Secrets and Lies

The Rise of Corporate Espionage in a Global Economy

Eamon Javers

In 2008, thousands of employees at American defense and technology companies received emails from an executive-recruiting firm based in Tokyo called Fox Adams. The correspondence hinted at lucrative job opportunities and urged the employees to reply with contact information. However, there was something wrong with the email: Fox Adams did not exist.

Security experts and veteran U.S. intelligence agents examined the issue and concluded that Fox Adams was simply a front for Chinese intelligence.[1] According to these authorities, the spam emails were part of a very wide net cast by the Chinese to help identify American executives with access to sensitive technologies. Under the guise of a job interview, anyone who replied to the email would likely be quizzed for details about his or her work, access to technology, and experience. Several veteran U.S. intelligence officers described the Fox Adams ploy as a routine Chinese intelligence probe of U.S. corporate infrastructure, something they say has been on the rise in recent years as the Beijing government attempts to steal technology and infor-

Eamon Javers is a Washington correspondent for CNBC and author of the book *Broker, Trader, Lawyer, Spy: The Secret World of Corporate Espionage*.

mation that can help keep the country's astonishing economic growth on pace with aggressive government goals.

All of this means that American corporate executives must be increasingly guarded against spying by current employees, former employees, computer hackers, and the full gamut of Cold War-style intelligence techniques.

credentials, the Mattel market intelligence employees allegedly used spy cameras to film secret demonstration models of toys that rival companies planned to launch. Mattel said there was no merit to the charges, which came in the course of a long-running litigation battle over which company should hold the rights to the Bratz dolls.

In the second category—financial

It was this wave of Chinese hacking attacks that finally drove Google into the arms of the U.S. National Security Agency.

Forms of Corporate Espionage. China is not the only perpetrator. Corporate espionage can be separated into three broad categories: spying practiced by companies, by financial firms, and by nations.

An example of the first category of corporate espionage—companies spying against other companies in order to harm competitors—came to light late this summer. MGA Entertainment Inc., the maker of the wildly popular Bratz line of toy dolls, filed documents in federal court alleging that rival Mattel Inc. maintained an internal "market intelligence" unit whose members traveled the country under fake identities, gaining entrance to confidential product briefings by posing as potential customers of rival toy makers.[2] There, with their cover stories backstopped by fake business cards and

firms gathering information to use in market trading—corporate spy organizations operate around the globe, working for Wall Street, hedge funds, and wealthy individuals. In one case, a private spy firm even flew aerial surveillance missions for the notorious energy-trading firm Enron.

This private spy firm was Diligence, a company founded by two former intelligence officers (one previously worked for the CIA, the other for British MI5). In the early 2000s, Diligence was hired by Enron to develop information about the European power industry that might prove advantageous in Enron's daily buying and selling of energy contracts. However, Diligence operatives didn't scour trade publications and interview experts, as a typical consulting firm might have; instead, the spies-for-hire set up thermal imaging equipment in fields around some

of Europe's biggest power plants.[3] They used the data to develop a comprehensive, real-time look at the production of energy being sold into the market. The more energy being moved into the market, the lower prices would be. The less energy, the higher prices would be. That is invaluable information for an energy trader like Enron.

Diligence did not stop with thermal imaging. Veteran CIA officer and co-founder Mike Baker chartered private airplanes and flew surveillance missions over the power plants, looking for signs of when the plants might be taken off line for maintenance.[4] A power plant shutting down has a dramatic effect on supply and demand in the market, and pinpointing the dates of such a shutdown in advance could yield arbitrage opportunities for Enron. Baker relentlessly circled the plants, looking for declining coal stacks—because the power companies would not order more coal in advance of a shut down. The planes even searched for port-o-potties being set up on the property since annual maintenance can involve a large number of workers.[5] By watching for such mundane details, Diligence was able to spot trading opportunities in the market.

The last category of corporate espionage—nations spying on companies—can be difficult to prove. Government intelligence agencies operate behind layers of plausible deniability. The bogus Fox Adams emails were ham-fisted in comparison to a slew of recent cases in which Chinese-connected agents have tried to steal American hybrid car technology, insecticide manufacturing techniques, and—in the most high profile case to date—the cyber secrets of the search-engine giant Google.

In order to keep their economic growth miracle going, the Chinese are trying to move up the manufacturing food chain, evolving from low-cost providers of unskilled labor to producers of more technically complicated goods at higher price points.[6] Since the United States is far ahead in a wide array of industries, one way to catch up is to steal the plans, formulas, and algorithms that allow American companies to dominate world markets. If the Chinese can steal such secrets faster than Americans can develop new ones, they will close the gap between the two economies. Andrew Arena, Special Agent in Charge of the FBI office in Detroit that conducted one investigation into Chinese corporate espionage, noted that "theft of trade secrets is a threat to national security," demonstrating the U.S. government's concern with these intrusions.[7]

In secret diplomatic cables revealed by the website Wikileaks in late 2010, American diplomats in Beijing concluded that the electronic attacks on Google's home servers to obtain the identities of Chinese dissidents and Google's proprietary source code had been ordered at the highest level of the Chinese government. In one cable, the diplomats said they had a well-placed source who said that Li Changchun, a

member of China's Politburo Standing Committee, had been shocked to find negative information about himself when he Googled his own name on the Chinese language version of the search engine's website. Another cable revealed that Mr. Li was a key leader in China's anti-Google efforts, and that his self-Googling likely led to his interest in the company.[8]

The effort was part of a wider campaign of corporate espionage against American companies and government agencies that began as early as 2002, the American cable-writers concluded. Particularly vulnerable were Chinese subsidiaries of non-Chinese companies, whose local executives were often afraid to inform their Western bosses about the extent of Chinese government meddling. "Contacts in the technology industry tell us that Chinese interference in the operations of foreign businesses is widespread and often underreported to U.S. parent companies," reported one U.S. diplomat.[9]

It was this wave of Chinese hacking attacks that finally drove Google into the arms of the U.S. National Security Agency, announcing a partnership with the American technological spy agency to help Google fend off intrusion attempts.[10] For Google, as for many companies, one option when faced with government-funded spying is to team up with another government. Even in a global economy, it seems, companies sometimes have to choose sides. Although it appears that the Google incident was partially motivated by politics, it highlights the willingness of foreign countries—and China in particular—to resort to illegal activities in order to collect the secrets of private companies.

If it is any consolation to Western intelligence, Chinese economic espionage is not always flawless. Fox Adams, the bogus executive recruiting firm experts suspected of being a front for Chinese intelligence, made some noticeable mistakes. Emails coming from purported "Fox Adams" recruiters used names that looked like they had been randomly mixed and matched from American phone books—and by someone with little feel for American culture. One email was signed by a recruiter supposedly named "Jesus Black." The Internet domain registration for the website www.foxadams.com was listed to a New Jersey address that does not seem to exist. The phone number listed was "1-234-5678."[11]

The Rise of Private Intelligence Firms. Corporate intelligence gathering has created a new market for a rising class of private espionage firms—companies set up by veterans of the world's intelligence agencies that sell their services on a contract basis to companies and financial firms. In the 21st Century, companies and financial firms have a greater need for information than ever and—particularly in emerging markets—the best providers of that information are former intelligence officers who are deeply steeped

in the leadership and politics of a given country and intimately familiar with its local powerbrokers.

There is nothing wrong with companies turning to such intelligence advisors for information on potential new business partners and advice on the political landscape in unfamiliar countries, but there is enormous potential for abuse by corporate intelligence firms. The ways in which they gather information can wander into a legal gray area, and their offensive operations—efforts to damage competitors through underhanded tactics including surveillance, placing of operatives inside competitors' firms, and other techniques the companies would be embarrassed to admit in public—can deprive legitimate businesses of opportunities to succeed.

The corporate espionage industry is deliberately hidden in a thicket of complex relationships.

Indeed, the corporate espionage industry is deliberately hidden in a thicket of complex relationships designed to obscure just who is working for whom. Often, these firms are hired as subcontractors for corporate law firms and they argue that everything they do is covered by attorney-client privilege.[12] Thus, their operations do not surface to the public. In other cases, these private spy firms protect the secrecy of their operations around the world by using a series of cutouts and freelancers, each layer papered with strict non-disclosure agreements.

In public, they describe their services as "strategic advisory consulting," "risk mitigation analysis," or "litigation support." With names like "Diligence," "Control Risks Group," and "Hakluyt," these private intelligence firms hide in plain sight, offering extremely lucrative post-government career options for veterans of the CIA, the British MI5, and the former Soviet intelligence agency, the KGB.

The industry's growth is driven by several trends. The increased globalization of commerce has created a demand for companies to understand the relationships between business and political elites in countries they often know little about. Who better to help piece together the puzzle than the men and women who spent their careers gathering the same information for their governments?

And, of course, there is the romance of it all. Globe-hopping corporate executives sometimes cannot resist the glamour of the spy business. The romance factor is often implicit in the spies' sales pitches to prospective clients. In 2001, for example, former British secret intelligence service officer Christopher James wrote to Enron executive Jeff Skilling, hop-

ing to land Skilling as a new client of his London-based private intelligence firm, Hakluyt. "Dear Mr. Skilling," he wrote, "Your office has asked me to outline Hakluyt's services. … I would simply say this: Hakluyt is what you make of it—it places an unparalleled private intelligence network at the personal disposal of senior commercial figures." [13]

Responding to Corporate Espionage. What is astonishing about this private spy industry is how little the U.S. government seems to know about it. The CIA says it does not know where its former agents are working today and argues that tracking where they are employed would violate the civil rights of those agents; it surely behooves the U.S. intelligence community to have some sense of where its alumni are plying their trade, however, and whose payrolls they join when they enter the private sector.[14]

What is astonishing about this private spy industry is how little the U.S. government seems to know about it.

The CIA and similar organizations should know where their alumni work, particularly when they are being hired by foreign governments, oligarchs, and political parties. Some of the information is not difficult to come by; the websites of some of the private intelligence firms are a handy place to start. Western intelligence agencies have a vested interest in knowing where such people are employed and they should therefore track that information. Retired spies working in corporate espionage are not motivated by love of country any longer; they are motivated by love of money. When the spies have taken their skills and gone to work for paying clients, the governments that trained them with taxpayer money should monitor their activities to make sure that they are not deploying those skills in ways that undermine the very governments that provided them.

What is more, Western governments should be working harder to learn just how intertwined their intelligence services are with companies in the global economy. American intelligence agencies, for example, have long had a policy stating that their operatives are allowed to "moonlight" in their off hours and work for private sector firms.[15] That is, active duty intelligence officers, including those of the CIA, are allowed to work for private companies in order to make extra money. This creates a conflict of interest; agents who have access to classified materials of national security are also working with private firms that sometimes engage in questionable practices and undermine or violate domestic and international

laws. But even intelligence community leaders profess ignorance of the entire moonlighting system. In public testimony, Director of National Intelligence Dennis Blair said he had been surprised when the moonlighting was first revealed in the media. "Sometimes I too am surprised about what I read in the press about my own organization," Blair told Congress in February.[16]

As of fall 2010, the Director of National Intelligence has promised that a full review of such moonlighting will be completed and turned over to Congress.[17] That is a promising first step, but the American taxpayers need to know much more about the moonlighting habits of their intelligence officers. How often, for example, are active duty officers going to work for intelligence contractors—effectively forcing the taxpayer to pay twice for the same work?

American executives, too, need to educate themselves on the range of corporate espionage tactics arrayed against them. Unfortunately, the best way for them to do that right now is to reach out to some of the very private spy firms that are already in the corporate espionage business. Companies would be well advised to create internal monitoring units so that they can increase their ability to recognize and respond to corporate espionage. Some firms have already implemented these practices, but these are few and far between.

At its worst, corporate espionage between Western companies can include unethical and even illegal tactics, resulting in economic victories for the most underhanded firms, not necessarily for the most innovative. That is bad for capitalism. Corporate espionage by financial firms results in a transfer of information—and huge financial rewards—into the hands of the most powerful and wealthy, robbing average investors of a chance to participate in the benefits of the financial markets. That too, is damaging to the market economy, causing market participants to conclude that the system is stacked against them. Markets only work best when all players—large and small—have confidence that the rules are fair.

Finally, Western intelligence agencies must ratchet up their counterintelligence capabilities in the economic space. The intelligence community needs to focus on the threat to American global economic dominance that comes from Chinese economic espionage. One of the United States' greatest advantages in its competition with China is its corporate ingenuity, inventiveness, and sophistication. If Chinese intelligence is able to chip away at that advantage though corporate espionage techniques, it will do as much or more for China's position in the world than traditional spying on America's military capabilities or political leadership. Corporate espionage against the United States is one of many tools that China uses in its effort to

undermine America's position as the number-one economy on the planet, and to take for itself the geopolitical power and influence that comes with the position. This is a far deeper threat to free-market capitalism and is why America's counter-intelligence effort had better be up to the challenge.

NOTES

1 Eamon Javers. Anonymous interview, July 2009.

2 Jonathan Stempel and Dan Levine, "Mattel accused in Bratz battle of spying on rivals," Internet, http://www.reuters.com/article/idUSTRE67G4FZ20100817 (date accessed: 17 August 2010).

3 Eamon Javers, *Broker, Trader, Lawyer, Spy: The Secret World of Corporate Espionage* (New York: HarperCollins Publishers, 2010) 18.

4 *Ibid.*

5 *Ibid.*

6 Li Cui and Murtaza Syed, "IMF Working Paper: The Shifting Structure of China's Trade and Production," Internet, http://books.google.com/books?hl=en&lr=&id=dADHBsFWJLQC&oi=fnd&pg=PA3&dq=Chinese+economy+more+sophisticated+manufacturing&ots=FBaAzl5ZPY&sig=7uC-JIlzZD5igh1Bm1xtcBjQB34#v=onepage&q&f=false (date accessed: September 2007).

7 The Associated Press, "Ex-General Motors worker, husband accused of stealing hybrid vehicle secrets," Internet, http://www.mlive.com/auto/index.ssf/2010/07/ex-general_motors_worker_husba.html (date accessed: 23 July 2010).

8 James Glanz and John Markoff, "Vast Hacking by a China Fearful of the Web," The New York Times, 4 December 2010.

9 "A Selection from the Cache of Diplomatic Dispatches," Internet, http://www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html#report/china-99BEIJING999 (date accessed 5 December 2010).

10 Ellen Nakashima, "Google to Enlist NSA to help it Ward off Cyber Attacks," The Washington Post, 4 February 2010.

11 *See supra* note 1

12 Eamon Javers, *Broker, Trader, Lawyer, Spy: The Secret World of Corporate Espionage* (New York: HarperCollins Publishers, 2010), 265.

13 Archived Enron emails available at the website of the Federal Energy Regulatory Commission: http://www.ferc.gov/industries/electric/indus-act/wec/enron/info-release.asp.

14 Interview by the author with CIA public affairs office, 2009.

15 Eamon Javers, "CIA moonlights in corporate world," *Politico*, 1 February 2010.

16 Kasie Hunt, "CIA Moonlighting to be Investigated," *Politico*, 3 February 2010.

17 *Ibid.*