237] *See id.* at 18 (discussing the Argentine junta's need to appear strong at home).

[238] *See supra* notes 29–35 and accompanying text.

[239] *See supra* Part II.A.1.

[240] Legro, *supra* note 29, at 525.

[241] UNDERSTANDING THE WTO, *supra* note 158, at 55.

correct its fault."[242] Thus, a state deemed to be in violation of the WTO rules or spirit of agreement is given the chance to develop a means to bring its policies and laws "into line with the ruling or recommendations."[243] Sanctions—which are punitive in nature and, arguably, viewed by a state as more shameful—cannot be applied unless the violator refuses to follow the Panel or Appeal Body's recommendations after a reasonable period of time and then fails to agree to compensate the complaining country for that failure.[244] This system would essentially allow a violator state to take ownership of the problem, without admitting direct malfeasance—albeit essentially conceding its state responsibility—to remedy the economic cyber espionage.

V. CONCLUSION

This Article considered the lack of norms and institutional mechanisms that apply to economic cyber espionage in international law. It argued that economic cyber espionage is both a breach of well-established customary norms—as those norms have evolved to provide derivative rights to economic sovereignty and non-economic intervention—as well as a violation of WTO rules. The Article then explained why the WTO, as the anchor of the world economic community, is the most appropriate and effective forum for asserting claims regarding this conduct. It explained why the WTO's treaties and rules should be interpreted through these customary norms to establish that economic cyber espionage violates both the letter and the spirit of the TRIPS Agreement. The Article concluded with some realist perspective on why this institution would be effective in ensuring compliance: it has the power and authority to decide that economic cyber espionage violates international law and offers a credible process for ensuring that these rules will be enforced.

---

[242] *Id.* at 58.

[243] *Id.*

[244] *See id.* ("If after 20 days, no satisfactory compensation is agreed, the complaining side may ask the Dispute Settlement Body for permission to impose limited trade sanctions . . . against the other side. . . . In principle, the sanctions should be imposed in the same sector as the dispute. If this is not practical or if it would not be effective, the sanctions can be imposed in a different sector of the same agreement.").