Industrial Intelligence and Espionage

The proliferation of books dealing, like the half dozen listed below as references, with industrial intelligence and espionage activities may, as many authors claim, reflect a real increase in efforts by adversary governments and business competitors to ferret out the private industrial secrets of the United States and other leading Western nations. In a field in which there are obviously no reliable statistics, since neither professional spies nor legitimate private intelligence organizations need to report their operations to national authorities, the available guideposts do indeed point to the likelihood of an increase in such activities.

What makes industrial espionage profitable is gaining knowledge of some industrial process or technique without incurring the R&D expenditures which would otherwise be necessary to master it via the laboratory. It is a method of closing the technological gap "on the cheap." One can conclude that since research and development is a rapidly growing component of gross national product, not only in the United States but in the industrial West generally, the resulting technological innovations provide a multiplication of targets for industrial espionage. That neither governments nor private firms have been able to resist the temptation is reflected in the number of publicized cases of espionage in those industries devoting the highest relative effort to research and development—aero-space and associated weaponry, chemical (including drug), and electronics, all of which generate an unusual amount of proprietary information.

The efforts of Communist governments, particularly the Soviet Union, in this field have been well publicized. In 1964 they were summarized in the Harvard Business Review by J. Edgar Hoover in an article entitled, "U.S. Businessman Faces the Soviet Spy." Mr. Hoover's analysis concluded that the Soviet Bloc nations were carrying out a massive systematic and purposive attempt through their intelligence services to obtain information about American industry. While the activities of their clandestine agents, particularly in connection with the nuclear energy industry, are much publicized, Mr. Hoover estimated that 95% of the information which Moscow needs is obtained openly and legally.
Recent Books: Industrial

Since intelligence officers are relatively familiar with Soviet espionage, for us the more novel and interesting aspects of the industrial intelligence literature are those on the activities of private firms and individuals. Several of the authors listed make a distinction between business or industrial intelligence on the one hand and industrial espionage on the other. Any business firm needs reasonably adequate information on the sales activities of its rivals and on potential customers in order to survive. Business intelligence units are therefore frequently organized in marketing departments. An appendix to the November-December 1959 Harvard Business Review based on a survey of over 1,500 companies found that 85 percent had an organized system for reporting on their competitors, and 35 percent had a formally designated department of competitive information.

Richard Greene's Business Intelligence and Espionage devotes most of its text to the nuts and bolts of organizing and operating a business intelligence unit designed to help guide policy decisions by supplying, on a systematic basis, analyzed information secured in an aboveboard manner. It devotes chapters specifically to data sources and their evaluation, to automatic information storage and retrieval systems, and to methods of using overt business intelligence in various decision situations; it deals only briefly with private investigators and electronic eavesdropping. The book consists of a series of articles by West Coast management consultants and is based almost entirely on their experience in the aero-space industry. It could well have been titled How to Get and Use the Facts Needed to Bid on Government Aero-Space Contracts.

The reader of such works would find the goals and, in large part, the methods of industrial intelligence to be similar to those of military intelligence. But when he turns to privately initiated covert operations, or industrial espionage, there are apparent differences between these and national spying activities. There is first of all the question of the level of ethics which a society will demand of its industrial leaders. Not all industrial espionage, to be sure, seems devious enough to bring public condemnation if exposed. For example, it is well known that automobile manufacturers use long-range cameras and electronic devices to gain knowledge of their competitors' new models in as early a stage of development as possible, and these activities are not condemned by an indignant public.

But when General Motors, through the services of ex-FBI agent Vincent Gillen, probed too closely into author Ralph Nader's private life, it was a different story. General Motors President James Roche
himself went to Washington and, before an audience of Senators asking pointedly embarrassing questions, apologized to the author of *Unsafe At Any Speed*. Strangely enough, none of the authors here discussed seems to have been interested in the key question of the ethical limits imposed on corporate espionage by society through the threat of public revulsion which would damage the company's earning power.

Peter Hamilton, in his straightforward *Espionage and Subversion in an Industrial Society*, includes a chapter on "The English Way of Industrial Espionage," which he concludes to be limited because of the high level of British ethics. Not that English managing directors have no thirst for non-public information about their business rivals; they have other ways of procuring it, including the "old boy" network. Indeed, there are cases on record of drug firms, when offered secret formulae by disgruntled employees of their competitors, not only turning down the offers but cooperating in prosecution of the culprits.

Business ethics are not uniformly high, however, as the famous American Cyanamid case showed. This was the instance when Italian pharmaceutical firms took the initiative in obtaining antibiotic cultures and procedural information clandestinely from a U.S. producer, gaining access through a disaffected employee of Cyanamid. This case is discussed in varying detail by Payne and Engberg as well as Hamilton and is mentioned by Wade. The Hamilton volume contains a number of detailed appendices, including one on "Graphology as an Aid to Personnel Selection." The author believes that handwriting is a useful discriminant.

A review of the sources used for these works reveals that most of the authors relied heavily for their information on materials published in court decisions, in journal articles, and in the press. Wade is an exception; he is a practicing patent attorney. His *Industrial Espionage and Mis-Use of Trade Secrets* reflects this background, having chapters on the legal remedies to which a company may resort in industrial espionage cases and extensive coverage of patent protection, requirements of the Department of Defense for plant industrial security, etc. Wade's intended audience is the company manager, for whom the book is designed to give a good deal of practical advice and to serve as a ready reference. It contains an extensive bibliography, largely legal case citations but also references to the press and periodical literature.
Recent Books: Industrial

At the opposite end of the spectrum is Payne's Private Spies, a chatty collection of potpourri which covers the subject of industrial espionage from 300 AD (the Chinese silk case) up to the latest press reporting on cases in the United States and United Kingdom. Payne obviously has the famous "general reader" in mind; his book contains lots of familiar but colorful material on oil intrigues in the Middle East, Zaharoff's machinations on behalf of Vickers munition sales, and Japanese and Soviet industrial espionage. Payne's work is definitely not a "how to cope with" volume. But if you have never heard of Ulmont Cumming, who for 40 years was the acknowledged number one industrial spy in the United States and employed by many respectable firms, his story plus the other yarns that Payne spins will make a pleasant evening's reading.

At the bottom of the readability scale stands the brief (100 pages) The Scope and Limitation of Industrial Security by Knight and Richardson. They describe their purpose as seeking "to acquaint the reader with an overall theory of the industrial security function, and to indicate its scope and limitations as an integral aspect of the contemporary economic scene." Apparently aimed at college students studying industrial security, the book displays the same dull, ritualistic formalism that one associates with many "how to" courses in teachers' colleges. What Knight and Richardson do—without developing the promised overall theory, unless the entire 100 pages are intended to be that—is to outline their topic under a variety of functional headings. The resultant chapters are so short that little emerges except a skeleton of fundamental points arranged according to the authors' preferences. The brief bibliography is confined largely to U.S. Government manuals on plant protection and security. Reading is not recommended.

The subtitle of Engberg's volume on The Spy in the Corporate Structure is And the Right to Privacy. This is a tipoff to the broad sweep of subject matter that he covers and to the fact that many of his essays have nothing to do with industrial espionage and many of the spies he talks about are outside of the corporate structure. For example, his several chapters on individual privacy end up discussing the proposed National Data Center (a scheme, on which the Gallagher Committee held hearings in 1966, to combine all the Federal Government's files on each citizen in a central place as an aid to operations research and planning) and advocating that access to the data on an individual, except by the individual himself, be granted by court...
Engberg also believes that the American Telephone and Telegraph Company should be held liable for the integrity of its circuits.

Engberg titillates the reader with a series of pieces about restrictions imposed on the passing of trade information by the guild system of the Middle Ages until the breakup of that system with the industrial revolution, recounts Samuel Slater's famous purloining of the secrets of Arkwright's textile machinery, and winds up with a recap of some of the present-day industrial espionage cases, including those involving Cyanamid, Merck, and SKF. Indeed, he ranges widely over things that obviously interest him, whether or not they shed light on the theme implied by his title. In short, this is another "general reader" volume, designed to inform, to entertain, to philosophize and propagandize the author's ideas. It is not a comprehensive nuts-and-bolts book that would give the intelligence professional or plant manager a grasp of industrial espionage.

REFERENCES

Greene, Richard M., Business Intelligence and Espionage, Homewood (Dow-Jones Irwin) 1958
Hamilton, Peter, Espionage and Subversion in an Industrial Society, London (Hutchinson) 1967
Wade, W., Industrial Espionage and Mis-Use of Trade Secrets, Ardmore (Advance House) 1964