From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES

VOLUME 22 • NUMBER 1 • $15 SINGLE COPY PRICE Spring 2016 ©2016, AFIO

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
Web: **www.afio.com**, E-mail: **afio@afio.com**

GUIDE TO THE STUDY OF INTELLIGENCE

Industrial Espionage

by Edward M. Roche, PhD, JD

No information I received was the result of spying. Everything was given to me in casual conversations without coercion.

— Richard Sorge, interrogation at Sugamo Prison.[1]

Some persons argue that there is little harm from industrial espionage because "technology inevitably leaks out anyway."

— Count Alexandre de Marenches[2]

Industrial espionage comes in many forms as illustrated from the following case studies:

- The head of an adhesives company's research and development (R&D), a naturalized US citizen, became involved with the daughter of a Taiwanese industrialist, and eventually started to supply the Taiwanese company with all the R&D technical information from his American company, resulting in competing imports at a much lower cost.
- An American with close ties to a Middle East country provided to them information on government contracts and technical information, which allowed companies there to develop new products ahead of the US companies from which the original technical information was stolen.
- A secretary in a major soft drink manufacturer in Atlanta, Georgia, got involved with an ex-con and was induced to steal product samples and technical details for the next new soft drink product, and an attempt was made to sell this information to a competitor.
- A trained foreign agent, who had been in the United States for more than 20 years and had become a citizen, suddenly was "activated" by his controllers in Asia and given a "shopping list" of technical information to obtain, and then proceeded to steal massive amounts of technical information from his company on the next generation of nuclear submarines being constructed for the US Navy.
- An employee working for a large US manufacturing company decided to strike out and form his own company, but first stole all of the necessary technical information to manufacture competing high-technology products.
- A country that is an enemy (or "strategic competitor") to the United States sent a number of "illegals" into various companies to systematically report on all technical developments and strategies of the targeted US companies.
- A major hotel chain vice president decided that he was not being paid enough and took all of the records regarding the development of a new hotel concept to a competitor, where he got better pay and a substantial promotion.

These are many variations on the same theme: the theft of secret or proprietary information, usually for commercial purposes. The word "industrial" in "industrial espionage" has a specific reference to manufacturing companies, but in actuality, services industries (banking, hotels, R&D) are lucrative targets as well. Thus, the term "industrial" is an artifact.

Some industrial espionage is done by individuals out of greed, but other industrial espionage is done by organizations or even by governments. In most cases, there is a large financial component to industrial espionage, since at heart it is an operation involving business secrets and commercial gain. But there also are instances where industrial espionage is driven by the strategic competition (economic and military) between nation states.

There is an important distinction between classical and industrial espionage. Industrial espionage is a sub-set of espionage, but also has sui generis aspects; the term "espionage" refers to the taking of government secrets. Classical espionage would include stealing the US' negotiating position at the next Doha Trade round, or any information regarding troop movements, or the design of a stealth aircraft, or a sample of the surface paint or metallurgy of a stealth aircraft.

In the United States, the 1996 Economic Espionage Act divides industrial espionage into two classes:

1. Soviet spy in Tokyo before World War II, who warned Stalin of Operation Barbarosa, Hitler's intent to invade the USSR.
2. Former director of France's external intelligence service.

Table 1. Characteristics of Classical Espionage and Industrial Espionage[3]

	Classical Espionage		Industrial Espionage
	Government Information	*Private Sector Information*	
		Defense and Intelligence Contractors	Non-Government Business
Tangible	Equipment	Sample; Designs	Technology; Operations Manuals
Intangible (Intentions; Plans)	Negotiating Position (Trade talks; Arms control)	Plans; Software	Business Strategy (Pricing; negotiations; alliances; new products, R&D, etc.)

(1) industrial espionage committed against a corporation by anyone other than a foreign entity, and (2) industrial espionage committed by a foreign entity. The penalties are more severe for industrial espionage carried out by foreign entities. Unfortunately, there have been relatively few successful prosecutions under the 1996 Act.

Industrial espionage has a long history because, in a broader sense, it is part of the story of international technology diffusion.

American Industrial Espionage

In 1782, a young man named Samuel Slater was working in an English cotton mill. He memorized as much as he could about textile machinery, and then took his knowledge to the United States. At the time, England had strict laws against exporting such information.

Francis Cabot Lowell travelled to England in 1810, and learned enough so that, upon returning to the United States, he was able to set up a power loom that could turn raw cotton into finished cloth.[4]

The Soviet Union's Industrial Espionage

During the Stalin era (1922–1953), primarily prior to the World War II, the USSR operated a system of international industrial espionage targeting primarily Western Europe, but also the United States and Japan. Known as *rabochy korrespondenti* (рабочие корреспонденты, "people's correspondents"), these workers filed technical reports to Moscow. The program was expanded to include communist sympathizers working in factories throughout the West.

> *"Engineers and experts of Russian war industries back home were asking a host of technical questions. The lists of questions from Russia were turned over by military intelligence headquarters to the military attachés, who had them translated at the embassies."*

These were then rewritten and distributed to agents. p 34. For details on the worker correspondent movement.[5]

Unlike many types of espionage, these "correspondents" worked on a voluntary basis for ideological reasons. As the West opened up more to the Soviet Union, it became easier to conduct industrial espionage through organizations such as trade delegations. This type of state-supported system of international industrial espionage persisted until the fall of the Soviet Union. Industrial espionage for science and technology was operated under the KGB First Chief Directorate Directorate T. "Since 1970, Line X had obtained thousands of documents and sample products, in such quantity that it appeared that the Soviet military and civil sectors were in large measure running their research on that of the West, particularly the United States. Our science was supporting their national defense. Losses were in radar, computers, machine tools, and semiconductors. Line X had fulfilled two-thirds to three-fourths of its collection requirements – an impressive performance."[6]

Individuals become involved in industrial espionage for a variety of reasons:

- *Resentment*: General Motors employee Shanshan Du became dissatisfied with his employer and decided to start his own business using GM trade secrets. He teamed with Yu Qin to create a

3. Note that espionage against "Defense and Intelligence Contractors," can be classified as either industrial espionage or as a type of classical espionage. Historically, classical espionage targeted only governments, and corporate contractors to the government were not included since contractors are private enterprises. Any theft of their technology or trade secrets is certainly a type of industrial espionage. In reality, espionage against defense and intelligence contractors can be called either classical espionage or industrial espionage.

4. For the astounding growth of United States manufacturing during this period, see Engerman & Sokoloff, "Technology and Industrialization, 1790 – 1914" in *The Cambridge Economic History of the United States*, Vols. 1 & 2 (Cambridge: Cambridge University Press, 1996, 2000).

5. The work of the "people's correspondents" is detailed in David Dallin's book *Soviet Espionage* (New Haven: Yale University Press, 1955), 50-51.

6. Gus W. Weiss, "The Farewell Dossier," *Studies in Intelligence*, Washington, DC: Central Intelligence Agency, 39 (5), 1996.

company to manufacture advanced batteries for hybrid cars using GM proprietary information.[7]

- *Greed*: In France, to make extra money on the side, three executives were investigated for selling the economic model of the Renault car to foreign interests rumored to be from China.[8]
- *Seduction and blackmail:* Karl Heinrich Stohlze, working for the West German BND, seduced a senior secretary in a Boston defense company and sought to blackmail her into providing information on gene-splicing technology.[9]
- *Foreign spy:* Chi Mak (real name: Dazhi Mai) had planned to enter into a position of trust specifically for the purpose of stealing confidential information. He was a long-term illegal from China who stole information on the quiet electric drive propulsion system for the next generation of US Navy Virginia Class nuclear submarines. It was more than 20 years before he was activated to begin stealing secrets.[10]
- *Divided loyalty:* A variation on the above theme is someone who responds to an appeal to assist his native country. This is a common pitch to ethnic Chinese living in other countries. Dongfan Chung began to hand over massive amounts of space shuttle design and other aircraft secrets from Boeing to China out of a sense of duty to the homeland that had been carefully cultivated by his handlers.[11]
- *Fear:* The German technology company Bosch inserted a paid mole into its increasingly successful market competitor, the British firm Dyson, to steal its new technology secrets. The spy never identified himself as being affiliated with Bosch.[12]

More than 80 percent of industrial espionage involves individuals operating *within* the target organization – an insider.

In some companies, industrial espionage, which is illegal, has been closely related to accepted business functions such as "competitive intelligence," "market research," or "planning." Industrial espionage has been used in instances where the amount of information available through public sources ("open sources") is insufficient, and the situation was seen as crucial. For example, when General Motors learned that a competitor had purchased property to construct a very large factory, but did not know for what purpose, it set up a "spy center" to determine what its competitor was doing.[13] The urgent need for information can arise from a number of business scenarios. In a takeover, one company may wish to know the salaries of top executives so it can better negotiate the deal. Any time an innovative and disruptive technology is introduced, competitors scramble to learn as much as possible. Companies regularly collect all the information they can regarding the new product pipeline of their competitors.

Most companies caught conducting industrial espionage had outsourced these activities to "consultants" or similar companies for a variety of reasons. For example, the company may not have had the internal capabilities to perform the service that is required. It is less expensive to outsource than to invest in developing one's own talent in-house. Management of companies often do not understand what needs to be done so that, even if it had internal resources, they would not be effective; therefore, management needs outside advice. In some cases the company wished to isolate itself from the actual industrial espionage because if caught it would face a scandal or worse.

A variety of companies have been associated with industrial espionage, including international law firms; consulting firms; persons retired from a career in government intelligence and now "free-lancing" their skills in the private market; and service firms, which act as intermediaries between a "legitimate" service provider (consultants or law firms) and sub-contractors, which have fewer scruples. Much of the utility in using sub-contractors is to reduce the legal vulnerability of the company, which usually works. For example, KPMG Financial Advisory Services Ltd. in Bermuda was penetrated via a false-flag recruitment of one of its accountants, Guy Enright. Enright thought he was working for British intelligence, but actually was being used by an agent of a US law firm that the Alpha Group, a Russian conglomerate, had retained. Alpha Group set up a differently named subsidiary, which hired the US firm Barbour Griffith & Rogers. In turn, Barbour hired the Diligence Corporation, which sub-contracted the operation to a retired British spy, going by the name of Nick Hamilton, who went to Bermuda and recruited the KPMG employee. These

7. US v. Yu Qin and Shanshan Du, Opinion, United States Court of Appeals for Sixth Circuit, July 20, 2012.
8. Espionnage chez Renault – La piste chinoise privilégiée, Le *point.fr*, January 7, 2011.
9. Markus Wolf & Anne McElvoy. *Man Without a Face* (New York City: Times Books, 1997), 149.
10. U.S. v. Chi Mak et al., Second Superseding indictment, U.S. Dist. Court for Central Dist. of Calif., Grand Jury, October 2005.
11. U.S. v. Dongfan "Greg" Chung, Indictment, U.S. Dist. Court for Central Dist. of Calif., Grand Jury, October 2007.
12. Sean Poulter, Bosch "sent mole into British rival Dyson to steal details of its revolutionary digital motors," *MailOnline*, October 24, 2012.
13. John J. McGonagle & Carolyn M. Vella. *A New Archetype for Competitive Intelligence* (Westport: Quorum Books, 1996), 88-90.

layers of hiring were designed to create an impenetrable barrier to hide Alpha's identity.[14]

The countries responsible for most industrial espionage against the United States have shifted over the years. The current "winner" (as of mid-2014) is the People's Republic of China (PRC). Other countries frequently mentioned include Israel, France, and Russia. Since it is difficult to account for most industrial espionage, knowing who is most responsible is problematical. Both allies and "enemies" (or to use a more polite term, "strategic competitors") appear equally responsible for industrial espionage. Intelligence on industrial espionage by US allies, such as Israel and France, to the extent it is known to the government, remains highly classified for fear of political backlash if discussed in public.

Industrial espionage reduces R&D costs for the entity that is able to exploit the stolen information. By stealing information, the recipient does not have to spend the resources or the time on R&D. In many cases, it would not be possible to discover how an innovation operates without industrial espionage. For example, the PRC stole all the relevant design information for various thermonuclear weapons from Los Alamos National Laboratory. These weapons were developed at substantial US cost. A Japanese mainframe computer company stole the design information and a sample for an IBM mainframe central processing unit (CPU) cluster, thus both saving time in R&D, but also learning crucial secrets about how the module operated.[15]

Another advantage of stealing information is that the recipient is able to produce the product much faster. It is estimated that the PRC created world-class supercomputers in approximately one-fifth of the time it should have taken if all of the R&D had been "home grown."[16] Similar stories apply across almost the entire Chinese defense sector. In a domestic case, when Hilton Hotels received the entire blueprint for Starwood's new line of boutique hotels, it saved years of work, and millions of dollars of consulting and market research costs to compete with its own.[17] This case eventually was settled out of court with Hilton making a $75 million cash payment to Starwood.

The broader effect of industrial espionage is to change the strategic balance of nations[18] and the *causal pattern is easy to recognize*: the theft of industrial secrets leads to the competitive weakening of companies. In turn, this leads to the competitive weakening of sectors and the reduction in economic value for the economy as a whole. This can reduce the resources available to exercise national power, such as military capabilities. The end result is a shift in power away from the weakened nation state.

The US' post-World War II dominance was so advantageous that the possibility of it slipping away has been inconceivable to many. Yet the US' continued technological dominance is a dangerous illusion. A shift in the "technology balance of power" can occur rapidly. Industrial espionage has substantially weakened the United States to the point that the US' *relative* economic dominance has declined drastically. While much of this decline in economic power has been due to the export from the United States of technologies that were a source of competitive advantage, industrial espionage accounts for an important part of the US' *relative* technology decline.

Readings for Instructors

Amaral, John. "Maximizing compliance and content protection," *Information Systems Security*, 2007. *http://www.infosectoday.com/Articles/Content_Protection.htm.*

Dallin, David J. *Soviet Espionage* (New Haven: Yale University Press, 1955).

Engerman, Stanley L. and Robert E. Gallman (eds.), *The Cambridge Economic History of the United States*, *Volume II*, chapter on "Technology and Industrialization, 1790–1914," (Cambridge: Cambridge University Press, 2000), 367-402.

Fenwick & West LLP, *Trade Secrets Protection: A Primer and Desk Reference for Managers and In House Counsel*, miscellaneous paper, (San Francisco, Fenwick & West LLP, 2001).

Roche, Edward M. *Corporate Spy: Industrial Espionage and Counterintelligence in the Multinational Enterprise* (New York: Barraclough Ltd., 2009).

Roche, Edward M. *Snake Fish: The Chi Mak Spy Ring* (New York: Barraclough Ltd., 2009).

Tellis, Ashley J., Janice Bially, Christopher Layne, and Melissa McPherson. *Measuring National Power in the Postindustrial Age*, Number MR – 1110-A in Monograph Reports, (Santa Monica, CA: RAND Corporation, 2000).

Weiss, Gus W. "The Farewell Dossier," *Studies in Intelligence* 39 (5), 1996.

14. Eamon Javers, "Spies, Lies & KPMG," *Bloomberg Businessweek Magazine*, February 25, 2007. More details of the dispute are found in IPOC International Growth Fund, Ltd. v. Leonid Rozhetskin, et al., Am. Compl., 06 Civ. 4338 (JVM) (S.D.N.Y. Feb. 7, 2007).

15. See Congressional Record, "The Japanese Conspiracy," House of Representatives, July 12, 1989, H3666.

16. Commission on the Theft of American Intellectual Property, *The IP Commission Report*, (Seattle: National Bureau of Asian Research, 2013)

17. See Starwood v. Hilton, 09-03862, U.S. District Court, Southern District of New York (White Plains).

18. For a discussion of the components of national power see Ashley J. Tellis, Janice Bially, Christopher Layne, and Melissa McPherson. *Measuring National Power in the Postindustrial Age.* Number MR – 1110-A in Monograph Reports. RAND Corporation, Santa Monica, California, 2000.

Edward M. Roche was educated at The Johns Hopkins School of Advanced International Studies in Washington, DC, Concord Law School, and Columbia University in New York City. In his overseas work, he has organized and run research projects on national technology policies for microelectronics, information technology, and telecommunications in Brazil, Japan, Korea, Russia, China, and Europe. He is the author of *Corporate Spy: Industrial Espionage and Counterintelligence in the Multinational Enterprise*, and *Snake Fish: The Chi Mak Spy Ring*. He teaches business intelligence, international law, and technology intelligence at the Grenoble École de Management, Grenoble, France.

"This bodes some strange eruption
to our state…
If thou art privy to thy country's fate,
which, happily, foreknowing may avoid,
O speak!"

— Soldier, said to the ghost of the late King of Denmark, in William Shakespeare's *Hamlet* (1601), Act I, scene 1.

"Say from whence
You owe this strange intelligence."

— Macbeth, after hearing the witches' prophecy that he would be king, in William Shakespeare's *Macbeth* (1606), Act I, scene 2.

"It is pardonable to be defeated,
but never to be surprised."

— Variously attributed to Frederick the Great, Napoleon, the U.S. Cavalry, and others.

"Often do the spirits
Of great events stride on before the events, And in today
already walks tomorrow."

— Samuel Taylor Coleridge, *Wallenstein* (1800).