Guide to the Study of Intelligence
Industrial Espionage

Edward M. Roche, Ph.D., J.D.

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”.

Comments Alexandre de Marenches²

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

• The head of R&D for an adhesives company, a naturalized U.S. 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 information on government contracts and gave parties in the Middle East technical information that allowed companies there to develop new products ahead of the companies from which the original technical information was stolen in the United States.

• 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 U.S. Navy.

• An employee working for a large U.S. 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 in order systematically report on all technical developments and strategies of the targeted U.S. companies.

• A vice president of a major hotel chain decided that he was not being paid enough money 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.

There 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)

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.
are lucrative targets as well. So 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 espionage 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 negotiating position of the United States 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) 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.

| Table 1. Characteristics of Classical Espionage and Industrial Espionage³ |
| --- | --- | --- |
| **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.) |

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

*American industrial espionage*

Samuel Slater in 1782 was working in a cotton mill in England whereupon at age 21 he memorized as much as he could about textile machinery, 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 the United States

---

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.
he was able to set up a power loom that could turn raw cotton into finished cloth.

Soviet Union’s industrial espionage

During the Stalin era (1922–1953), primarily prior to the Second World War, 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. 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.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 trade secrets from GM. He teamed with Yu Qin to create a 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) was an individual who had planned from the very beginning to enter into a position of trust specifically for the purpose of stealing confidential information. He was a long-term illegal for China who stole information on the quiet electric drive propulsion system for the next generation of U.S. Navy Virginia Class nuclear submarines. It was more than twenty years before he was activated to begin to steal secrets.10


5 The work of the “people’s correspondents” is detailed in David Dallin’s book Soviet Espionage, New Haven: Yale University Press, first edition, 1955. “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, see pp 50-1.

6 Industrial espionage for science and technology was operated under Directorate T of the KGB’s First Chief Directorate. “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.” See Gus W. Weiss, “The Farewell Dossier,” Studies in Intelligence, Washington, DC: Central Intelligence Agency, 39(5), 1996.


• **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.\(^\text{11}\)

• **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.\(^\text{12}\)

More than 80% 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.\(^\text{13}\) 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 industrial espionage, including international law firms; consulting firms; persons retired from a career in government intelligence and now “freelancing” 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 less scruples. Much of the utility in using sub-contractors is to reduce the legal vulnerability of the company, which usually works. For example, the KPMG Financial Advisory Services Ltd. in Bermuda was penetrated via a false-flag recruitment of one of its accountants. The accountant, Guy Enright, thought he was working for British intelligence, but actually was being used by an agent of a U.S. law firm that had been retained by the Alpha Group, a Russian conglomerate. Alpha Group set up a differently named subsidiarity, which hired the U.S. firm Barbour Griffith & Rogers.

---


\(^\text{12}\) See Sean Poulter, Bosch "sent mole into British rival Dyson to steal details of its revolutionary digital motors", MailOnline, October 24, 2012.

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 layers of hiring were designed to create an impenetrable barrier to hide the identity of Alpha.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. 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 allies of the United States, 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 People’s Republic of China stole all the relevant design information for various thermonuclear weapons from Los Alamos National Laboratory. These weapons were developed at substantial cost to the United States. A Japanese mainframe computer company stole the design information and a sample for an IBM mainframe 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 People’s Republic of China 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 defense sector in China. 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

The broader effect of industrial espionage is to change the strategic balance of nations18 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 post World War II dominance of the United States was so advantageous, that the possibility of it slipping away has been inconceivable to many. Yet, the continued technology dominance of the United States is a dangerous illusion. A shift in the “technology balance of power” can occur rapidly. The United States has been substantially weakened by industrial espionage to the point

17 See Starwood v. Hilton, 09-03862, U.S. District Court, Southern District of New York (White Plains). This case eventually was settled out of court with Hilton making a $75 million cash payment to Starwood.
that the relative economic dominance of the United States 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 relative technology decline of the United States.

Readings for Instructors

Author
Edward M. Roche was educated at The Johns Hopkins School of Advanced International Studies in Washington, D.C., Concord Law School, and Columbia University in the City of New York. 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.