Chinese Economic Cyber Espionage

U.S. Litigation in the WTO and Other Diplomatic Remedies

Stuart S. Malawer

Countering Chinese economic cyber espionage is one of the most complex challenges of contemporary U.S. foreign policy. The Chinese government's systematic hacking into the computer networks of companies to gain commercial advantages for Chinese firms has resulted in "the greatest transfer of wealth in history."[1] Fundamentally, Chinese economic cyber espionage compromises the competitiveness of U.S. firms in China and worldwide. It is integral to China's mercantilist economic and trade policies.

Such espionage, more precisely termed 'commercial cyber espionage', is difficult to detect, to guard against, and to formulate policy around. In particular, the diplomatic and global legal regime governing intellectual property rights predates such commercial espionage. The Internet along with information and advanced communications technologies only became significant features of global transactions since the implementation of the Uruguay Round Agreements,[2] which included the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), in 1995. Thus, any effective international legal remedy to commercial cyber espionage needs to creatively interpret and apply the terms of TRIPS.

Stuart S. Malawer

JD, PhD is a Distinguished Service Professor of Law and International Trade at George Mason University. He serves as a board member of George Mason University's International Cyber Center, and has been a member of the Virginia Governor's trade missions to China and to India.

Fortunately, a creative legal response is available to counter this threat. The most promising and immediate remedy for the United States is to launch litigation against China in the World Trade Organization (WTO) dispute resolution system by relying on the TRIPS Agreement. Litigation would have a significant possibility of success and, at the minimum, a potential to foster a settlement and adoption of basic understandings between the United States and China during or after these proceedings. A corollary of this legal strategy is to commence diplomatic actions within the WTO's negotiating process to update TRIPS, or conclude a new plurilateral agreement that explicitly addresses economic cyber espionage. Additionally, the United States should convene a general diplomatic conference to propose general rules for the cyber domain and international agreements to reflect these rules.

Background. "(A)fter hundreds of billions of dollars spent on computer security, the threat posed by the Internet seems to grow worse each year."[3] The 2015 national security strategy report by the Obama administration declares that "the United States has a special responsibility to lead a networked world."[4] It argues that cybersecurity requires observed international norms and a shared responsibility among states. This reflects the administration's earlier views--enunciated by its 2011 report on international cyberspace strategy--that its goal is to support the rule of law in cyberspace.[5] The 2015 White House Summit on Cybersecurity, while focusing on the need for domestic legislation, also declares that cybersecurity is a shared responsibility between government and the private sector.[6]

President Obama recently raised the specific issue of cybersecurity and the stealing of trade secrets and intellectual property rights with Chinese President Xi Jinping at the Asia-Pacific Economic Cooperation (APEC) summit in Beijing in November 2014.[7] Obama had raised this issue before in private talks with China's president in June 2013. Tom Donilon, the U.S. national security advisor, had also highlighted the administration's focus on cyber security at the Asia Society in 2013, when he stated:

> [Cybersecurity] is not solely a national security concern or a concern of the U.S. government. Increasingly, U.S. businesses are speaking out about their serious concerns about the sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale…As the President said in the State of the Union, we will take action to protect our economy against cyber-threats. [8]

In May 2014, the U.S. Department of Justice indicted five members of the Chinese military for hacking into corporate computer networks and stealing trade secrets from major American firms. This was the first time such criminal charges were filed against officials and military officers in another country.[9] This indictment was

based upon an earlier private report revealing the role of the People's Liberation Army in hacking into computer systems of American firms.[10] A newer report has been released, claiming that a second Chinese military unit has been identified as hacking into U.S. companies.[11] In May 2015, the U.S. Department of Justice charged six Chinese citizens with economic espionage for helping state-controlled companies.[12] It now appears that criminal gangs, adapting their criminal activity to the digital age, may be becoming proxies for nations carrying out cyber attacks.[13,14] This newer focus on specific firms for commercial advantage is coupled with more widespread intrusions by intelligence agencies into critical infrastructure and private firms for traditional intelligence and national security reasons.

The Obama administration's policy concerning cyber espionage has gradually developed to include the use of "trade tools."[15] In explaining the administration's 2013 cyber security strategy, a report from the Executive Office of the President indicated that one of the strategy's action items was sustaining and coordinating international engagement with trading partners.[16] In particular, the report concluded, "The Administration will utilize trade policy tools to increase international enforcement against trade secret theft to minimize unfair competition against U.S. companies."[17] The use of trade tools and restrictions would impose real costs on China. In June 2014, the then-new ambassador to China, Max Baucus, specified the trade strategy by arguing that China's criminal behavior ran counter to its WTO commitments.[18] Around the same time, Senator Charles Schumer (D., N.Y.) called on U.S. Trade Representative Michael Froman to file legal action against China in the WTO as a response to Chinese cyber attacks on American firms.[19] Specifically, Schumer noted "that the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) contained in the WTO requires each participating nation to protect trade secrets."[20] A Department of Defense consultant and former CIA officer supported filing charges against China in the WTO because the "burden of proof in a WTO proceeding is far easier to sustain than a criminal indictment in U.S. District courts."[21] They also pointed out that a ruling would be from distinguished international jurists and not merely from

A [WTO] ruling would be from distinguished international jurists and not merely from a national court, thus **elevating the international perception of the legitimacy of the proceedings and findings.**

a national court, thus elevating the international perception of the legitimacy of the proceedings and findings.

The TRIPS Agreement. TRIPS does not explicitly address economic cyber espionage for commercial or trade gain. As it was adopted in 1994 and went into effect in 1995, the agreement preceded the great changes brought about by the revolution in information and communications technologies during the last twenty years. But one needs to see how the general and specific provisions of that agreement, as a multilateral agreement that is intended to govern intellectual property rights, apply to newer events in the future. As of today, no WTO cases have addressed this issue.

The starting point is Article III (1) of TRIPS, which restates the National Treatment Principle, the most basic GATT principle that is incorporated in all of the Uruguay Round Agreements and applied to intellectual property rights. The key language is "Each Member shall accord to the nationals of other members treatment no less favorable than that it accords to its own nationals with regard to the protection of intellectual property. . ."[22] The obvious intent of this provision is to make sure that a member state does not discriminate between domestic and foreign companies within the member state as to the recognition and enforcement of intellectual property rights.

Does this provision intend to restrict a member state's efforts to secure trade secrets and other intellectual property information within its territory and then pass it on to its domestic firms? This seems to fall squarely within the provision's language. What if the member state directs its efforts to secure information abroad, and then turn it over to its domestic firms? Is this a loophole? Not in this case. As is apparent in snooping on foreign firms within the member state, the protected information is being used to benefit local firms. In other words, it is providing treatment to foreign firms doing business within the member state that is less favorable than it provides to its own national firms.

Does GATT Article XXI (as restated in TRIPS Article LXXIII), "Security Exception," provide a defense to a member state for such activities? No, because GATT Article XXI (b)(iii) provides that "Nothing in this agreement shall be construed to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests taken in time of war or other emergency in international relations."[23] China could hardly claim that cyber theft of commercial information is part of its "essential security interests" and that this is a "time of war or other emergency in international relations." It is important to note that no WTO cases have ever involved the Security Exception. A determination involving this clause would certainly be highly important to developing global trade law in the context of technological advances and national security concerns today. Needless to say, almost any determination concerning the Security Exception would be seen as highly politicized one affecting a state's

national sovereignty.

Recent Viewpoints in the Literature. David Fidler from Indiana Law School has argued that the WTO is not an appropriate venue for addressing economic cyber espionage by China.[24] His three arguments can be summed up as making the following points: that intellectual property rights are granted and protected by TRIPS on a territorial basis, overcoming the burden of proof is difficult to achieve in the dispute resolution system, and there is a lack of public international law on economic espionage. Fidler fails to consider that cyber actions by China outside of its territory, but with effects and benefits within its territory, as to its own firms, are reasonably included within the language of the National Treatment Principle of TRIPS (Article III). The burden of proof in the WTO's trade and commercial proceedings is much less stringent than in criminal proceedings against Chinese officials in the United States.[25] The WTO proceedings are intended to resolve typical trade disputes, not criminal activity. It is best to understand that any discussion of China's cyberespionage today does not involve public international law or economic espionage generally, but rather the more properly termed commercial espionage against specific firms under particular WTO obligations.

In a 2014 law review article, Christina Skinner concluded that the WTO "is the most appropriate and effective forum for asserting claims regarding" China's economic cyber espionage.[26] She argued further that general international law would support this claim. She further contended that an action would also be available under Article XXIII (1)(b) of GATT as a "non-violation complaint." That provision allows contracting parties to bring complaints if a benefit is being nullified as a result of a government measure, whether or not it conflicts with a particular provision.

An earlier analysis by a leading Washington law firm suggests that two additional remedies might be considered: updating TRIPS through the negotiating process of the WTO, and considering some sort of Special Section 301 action (under the Trade Act of 1974)[27] with the USTR.[28] An earlier review by another expert concluded that, "no grand, ambitious overhaul of the TRIPS Agreement is necessary to reach consensus on the problem cyber attacks pose for owners of targeted proprietary information."[29] A Section 301 action, or a more specific Special Section 301 action concerning intellectual property rights, is based upon either an illegal or unreasonable foreign action. The administration can do either of these without a private complaint. Nevertheless, these options should be considered carefully, since they involve unilateral trade sanctions by the United States without prior authorization by the WTO.

The U.S. Department of Commerce (International Trade Administration) is currently considering a case involving solar panel imports from China where the U.S. firm is seeking higher tariffs to counter the Chinese government's hacking and theft of trade secrets from

it.[30] This case could give the Obama administration another statutory means of imposing unilateral restrictions. This would be via the actions of the two agencies (the U.S. Department of Commerce and the U.S. International Trade Commission) charged with administering trade remedy laws.

If the United States takes unilateral action under Section 301 or other trade provisions and imposes trade sanctions, then China would most likely file an action against the United States in the WTO. As a respondent, the United States would then be forced to rely on an Article XXI defense of national security. This might be yet another approach to counter Chinese cyber activities. In an action by China the United States would have the burden of proof to establish that its actions were required by national security considerations in a time of an international relations emergency or in a time of war.

This alternative approach would be the inverse of the strategy of bringing an action against China. The unilateral imposition of U.S. sanctions would have less global legitimacy at the outset than if they were imposed pursuant to authorization by the Dispute Settlement Body of the WTO.

Legal and Diplomatic Strategies to Counter Chinese Cyber Espionage

The best approach is for the United States to file an action in the WTO, and receiving WTO authorization prior to imposing sanctions. This would garner the most international support for U.S. actions. China has a relatively good record of observing WTO dispute resolution system recommendations.[31] Compliance is in its national interest and part of its desire to be viewed as a responsible global player. The most difficult part of bringing a WTO case is determining the source of the computer intrusions, the information taken, and the information provided to commercial operations in China.

In such an action by the United States, China would probably raise the issue of U.S. cyber espionage for economic purposes, citing the recent disclosure of the National Security Agency's (NSA's) penetrations into Huawei.[32] The U.S. reply would reference economic espionage to protect the national security interests of the United States,[33] and that commercial information was not turned over to private industry. Independent of speculation, the NSA's company-specific intrusion into the network and equipment of China's leading telecom company does dilute the strength of U.S. claims against China's targeting

The unilateral imposition of U.S. sanctions would have less global legitimacy at the outset than if they were imposed pursuant to authorization by the Dispute Settlement Body of the WTO.

of specific firms for their commercial secrets.

One additional point needs to be made. Formal consultations are required before full litigation in a WTO panel. It is often in this context that diplomatic solutions are worked out bilaterally. Parties often report mutually agreed upon solutions to the WTO. More cases have actually been resolved in this stage than have gone through the full litigation process.[34] If this diplomatic-legal process of the WTO can somewhat successfully address the issue of China's economic cyber espionage, it could help resolve similar disputes between other countries. It might help establish a mindset and a willingness among government officials to create diplomatic solutions to other instances of cyber espionage by both state and non-state actors. For example, China, in promoting itself as a responsible member, may very well agree to pressure North Korea to abide by these newer rules.

The United States could pursue two additional diplomatic remedies. First, it could start negotiating within the WTO system for the extension of the TRIPS agreement to explicitly address cyber espionage. This could be either open to all members or perhaps as a more limited plurilateral agreement for interested members. Second, it could promote a general diplomatic conference outside of the WTO to address a broad range of issues concerning cyber espionage, including but not limited to its commercial aspects. This would be something akin to the naval disarmament conferences of the inter-war period[35] and the arms-control treaties of the Cold War era.[36]

Conclusion. In 2015, the United States imposed limited economic sanctions on North Korea in response to its cyber attack on Sony Pictures Entertainment over the movie "The Interview."[37] For the first time, the United States has imposed economic and trade sanctions to counter a country's use of destructive cyber actions. While these were limited trade and financial sanctions, mainly directed at North Korea's export arms industry and select senior government and intelligence officials, they highlight the lack of both a domestic and international legal architecture governing cyber actions by state actors, especially in retaliation for a state attack on a commercial entity.

The havoc produced by the recent North Korean cyber attack on Sony glaringly demonstrates the need to take first steps in creating global rules for the cyber domain since "there are no international treaties or norms

The NSA's company-specific intrusion does dilute the strength of U.S. claims against **China's targeting of specific firms for their commercial secrets.**

about how to use digital weapons or respond to cyberattacks."[38] A recent report from the Center for Strategic and International Studies concluded "Some cyber threats can only be addressed through indirect action, using agreements on trade or law enforcement cooperation to restrain cyber espionage, the use of proxies, or nonstate actors."[39] A successful action by the United States and compliance by China would be a limited, but an important step in tackling the technological advances in cyber espionage and promoting a rules-based system of global governance. Bringing an action at the WTO would use existing institutions and agreements to address this newest national security threat to the United States and the competitiveness of U.S. firms worldwide.

Chinese economic cyber espionage has become a critical issue in U.S.-China trade. The WTO is the premier international institution addressing trade issues. The TRIPS Agreement addresses many of the intellectual property issues. The dispute resolution system of the WTO has a good track record of resolving high-flying trade disputes at the consultation stage or through the entire resolution process. This involves multilateral authorized sanctions to coerce national compliance. The United States should use this effective and creative process that has developed over the past twenty years to address the evolving nature of global trade in this digital era.

President Obama recently issued an Executive Order on April 1, 2015.[40] It authorizes restricting certain transactions and freezing property owned by foreign nationals engaged in cyber attacks that are aimed at stealing trade secrets for commercial gain, among other reasons. This Executive Order applies to individuals, not foreign states. Applying trade sanctions to foreign nationals engaged in cyberespionage, combined with bringing a WTO action against China for stealing trade secrets, are a complimentary set of domestic and international policies and actions. They would impose significant costs on offensive cyber behavior. The new Executive Order recognizes that cyber attacks pose "an extraordinary threat to the national security, foreign policy and economy of the United States."[41] This indicates that the United States is at a "transformational moment" in the way we respond to cyberespionage.[42]

This moment is even more pronounced in light of the U.S. Department of Defense cyber strategy announced in late April 2015.[43] It proclaims "the U.S. military may conduct cyber operations to counter an imminent or ongoing attack" which is having "a serious economic impact on the United States."[44] This is part of the administration's evolving international cyber policy. It complements various domestic initiatives including, among others, increasing criminal prosecutions for economic espionage and congressional proposals delineating corporate cyber rights and obligations. Current Presidential policy would be enhanced by filing a WTO action under the TRIPS agreement.

This article first appeared in an abbreviated version as "Confronting Chinese Economic Cyber Espionage With WTO Litigation," 252 New York Law Journal No.120 at 4 (December 23, 2014).

NOTES

1 General Keith Alexander, former director of Cyber Command and former Director of the National Security Agency, as quoted in Goldstein, "The Internet as Battlefield." *Washington Post* (December 26, 2014).

2 "Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations." Internet, https://www.wto.org/english/docs_e/legal_e/03-fa_e.htm.

3 Craig Timberg, "A Flaw in the Design." *Washington Post* (May 31, 2015).

4 Executive office of the President of the United States, *National Security Strategy* 12 (February 2015).

5 Executive Office of the President of the United States, *International Strategy for Cyberspace* 8 (May 2011).

6 "FACT SHEET: The White House Summit on Cybersecurity and Consumer Protection." (White House, Office of the Press Secretary) (February 13, 2015).

7 Cory Bennett, "Obama Urges China to Stop Cyber Theft," Internet, http://thehill.com/policy/cybersecurity/223555-obama-urges-china-to-stop-cyber-theft (date accessed: 18 November 2014).

8 Tom Donilon, "The Asia-Pacific in 2013," (Remarks given to the Asia Society, White House Press Office, Washington, D.C., 11 March 2013).

9 Ellen Nakashima and William Wan, "U.S. Announces First Charges against Foreign Country in Connection with Cyberspying," Internet, 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.

10 Mandiant Intelligence Center Report, *APT 1: Exposing One of China's Espionage Units* (2013). See also Sanger, Barboza, and Pehlroth, "Chinese Army Unit is Seen as Tied to Hacking against the U.S.," New York Times (February 13, 2013).

11 Hannah Kuchler and Demetri Sevastopulo, "Second China Unit Accused of Cyber Crime," Internet, http://www.ft.com/cms/s/0/3a1652ce-f027-11e3-9b4c-00144feabdc0.html#axzz3SVXsLA8t.

12 Gina Chon, "US Arrests Chinese Professor in Move Against Corporate 'Spy Ring'." *Financial Times* (May 20, 2015.

13 Sam Jones and Hannah Kuchler, "World's most advanced hacking spyware let loose," Internet, http://www.ft.com/intl/cms/s/0/8392d196-7323-11e4-907b-00144feabdc0.html#axzz3SVXsLA8t.

14 Ellen Nakashima, "Foreign Powers Steal Data on Critical U.S. Infrastructure, NSA Chief Says," Internet, http://www.washingtonpost.com/world/national-security/nsa-chief-foreign-powers-steal-data-on-critical-us-infrastructure/2014/11/20/ddd4392e-70cb-11e4-893f-86bd390a3340_story.html.

15 Executive Office of the President of the United States, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (February 2013).

16 Ibid.

17 Ibid.

18 Reuters, "US Ambassador Baucus Says China Hacking Threatens National Security," Internet, http://www.ibtimes.com/us-ambassador-baucus-says-china-hacking-threatens-national-security-1611080.

19 Press Release, U.S. Senator Schumer, "Schumer Calls on U.S. Trade Rep to File WTO Suit in Response to Chinese Cyberattacks," Internet, http://www.legistorm.com/stormfeed/view_rss/535617/member/85.html (Accessed Feb. 19, 2015).

20 Ibid.

21 James P. Farwell and Darby Arakelian, "China Cyber Charges: Taking Beijing to the WTO Instead," Internet, http://nationalinterest.org/blog/the-buzz/china-cyber-charges-take-beijing-the-wto-instead-10496.

22 Article III (1).

23 Emphasis added. GATT Article XXI(b)(iii).

24 David P. Fidler, "Why the WTO is Not an Appropriate Venue for Addressing Economic Cyber Espionage," http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/; David P. Fidler, "Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies," *Insights* 17, no. 10 (March 2013): 1

25 James P. Farwell and Darby Arakelian, "China Cyber Charges: Taking Beijing to the WTO Instead," Internet, http://nationalinterest.org/blog/the-buzz/china-cyber-charges-take-beijing-the-wto-instead-10496.

26 Christina Parajon Skinner, "An International Law Response to Economic Cyber Espionage," *Connecticut Law Review* 1165 (May 2014).

27 Pub. L. 113-185, 19 USC §2411.

28 Kurt Calia and others, "*Economic Espionage and Trade Secret Theft: An Overview of the Legal Landscape and Policy Responses,*" Internet, http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Covington_SpecialIssueBrief.pdf .

29 Gerald O'Hara, "Cyber-Espionage: A Growing Threat to the American Economy," *CommLaw Conspectus* 19 (2010): 241.

30 Diane Cardwell, "Solar Company Seeks Stiff U.S. Tariffs to Deter Chinese Spying," Internet, http://www.nytimes.com/2014/09/02/business/trade-duties-urged-as-new-deterrent-against-cybertheft.html?_r=0.

31 Malawer, "U.S.-China Litigation in the World Trade Organization." *New York Law Journal* No. 250 at 5 (August 8, 2013).

32 David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," Internet, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

33 David E. Sanger, "Fine Line on U.S. Spying on Companies," Internet, http://www.nytimes.com/2014/05/21/business/us-snooping-on-companies-cited-by-china.html.

34 Stuart Malawer, "U.S. - China Trade Relations -- Litigation in the WTO Since 2001," 26 *International*

Law Practicum 122 at 123 (Autumn 2013).

35 Stuart Malawer, "Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance," 58 *Virginia Lawyer* 28 (February 2010).

36 "Arms Control for a Cyberage." Internet, http://www.nytimes.com/2015/02/26/opinion/arms-control-for-a-cyberage.html?_r=0

37 David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea After Sony," Internet, http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html .

38 Editorial, "Deterring Cyberattacks From North Korea," Internet, http://www.nytimes.com/2014/12/30/opinion/deterring-cyberattacks-from-north-korea.html.

39 Center for Strategic & International Studies, *Conflict and Negotiation in Cyberspace* 52 (February 2013).

40 Executive Order -- "Blocking the Property of Certain Person Engaging in Significant Malicious Cyber-Enabled Activities." (April 1, 2015). Internet, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

41 Id. at paragraph 2.

42 Lisa Monaco (Assistant to the President for Homeland Security and Counterterrorism), "Expanding Our Ability to Combat Cyber Threats." Internet, https://www.whitehouse.gov/blog/2015/03/31/expanding-our-ability-combat-cyber-threats

43 David Sanger, "Pentagon Announces New Strategy for Cyberwarfare." *New York Times* (April 24, 2015).

44 "The Department of Defense Cyber Strategy" 5 (April 2015). Internet, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf