Exploring a Bad(?) Idea for Countering Economic Espionage

Herbert Lin

DO NOT CITE OR QUOTE
FOR DISCUSSION PURPOSES ONLY
NOT A SERIOUS PROPOSAL!!

State-supported (or at least state-tolerated) cyber-enabled espionage for economic purposes is a significant threat to U.S. interests. At the same time, recognizing that such activities do not rise to the level of an act of war, the United States has struggled to find an appropriate response that would help to curb such activities. On April 1, 2015, President Obama did sign an executive order allowing the imposition of penalties (e.g., freezing of assets, denials of visas) on individuals overseas who steal intellectual property or trade secrets or who benefit from the stolen secrets and property.[1] A Washington Post story elaborated on the order citing U.S. officials who said that the order would be particularly useful where law enforcement tools don't work in imposing a penalty on Chinese military hackers that engage in industrial espionage as well as the state-owned enterprises that benefit from their campaigns.[2] The story also stated that "any case must be supported by evidence that could withstand a court challenge", although this provision does not appear in the executive order itself.

While the authority to penalize individuals through the use of financial sanctions does give the United States tools that it did not previously have, it is important to recall that last year, the United States indicted under the Economic Espionage Act (18 USC 1831 and 18 USC 1832) 5 Chinese individuals alleged to have stolen "[U.S.] trade secrets that would have been particularly beneficial to Chinese companies" and "sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity."[3] Note also that this action seems not to have had the slightest effect on Chinese economic espionage activities against the United States.

This paper outlines a proposal to respond to foreign industrial espionage, where "industrial espionage" by Nation A (e.g., China) should be understood to mean the use of clandestine means to obtain information from a commercial firm in Nation B (e.g., the United States) for the benefit of a firm in Nation A. This proposal has the following elements:

- A declaration that as a general principle, the United States deplores the use of industrial espionage as a significant impediment to the smooth functioning of the world's economy. (The United States has made such statements in the past.)
- A recitation of the facts regarding foreign industrial espionage against the United States and its firms, including an association (when known) of nations known to have sponsored (or at least tolerated) such activities.
- A statement that if such activities do not cease (or are not significantly reduced) in the future, the United States will—with great reluctance—abandon its long-standing blanket ban on

[1] https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

[2] http://www.washingtonpost.com/world/national-security/us-to-establish-sanctions-program-to-combat-cyberattacks-cyberspying/2015/03/31/7f563474-d7dc-11e4-ba28-f2a685dc7f89_story.html.

[3] http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

industrial espionage, and will instead selectively target offending nations (or firms in such nations) with the explicit intention of obtaining information that will advantage certain U.S. companies for purposes of leveling the playing field until the offending nations take meaningful action against their own industrial espionage.

Objections to the U.S intelligence community engaging in industrial espionage for the benefit of U.S. companies have taken two primary forms. First is the long standing objection to explicit government intervention in the operation of free markets. Second is the difficulty of allocating benefits to specific U.S. companies—providing useful information from a foreign company to Company A rather than Company B may well result in a lawsuit by Company B for being denied those benefits.

On the first objection, the proposal acknowledges the undesirability of such an action, but suggests that such action is necessary if the economic playing field is to be fair and level. Moreover, it contemplates such action for only as long as such activities are being conducted against U.S. firms.

The second objection could be managed by a mechanism in which qualified companies bid at auction for the information derived from U.S. industrial espionage activities conducted by the intelligence community. Qualified companies would be those who passed certain background checks (e.g., for security clearances for its senior management) and established certain internal mechanisms for protecting sensitive information.

This idea is almost universally derided as a bad one. What I want to know is – why? Let me make clear – I am not advocating this idea in any way. But analyzing the proposal (or a similar one, modified in response to serious objections) is for me a way to understand the problem more deeply.