http://www.newyorklawjournal.com/id=1202712784205/Confronting-Chinese-Economic-Cyber-Espionage-With-WTO-Litigation#ixzz3MfIKeTXb

New York Law Journal

252 *New York Law Journal* No.120 at 4 (December 2014).

Outside Counsel

Confronting Chinese Economic Cyber Espionage With WTO Litigation

Dr. Stuart S. Malawer

Chinese economic cyber espionage, government hacking into computer networks of companies to gain commercial advantages for Chinese firms, is one of the most complex issues confronting U.S. national security and foreign policy today. A creative legal response is available.

Fundamentally, Chinese economic cyber espionage compromises the competitiveness of U.S. firms in China and globally. For many reasons, such espionage, more precisely termed 'commercial' cyber espionage, is difficult to detect, to guard against, and to formulate policy responses in regard to. In particular, the diplomatic and global legal regime governing intellectual property rights predates such commercial espionage. The Internet and information and advanced communications technologies only became a feature of the global landscape since the adoption of the Uruguay Round Agreements, which included the intellectual property agreement (TRIPS), in 1995.

Background

Most recently, President Barack Obama raised the issue of cybersecurity and the stealing of trade secrets and intellectual property rights with President Xi Jinping of China at the Asia-Pacific Economic Cooperation (APEC) summit in Beijing in November 2014.[1]

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 another country.[2] In many ways, 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.[3] Indeed, it now appears that criminal gangs may be becoming proxies for nations carrying out cyber attacks.[4]

The Obama administration's policy concerning cyber espionage has gradually developed to include the use of "trade tools."[5] In explaining the administration's strategy, in 2013, one of the strategy action items was to sustain and coordinate international engagement with trading partners.[6] In particular, this report from the Executive Office of the President concluded, "The Administration will utilize trade policy tools to increase international enforcement against trade secret theft to minimize unfair competition against U.S. companies."[7] Indeed, in June 2014, the then-new ambassador to China, Max Baucus, in his first major public address, made more specific the trade strategy by arguing that China's criminal behavior ran counter to its commitments to the World Trade Organization (WTO).[8]

At about the same time, Senator Charles Schumer (D.-N.Y.) called on U.S. Trade Representative Michael Froman to file a legal action against China in the WTO as a response to Chinese cyber attacks on American firms.[9] 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."[10]

The TRIPS Agreement

It is clear that TRIPS, adopted in 1994 and effective in 1995, does not explicitly address economic cyber espionage for commercial or trade gain. Of course, it doesn't. The agreement preceded the great changes brought about by the revolution in information and communications technologies in the last 20 years or so. 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 (General Agreement on Tariffs and Trade) principle that is incorporated in all of the Uruguay Round Agreements and applied here as 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…."[11] The most 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?

Of course, this seems to squarely fall within the provision's language. Now, 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 to me. In this case, as in the one concerning 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 Article XXI, "Security Exception," provide a defense to a member state for such activities? No, and here's why.

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*…." (Emphasis added) Would China's claim

that cyber stealing of commercial information intellectual property rights is part of its "essential security interests" and this is during an "emergency in international relations" really sound plausible? Hardly.

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.

Some Recent Views

Two pieces published by David Fidler from Indiana Law School last year argued that the WTO is not an appropriate venue for addressing economic cyber espionage by China.[12] 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, burden of proof is difficult to carry in the dispute resolution system, and there is a lack of public international law on economic espionage.

My response is 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. The burden of proof in WTO's trade and commercial proceedings is much less stringent than in criminal proceedings against Chinese officials in the United States.[13] The WTO proceedings are not criminal but typical trade disputes. We are not talking about public international law and 'economic' espionage generally but only the more properly termed 'commercial' espionage against specific firms in the context of particular WTO obligations.

In a 2014 law review article, the author, Christina Skinner, concluded that the WTO "is the most appropriate and effective forum for asserting claims regarding" China's economic cyber espionage.[14] Indeed, she argued further that general international law would support this claim. She also argued that an action would also be available under Article XXIII (1)(b) of GATT as a "non-violation complaint."

It is interesting to point out that in a recent corporate filing with the U.S. Department of Commerce (International Trade Administration) concerning the import of solar panels from China, a U.S. firm is asking for higher tariffs to counter the Chinese government's hacking and theft of trade secrets from it.[15] 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.

Conclusion

The best approach is for the United States to file an action in the WTO to receive the blessings of the WTO before imposing sanctions. This would garner the most international support for U.S. actions. The fact of the matter is that China has a pretty good record of observing recommendations of the WTO's dispute resolution system. It has found it to be in its national interest. To me, the most difficult part of bringing a WTO case is determining the source of the computer intrusions, the information taken, and what information is being given to commercial operations in China, along with building the causal relationship between the fruits of Chinese attacks and products to be sanctioned.

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 penetrations into Huawei and its equipment worldwide.[16] The U.S. reply would certainly be that this was economic espionage to protect the national security interests of the United States[17] and that the fruits of U.S. activity were not turned over to private industry. While this may very well be the case, we do not really know. 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 specific firms for their commercial secrets.

One additional point. Prior to full litigation before a WTO panel, there is a requirement of consultations. 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.

If this diplomatic-legal process of the WTO can somewhat successfully address the issue of China's economic cyber espionage, it could lead to resolving other instances of similar activity between other countries. In fact, it could help establish a mind-set and a willingness in government officials to help create diplomatic solutions to other instances of cyber espionage by both state and non-state actors. The havoc produced by the recent North Korean cyberattack on Sony Pictures Entertainment over the movie "The Interview" glaringly evidences the need to take first steps in creating global rules for the cyber domain.[18]

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."[19] Bringing an action in the WTO would be a proactive leveraging of existing institutions and agreements to address this newest national security threat to the United States and the competitiveness of its firms worldwide.

ENDNOTES:

1. Bennett, "Obama Urges China to Stop Cyber Theft," The Hill (Nov. 18, 2014): http://thehill.com/policy/cybersecurity/223555-obama-urges-china-to-stop-cyber-theft

2. Nakashima and Wan, "U.S. Announces First Charges against Foreign Country in Connection with Cyberspying," Washington Post (May 19, 2014).

3. 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 (Feb. 13, 2013).

4. Nakashima, "Foreign Powers Steal Data on Critical U.S. Infrastructure, NSA Chief Says," Washington Post (Nov. 21, 2014).

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

6. Id. at p.3.

7. Id. at p.4.

8. "US Ambassador Baucus Says China Hacking Threatens National Security," International Business Times (June 25, 2014): http://www.ibtimes.com/us-ambassador-baucus-says-china-hacking-threatens-national-security-1611080.

9. "Schumer Calls on U.S. Trade Rep to File WTO Suit in Response to Chinese Cyberattacks," (Press Release, U.S. Senator Schumer, May 22, 2014).

10. Id.

11. Article III (1).

12. Fidler, "Why the WTO is Not an Appropriate Venue for Addressing Economic Cyber Espionage," (Feb. 11, 2013): www.armscontrollaw.com; Fidler, "Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies," Insights 17, no. 10 (March 20, 2013).

13. James Farwell, "China Cyber Charges: Take Beijing to the WTO Instead," THE BUZZ (The National Interest) (May 20, 2014).

14. Skinner, "An International Law Response to Economic Cyber Espionage," Connecticut Law Review 1165 (May 2014).

15. Cardwell, "Solar Company Seeks Stiff U.S. Tariffs to Deter Chinese Spying," New York Times (Sept. 2, 2014).

16. Sanger and Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," New York Times (March 22, 2014).

17. Sanger, "Fine Line on U.S. Spying on Companies," New York Times (May 20, 2014).

18. Nakashima, Timberg and Peterson, "Sony Pictures Hack Appears to be Linked to North Korea, Investigators Say." Washington Post (Dec. 6, 2014).

19. Center for Strategic & International Studies. "Conflict and Negotiation in Cyberspace" (February 2013): 52.

Stuart S. Malawer is the *Distinguished Service Professor of Law and International Trade* at George Mason University.

Read more: http://www.newyorklawjournal.com/id=1202712784205/Confronting-Chinese-Economic-Cyber-Espionage-With-WTO-Litigation#ixzz3MfIKeTXb