The Export Practitioner

Timely News and Analysis of Export Regulations

JANUARY 2015

VOLUME 29
NUMBER 1

INSIDE

ALSO INSIDE

JUSTICE USING "ALL TOOLS" APPROACH TO EXPORT VIOLATIONS AND CYBERESPIONAGE

By: Jonathan C. Poling*

In recent months, the Justice Department's National Security Division has referred to what it calls an "all tools" approach to its international enforcement efforts against violations of export control, trade sanctions laws, and increasing cyberespionage and cybercrime cases.

The "all tools" approach considers criminal prosecution as only one tool in the government's toolkit and simultaneously deploys the government's other "tools," such as punitive trade-related measures and international diplomacy, to cease foreign, illegal activity targeting the United States.

Criminal prosecution is inherently limited in its ability to cease the illegal activity of individuals. Nowhere are these limits to government prosecution more challenging than in cybercrime and the need for "all tools" measures beyond an indictment more great.

Daily news headlines have emphasized the growing U.S. focus on cyberespionage, particularly from China. No U.S. company has been immune to cyber attacks, including major retailers, communications companies and service providers. As FBI Director James Comey has said: "There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked."

Example Seen in Li Fangwei Case

What this "all tools" approach may look like in the future is best illustrated in the case of Li Fangwei, an alleged supplier and contributor to Iran's defense program. The U.S. government successfully integrated the efforts of several agencies to disgorge almost $7 million in Li's profits. John P. Carlin, assistant attorney general for the national security division, called Li's case "an outstanding example of multiple agencies working together to focus various enforcement efforts on the significant threat to our national security posed by such proliferation networks."

Li, more commonly known as "Karl Lee," is an alleged supplier to Iran's Defense Industries Organization and Aerospace Industries Organization, as well as a principal contributor to the country's ballistic missile program. From 2006 to 2014, while the U.S. and its allies engaged in nuclear talks with Iran, Li is believed to have helped divert sanctioned weapons materials to Iran.

Li allegedly used a network of Chinese front companies to channel millions of dollars in illicit business to Iranian companies via U.S.-based financial institutions. According to the indictment, the illicit business included sales of specialized metals used in long-range missiles and centrifuges that can enrich uranium, as well as other highly-controlled goods that the United States, United Nations, and others have banned from transfer to Iran.

On April 28, 2014, Justice and the New York district attorney indicted Li, a Chinese national, for violating federal fraud laws and U.S. sanctions against Iran. Despite the indictment, a Justice press release said Li remains a fugitive.

If he ever were arrested, Li would face seven separate charges: one count of conspiracy to violate the International Emergency Economic Powers Act (IEEPA), two counts of violating the IEPPA, one count of conspiracy to commit money laundering, one count of conspiracy to commit wire and bank fraud, and two counts of wire fraud.

With a federal arrest warrant issued, the State Department offered a $5 million bounty for information leading to his arrest and/or conviction.

The FBI added Li to its Most Wanted List, splashing a grainy, black-and-white photo of Li on "WANTED" posters stating Li "should be considered an international flight risk." Although Li is unlikely to face trial anytime soon, his conviction could carry a maximum prison sentence of 20 to 30 years.

Li's Front Company LIMMT

Long before Li's indictment, the U.S. had already begun to impose targeted sanctions on him and his front company, LIMMT Economic and Trade Company, Ltd. (LIMMT). In 2006 and 2009, respectively, the Treasury Department's Office of Foreign Assets Control (OFAC) added Li and LIMMT to its List of Specially Designated Nationals and Blocked Persons, often called the SDN List (see *The Export Practitioner*, May 2014, page 13).

The listings blocked Li and LIMMT from conducting any business through the United States without OFAC's authorization and effectively forced some of Li's activities underground.

Based on the FBI investigation that led to Li's indictment, OFAC added eight more of his front companies to its SDN List in April 2014. Commerce's Bureau of Industry and Security (BIS) also put nine of Li's China-based suppliers to the BIS Entity List for their alleged roles in his plot.

Consequences and Benefits of Using All Tools

The use of designations and sanctions provide the government leverage based on intermediaries' needs to access U.S. markets, where the indictment against a foreign person or company with limited connections to the U.S. is not sufficient deterrence.

Although Li has denied selling any sanctioned materials to Iran, in September 2014, a British research team identified online advertisements by Li's company Sinotech (Dalian) Carbon & Manufacturing, a producer of electrodes used in ballistic missiles.

By November 2014, Alibaba -- China's largest e-commerce company which connects Chinese exporters with foreign customers -- removed Sinotech's ads, citing its willingness "to co-operate with law enforcement authorities worldwide to remove problematic product listings promptly upon receipt of notice."

In the past, Alibaba's website hosted online listings for companies accused of helping Iran and North Korea obtain nuclear and missile technology.

By leveraging sanctions and trade designations, the U.S. government put foreign governments and companies on notice of its enhanced scrutiny of trade violations. These measures also helped shut down some of Li's illegal activities, such as on Alibaba, and may have alienated Li's potential business associates.

The FBI's "Most Wanted" listing put Li on other international watchlists, and State's $5 million reward gave his cohorts an opportunity to profit from sharing information about Li rather than working with him.

Funds Seized from Li's Front Companies

The day after Li was indicted, Justice and the FBI announced that their combined efforts contributed to the ultimate seizure of $6.8 million from his front companies based on seizure warrants issued in December 2013 and April 2014. In addition to its criminal complaint, Justice issued a civil complaint for Li's alleged IEEPA and fraud violations and sought the forfeiture of those funds to the United States.

The "all tools" approach that Carlin has trumpeted in press releases is a continuation of a highly coordinated effort by Commerce, Treasury and other authorities to squeeze foreign companies that are under the control of or related to companies that are being investigation.

Other cases reflecting this approach involved *United States v. Aviation Services International*, *United States v. Balli Aviation*, and *United States v. Arc Electronics,* where the U.S. employed the use of designations as "tools" to disrupt illicit networks and obtain additional evidence relating to ongoing investigations. In *Arc Electronics*, over 165 persons and entities were placed on the Entity List the day Justice announced the indictment of the firm and its alleged co-conspirators.

In addition to having a powerful impact on companies beyond an indictment, this approach has led to new evidence being provided by companies that have been designated or those dealing with designated entities. This has included evidence from outside the U.S. that would otherwise be difficult for Justice to obtain and which must be provided to the U.S. government as part of a company's application to challenge the designation.

Cyberespionage & Cybercrime

Even the most casual observer can see the shift in export controls and sanctions enforcement to focus on data. This will likely remain a focus of David Laufman, the newly appointed chief of Justice's Counterespionage Section, which has responsibility for prosecuting export control and sanctions violations, including those involving cyberespionage.

As BIS Assistant Secretary David Mills said in a recent speech in 2014, "The theft of export-controlled information from your computer systems as a result of foreign cyber actions is a violation of export control laws."

U.S. export controls laws govern not just weapons and other defense-related or dual-use articles, but also technical data, sensitive software and proprietary technology.

In the wrong hands, export-controlled data and technology can be used to disrupt government or corporate infrastructure; give an unfair advantage to foreign state-owned enterprises or industry; and compromise national security.

The intersections between export control and cybercrime go beyond the issue of export-controlled data. There is some evidence that companies involved in international trade-related disputes may be targeted for cyberattacks.

Hacking Alleged in Antidumping Cases

Justice recently indicted five Chinese military officials who allegedly stole valuable trade secrets from the computer systems of U.S. nuclear power, metals, and solar products companies.

According to the May 2014 indictment, the individuals conspired to gain unauthorized access to American computers to steal information that would be profitable for Chinese companies, including state-owned enterprises, and at least some of the intrusions appeared to retaliate against U.S. companies involved in trade disputes with China.

In 2010, U.S. Steel, a major American steel manufacturer, was a lead petitioner in antidumping litigation against Chinese steel manufacturers, who were allegedly "dumping" steel in the U.S. market below market prices. According to a May 2014 indictment of Chinese military hackers, two of the defendants used spear-phishing emails to access U.S. Steel's computers, and one defendant was able to "identify and exploit vulnerable servers."

In another incident in 2011, SolarWorld, a solar panel manufacturer targeted by Chinese military hackers, was also a lead petitioner in antidumping litigation against its direct Chinese competitors. Following one preliminary determination by Commerce, one or two of the Chinese military defendants hacked into SolarWorld's computers over a dozen times to steal emails and files.

Although it is unclear what recourse a hacked company may have, SolarWorld Americas may be using the allegations contained in the recent indictments to initiate a Commerce investigation into the hacking incident.

The Chinese hackers allegedly stole highly detailed information about SolarWorld Americas' financial position, production capabilities, cost structure, business plan, and trade litigation strategy.

The company asked Commerce to investigate the breach and, if necessary, impose additional tariffs on imports of Chinese solar panels presumably to offset some of the company's estimated losses due to the breach.

Cybercrime Is Justice's High Priority

Cracking down on cybercrime and cyberespionage — specifically, the theft of trade secrets and export-controlled technology affecting national security — has been among Justice's highest priorities since 2006.

The National Security Division's integrated strategy is precisely what Assistant Attorney General Carlin credits for the Chinese military hackers' indictment, which Carlin called the "largest fusion of law enforcement and industry" in shutting down illegal cyber-operations. Meanwhile, the Chinese government has flatly denied the allegations.

Carlin argues that criminal prosecutions strip away anonymity and send an important message to cybercriminals that "[y]ou're not anonymous; you can't hide; [and] you're not just fingers on a keyboard."

Still, even though the Chinese military hackers are unlikely to face trial in the U.S., Carlin argues that criminal prosecution is a particularly important part of the "all tools" approach in the cybercrime context. Often sitting behind computers beyond U.S. jurisdictional reach, cybercriminals like the Chinese military hackers are sometimes sponsored, paid and protected by foreign governments.

But so far, the U.S. has not used robustly designations of persons or companies because of their involvement in cyberattacks. Justice clearly wants to move in this direction and, therefore, it is likely to use different tools more often to address this growing threat. If the "all tools" approach continues, it seems the public will see more multi-charge indictments from Justice and expanded designations from export control agencies to address export control and trade sanctions violations, cyberespionage and cybercrime, particularly in those areas involving the exfiltration of export-controlled data.

** Jonathan C. Poling is a partner in the International Trade practice at Akin Gump Strauss Hauer & Feld in Washington, DC. He can be reached at jpoling@akingump.com or 202.887.4029.*