insights

American Society of International Law

March 20, 2013 Volume 17, Issue 10

# Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies

By David P. Fidler

ASIL *Insights*, international law behind the headlines, informing the press, policy makers, and the public.

## Introduction

In late February 2013, a controversy erupted after a U.S. cybersecurity company released a report alleging that the Chinese military was using cyber technologies to obtain trade secrets from foreign companies.[1] The Chinese government rejected the allegations, but the report resonated with U.S. concerns about Chinese economic cyber espionage. After the report's release, the Obama administration issued a new strategy to counter theft of trade secrets from U.S. companies.[2] This *Insight* examines the international legal issues this controversy about economic cyber espionage raises.

## Economic Espionage and Cybersecurity

Espionage comes in different forms. Traditional espionage encompasses a government's efforts to acquire clandestinely classified or otherwise protected information from a foreign government. Economic espionage involves a state's attempts to acquire covertly trade secrets held by foreign private enterprises. “Corporate espionage" or "industrial espionage" describes a company's illegal acquisition of another company's trade secrets with no government involvement. Many countries have long considered economic espionage important to national security and economic development.

States engaged in economic espionage prior to the use of cyber technologies. The United States adopted the Economic Espionage Act (EEA) in 1996, before the Internet became a global means of communication. As societies became dependent on cyber technologies, experts identified economic cyber espionage as a growing threat. U.S. cybersecurity policy included economic espionage as a problem.[3] However, economic cyber espionage continued to metastasize, with U.S. leaders arguing that it was contributing to the "greatest transfer of wealth in history."[4]

**RELATED ASIL INSIGHTS**

Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law

International Law and the Future of Cyberspace: The Obama Administration’s International Strategy for Cyberspace

Google, China, and Search

WTO Panel Report on Consistency of Chinese Intellectual Property Standards

Insights Archive>>

**DOCUMENTS OF NOTE**

Mandiat Report: *APT1: Exposing One of China’s Cyber Espionage Units*

*Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*

Agreement on Mutual Legal Assistance in Criminal Matters, U.S.-China

Agreement on Trade-Related Aspects of Intellectual Property Rights

**ORGANIZATIONS OF NOTE**

Office of the National Counterintelligence Executive

World Trade Organization

INTERPOL

U.S. officials and cybersecurity experts have accused China of engaging in economic cyber espionage. In October 2011, the Office of the National Counterintelligence Executive (ONCIX) labeled China a "persistent collector" of U.S. economic secrets accomplished through cyber means.[5] However, attributing cyber intrusions to the Chinese government has proved difficult. The ONCIX admitted that "the [Intelligence Community] has not been able to attribute many of these private sector data breaches to a state sponsor."[6]

In late January 2013, the *New York Times* reported it had been hacked from China, and allegations followed that other newspapers had similarly been hacked.[7] On February 10, 2013, a National Intelligence Estimate “concluded that the United States is the target of a . . . cyber-espionage campaign that is threatening the country’s economic competitiveness,” with China identified “as the country most aggressively seeking to penetrate the computer systems of American businesses and institutions to gain access to data that could be used for economic gain.”[8]

On February 19, 2013, Mandiant, a cybersecurity company, released a report in which it claimed to have evidence linking Unit 61398 of the People's Liberation Army in Shanghai to a global cyber espionage campaign against nearly 150 companies from 20 economic sectors "designed to steal large volumes of valuable intellectual property."[9] Mandiant's report garnered widespread press coverage, prompted angry responses from China, and catalyzed the Obama administration's release of a new strategy to combat theft of U.S. trade secrets on February 20, 2013.

**International Law and Economic Cyber Espionage**

*International Law, Espionage, and Economic Espionage*

The desire to combat economic cyber espionage confronts a lack of international law on espionage and economic espionage. Although a victim country could assert that spying violates the principles of sovereignty and non-intervention, state practice has accepted state-sponsored espionage such that these appeals are not serious claims. Although cyber espionage is sometimes described as "cyber attacks" and "cyberwar," no government regards cyber espionage of any kind as a prohibited use of force. Other bodies of international law under which espionage issues arise, such as rules on armed conflict and on diplomatic relations in peacetime, do not prohibit or seriously constrain espionage or economic espionage.[10]

Thus, participation in, and tolerance of, spying indicates that espionage and economic espionage do not constitute wrongful acts triggering state responsibility under international law. Persons caught and accused of being spies can be punished, but international law contains protections for spies captured during armed conflict or covered by diplomatic immunity. The United States could not prosecute a Chinese diplomat caught engaging in economic cyber espionage unless China waived the immunity and, absent a waiver, could only declare the Chinese national *persona non grata,* triggering that person's return to China.[11]

*International Law, Criminal Law Enforcement Cooperation, and Economic Espionage*

Many countries prohibit economic espionage under national law. However, enforcement confronts difficulties because the offense’s elements include foreign government participation. Using extradition or mutual legal assistance treaties proves ineffective when the requested state is accused of sponsoring criminal acts.[12] The U.S.-China mutual legal assistance treaty[13]

is unlikely to be helpful to U.S. efforts to apply the EEA to perpetrators of economic cyber espionage linked to the Chinese government.

*International Law, Protection of Intellectual Property and Trade Secrets, and Economic Espionage*

Some experts have argued that the United States should use international trade law's protections for intellectual property against countries engaged in economic cyber espionage.[14] In trade and investment agreements, states have used international law to protect intellectual property rights of private-sector enterprises. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of the World Trade Organization (WTO) requires each WTO member to protect certain types of intellectual property rights, including trade secrets, within its territory.[15]

However, WTO members have, to date, shown no interest in addressing economic espionage within the WTO despite mounting worries about this practice.

One reason why WTO members have not used the WTO is the difficulty of formulating claims that economic espionage violates WTO agreements. WTO rules create obligations for WTO members to fulfill within their territories and do not generally impose duties that apply outside those limits. WTO members that covertly obtain intellectual property of nationals of other WTO members operating in their territories could violate WTO obligations to protect such property. However, the economic espionage of greatest concern—and especially acts of remotely conducted economic cyber espionage—involves governments obtaining information from private-sector companies located outside their territories.

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. Usually, establishing governmental responsibility for challenged acts is not difficult, but WTO cases have not involved accusations against government-sponsored espionage. It is not clear that a WTO member could satisfy this burden by relying on evidence from private-sector entities (e.g., Mandiant's report) and without revealing counter-intelligence means and methods.

Another strategy proposed by experts is for the United States to impose trade sanctions on countries engaged in economic cyber espionage and justify the sanctions under national security exceptions in WTO agreements.[16] This approach admits that unilateral trade sanctions would violate WTO obligations and require an exception to justify them. Whether a WTO member’s invocation of a national security exception could be successfully challenged remains controversial.

Other proposals focus on U.S. law rather than international law. For example, experts have argued that the United States should (1) impose sanctions on foreign nationals and companies that engage in, or benefit from, economic espionage, and (2) permit civil claims in U.S. courts against foreign governments that steal U.S. trade secrets under the Foreign Sovereign Immunities Act.[17] These proposals borrow from other contexts, such as countering terrorism and transnational crime.[18]

**The Obama Administration's New Strategy**

Arguing that trade secret theft threatens U.S. national security, the Obama administration's strategy contains five strategic actions:

- Focus diplomatic efforts to protect trade secrets overseas;
- Promote voluntary best practices by private industry to protect trade secrets;
- Enhance domestic law enforcement operations;
- Improve domestic legislation; and
- Public awareness and stakeholder outreach.

Although the administration considers trade secret theft a serious matter, its strategy does not assert that economic espionage violates international law. Nor does it contain a blueprint for international legal changes that would directly address economic cyber espionage. The strategy seeks "improved legal frameworks, stronger enforcement of existing laws and strong and efficient remedies for trade secret owners,"[19] but its focus is at the national level, as evidenced by the domestic-centric content of four of the action items.

Internationally, the strategy aims to raise trade secret protection as a priority in diplomatic processes and legal agreements. The administration will use "formal cooperative agreements or arrangements with foreign governments" in investigations that require law enforcement cooperation (e.g., mutual legal assistance treaties; INTERPOL).[20] The U.S. government will also emphasize trade secret protection in trade and intellectual property forums, including the TRIPS Council at the WTO and the Asia-Pacific Economic Cooperation process.[21]

More specifically on trade, the strategy includes using "trade policy tools to increase international enforcement against trade secret theft to minimize unfair competition against U.S. companies."[22] This approach will involve deeper cooperation with like-minded trading partners, seeking "new provisions on trade secret protections" in trade negotiations (e.g., the Trans Pacific Partnership Agreement), and using the Special 301 "priority watch list" process "to gather and . . . act upon information about the adequacy and effectiveness of trade secret protection by U.S. trading partners."[23]

None of the strategy's trade-related initiatives mention potential legal claims against other WTO members. Under WTO rules, any trade-restrictive measures imposed by the United States based on information gathered in the Special 301 process cannot be taken unilaterally and must be authorized by the WTO dispute settlement process—unless the United States relied on a national security exception to justify unilateral sanctions.

**Conclusion**

Through its strategy, the Obama administration seeks international change on attitudes about trade secret theft, including that undertaken through cyber technologies, and is putting increased pressure on China on this issue.[24] Whether the administration can achieve change and translate it into international law on economic cyber espionage remains to be seen, but obstacles exist.

Many countries, including China, do not consider economic espionage different from traditional espionage and will not cooperate when they perceive the United States to be a pervasive practitioner of cyber espionage. In addition, focusing on national criminal laws and law enforcement cooperation appears ill-suited to economic cyber espionage, especially given the lack of international law regulating economic espionage, the ability to conduct economic espionage remotely, the way cyber technologies exacerbate the attribution problem, and the problems cooperation confronts when economic espionage is the crime in question.

The flare-up between the United States and China over economic cyber espionage also intensifies geo-political competition over cyberspace and cybersecurity. Chinese perspectives on the accusations leveled against China emphasize the extent of U.S. cyber espionage and Chinese perceptions of American attempts to impose its interests and values on other countries through political and military cyber dominance.[25] In this deteriorating climate, espionage of all kinds is only likely to increase in the foreseeable future.

**About the Author:**

David P. Fidler, an ASIL member, is the James Louis Calamaras Professor of Law at the Indiana University Maurer School of Law. He is also a Fellow at the Indiana University Center for Applied Cybersecurity Research.

**Endnotes:**

[1] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[2] White House, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (Feb. 2013), http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[3] *See, e.g.*, White House, *National Strategy to Secure Cyberspace* viii (Feb. 2003), http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf; *see also* White House, *Cyberspace Policy Review* i (May 8, 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; *see also* White House, *International Strategy for Cyberspace* 17 (May 1, 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[4] Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History*, The Cable, July 9, 2012, *available at* http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

[5] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace* 5 (Oct. 2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[6] *Id.*

[7] Nicole Perlroth, *Hackers in China Attacked the Times for Last 4 Months*, N. Y. Times, Jan. 30, 2013, *available at* http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html; Craig Timberg and Ellen Nakashima, *Chinese Hackers Suspected in Attack on The Post's Computers*, Wash. Post, Feb. 1, 2013, *available at* http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html; Siobhan Gorman, Devlin Barrett, and Danny Yadron, *Chinese Hackers Hit U.S. Media*, Wall St. J., Feb. 1, 2013, *available at* http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html.

[8] Ellen Nakashima, *U.S. Said to be Target of Massive Cyber-Espionage Campaign,* Wash. Post, Feb. 10, 2013, *available at* http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html.

[9] Mandiant, *supra* note 1, at 3.

[10] *See generally* Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law,* 27 Mich. J. Int'l L. 1071 (2006).

[11] Vienna Convention on Diplomatic Relations arts. 31, 32, 9, Apr. 18, 1961, 500 U.N.T.S. 95 (entered into force Apr. 34 1964), *available at* http://untreaty.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf.

[12] *See* Susan W. Brenner and Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 Hous. J. Int'l L. 389, 438-440 (2006).

[13] Agreement on Mutual Legal Assistance in Criminal Matters, U.S.-China, June 19, 2000, T.I.A.S. No. 13,102, *available at* http://www.state.gov/documents/organization/126977.pdf.

[14] *See, e.g.,* Richard Clarke, *A Global Cyber-Crisis Waiting to Happen*, Wash. Post, Feb. 7, 2013, *available at* http://www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html.

[15] Agreement on Trade-Related Aspects of Intellectual Property Rights, 1869 U.N.T.S. 299, 33

I.L.M. 1197 (1994), *available at* http://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

[16] *See, e.g.,* James A. Lewis, Center for Strategic and International Studies, Conflict and Negotiation in Cyberspace 50 (Feb. 2013).

[17] *See, e.g.,* Dan Blumenthal, *How to Win a Cyberwar with China*, ForeignPolicy.com, Feb. 28, 2013, http://www.foreignpolicy.com/articles/2013/02/28/how_to_win_a_cyberwar_with_china?. *See also* Laura Saporito and James A. Lewis, *Cyber Incidents Attributed to China* (Mar. 11, 2013), *available at* http://csis.org/files/publication/130311_Chinese_hacking.pdf.

[18] *See* Foreign Sovereign Immunities Act, 28 U.S.C. § 1605A (2012); Exec. Order No. 13,581, *Blocking Property of Transnational Criminal Organizations* (July 24, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/07/25/executive-order-blocking-property-transnational-criminal-organizations.

[19] White House, *supra* note 2, at 3.

[20] *Id.* at 5.

[21] *Id.* at 4.

[22] *Id.*

[23] *Id.*

[24] Ellen Nakashima, *US Publicly Calls on China to Stop Commercial Cyber-Espionage*, Wash. Post, Mar. 11, 2013, *available at* http://www.washingtonpost.com/world/national-security/us-publicly-calls-on-china-to-stop-commercial-cyber-espionage-theft-of-trade-secrets/2013/03/11/28b21d12-8a82-11e2-a051-6810d606108d_story.html.

[25] *See, e.g.,* Yang Jing, *Deterrence Has No Place in Cyberspace*, China-US Focus, Feb. 28, 2013, *available at* http://www.chinausfocus.com/peace-security/deterrence-has-no-place-in-cyberspace/.