CYBERSECURITY

The U.S. Corporate Theft Principle

By Jack Goldsmith Wednesday, May 21, 2014, 8:07 AM

David Sanger's piece in this morning's NYT explores the USG's attempts to justify cracking down on cyber-theft of intellectual property of U.S. firms while at the same time continuing to spy on non-U.S. firms for different purposes. We are familiar with the USG policy. As DNI Clapper says in Sanger's story, the USG does not use its "foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of — or give intelligence we collect to — U.S. companies to enhance their international competitiveness or increase their bottom line." This convoluted but carefully worded statement permits the USG to engage in a great deal of theft of foreign company trade secrets. Sanger's story talks about the United States stealing information from Petrobras (the Brazilian national oil company), China Telecom, Huawei, Pacnet (the Hong Kong operator of undersea fiber optic cables), and other state-owned oil companies, as well as Joaquín Almunia, the antitrust commissioner of the European Commission. Sanger

Jack Goldsmith is the Henry L. Shattuck Professor at Harvard Law School, a Senior Fellow at the Hoover Institution at Stanford University, and co-founder of Lawfareblog.com. He teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws. Before coming to Harvard, Professor Goldsmith served as Assistant Attorney General, Office of Legal Counsel from 2003-2004, and Special Counsel to the Department of Defense from 2002-2003. Follow him on Twitter @JackLGoldsmith. His personal website can be found at jackgoldsmith.org.

MORE ARTICLES ›

RELATED ARTICLES

explains that USG policy allows spying on these firms and persons, and allows it to be done for the purpose of helping the American economy and American competitiveness in general. Sanger cites USG officials who say that "while the N.S.A. cannot spy on Airbus and give the results to Boeing, it is free to spy on European or Asian trade negotiators and use the results to help American trade officials — and, by extension, the American industries and workers they are trying to bolster." The officials might have added that the NSA can also spy on Airbus itself for purposes of analyzing the French economy, or preparing for a trade negotiation, or any other purpose that would serve U.S. economic interests generally, as long as the spying is not done specifically for an American company and the information is not given to the American company.

Sanger reports that "every one of the examples of N.S.A. spying on corporations around the world is becoming Exhibit A in China's argument that by indicting five members of the People's Liberation Army, the Obama administration is giving new meaning to capitalistic hypocrisy." I have used the word "hypocrisy" in this context as well, but maybe that is not the right term. Hypocrisy is professing to believe in certain principles while not in fact living up to them. One could argue that the United States is not hypocritical because it believes in and lives up to this principle: Spying on foreign firms is presumptively allowed, but not on behalf of a particular U.S. firm, and the information cannot be given to a U.S.

Five Important (Or At Least Interesting) Provisions in the Intelligence Authorization Bill HPSCI Passed
Robert Chesney Mon, Jun 8, 2015, 11:00 AM

The OPM Data Breach: Raising All Sorts of Government Enforcement and Privacy Protection Questions
Carrie Cordero, Paul Rosenzweig Sun, Jun 7, 2015, 1:30 PM

Et Tu, Charlie? The New York Times's Savage Blunder
Benjamin Wittes Fri, Jun 5, 2015, 7:37 AM

The Data Breach At The Office Of Personnel Management
Herb Lin Thu, Jun 4, 2015, 9:29 PM

A New Journal — Dedicated to Cybersecurity
Susan Landau Tue, Jun 2, 2015, 10:24 AM

firm. Setting aside those aspects of the recent indictment that appeared to go after spying in connection with trade negotiations, let us posit that the United States lives up to this principle and is not hypocritical. But is the principle – call it the U.S. corporate theft principle – defensible?

It does not find any basis that I know of in law. International law has traditionally not regulated espionage, especially cross-border cyber-theft. If this norm is changing after Snowden, it is not obviously changing in a way that conforms to the U.S. corporate theft principle. As for domestic law, what the Chinese hackers are alleged to have done definitely violates U.S. law. But they also would have violated U.S. law if they stole information from the Pentagon, or if they stole information from Google for purposes of enhancing China's overall economic posture (i.e. consistent with the U.S. trade theft principle). This is an important point: Most if not all cyber-snooping from abroad, against public or private entities, and for whatever purpose, violates U.S. domestic law. And most if not all USG cyber-snooping abroad violates foreign domestic law. With Monday's indictment the United States is selectively enforcing its domestic criminal laws to serve (and be consistent with) a broader national security policy. But the underlying federal laws – the Computer Fraud and Abuse Act, laws against private and public theft, and the like – are being violated every day on a much, much broader basis.

If the U.S. corporate theft principle has no basis in law, is it otherwise defensible as policy? As I have written before, the policy seems obviously designed to serve the interests of a country, the United States, that possesses enormous intellectual property resources and does prodigious amounts of spying abroad against nations that have relatively few intellectual property resources. If this is your position in the world, then you want a regime that maximizes room for cyber-espionage while carving out an exception of cyber-theft of intellectual property on behalf of, or to be given to, particular firms. And that is what the United States does. To China, of course, the situation is more or less the opposite. And so China sees the world, as Sanger reports, like this:

> In the Chinese view, the United States has designed its own system of rules about what constitutes "legal" spying and what is illegal.
>
> That definition, the Chinese contend, is intended to benefit an American economy built around the sanctity of intellectual property belonging to private firms. And, in their mind, it is also designed to give the N.S.A. the broadest possible rights to intercept phone calls or email messages of state-owned companies from China to Saudi Arabia, or even private firms that are involved in activities the United States considers vital to its national security, with no regard to local laws.

For years U.S. officials have explained where it draws the line on spying on foreign firms. What I have not heard is a response to China's claim that the line is self-serving and unprincipled. I imagine that the United States will try to find some basis in international law, perhaps international economic law, for its position, but all such arguments that I have seen are weak.

Of course there is nothing wrong with the United States trying to establish a principle of corporate espionage that serves its interests and that disserves our adversaries' interests – that is what international relations are about. As I have said before, "I would be quite pleased if the USG could establish a rule of espionage that allowed us to best serve our interests and that disserved China's interests." The question, however, is whether the United States has a strategy for establishing this principle. Indictments like the one we saw this week do not a strategy make, but perhaps other elements of a larger strategy are on the way. What the United States needs is an explanation convincing to audiences outside the United States about why its principle of corporate espionage is attractive beyond its furtherance of U.S. corporate and national security interests. I have never seen any such explanation.

Topics: Cybersecurity, Cybersecurity: Crime and Espionage