

October 15, 2008

---

## Espionage, Spies, and Industrial Espionage: The Evolving Challenge

*Espionage, the covert gathering of information, is a sinister and dangerous business that has been the subject of fascinated speculation through the ages. Intelligence, its organized form, is one of the oldest professions, with a history from the Biblical Rahab, who operated a safe house in Jericho four thousand years ago, to the ineffective Mata Hari, executed during the First World War, to the very recent and interesting admissions during September 2008 by Morton Sobel and John Le Carré. Morton Sobel, a controversial figure in the post-war period, admitted in a recent interview that he had been a Soviet spy while Le Carré, the well-known author of Cold War espionage thrillers, revealed he was a British intelligence officer assigned abroad during the early years of the Cold War. The heterogeneous cast of men and women — heroic, bizarre, gifted, mercenary, and psychopathic — who have achieved fame or notoriety as spies continue to provide intelligence. The principles and motives of espionage remain unchanged. However, the technology has progressed from intelligence reports written in cuneiform script on clay tablets to the microdots and burst transmissions of the early twentieth century to the encrypted e-mails and spy satellites of today.*

Despite the risks and betrayals and despite a rate of remuneration usually far below the levels of hazards involved, there has seldom been a shortage of spies. Many have been the victims of blackmail of one sort or another, coerced and reluctant and therefore neither suitable nor reliable. Some have been motivated by jealousy or a desire for revenge. Others have been strictly mercenary — and if a spy will take money from one side there is usually little to prevent him or her from taking money from the other as well. The incentives for some have been purely patriotic or ideological, without self-interest or any sort of payment and these are by far the most difficult to detect or catch, as with the spies who were recruited in universities and colleges. Others have become spies either because they are stimulated by danger or because they have a completely erroneous idea of what it is all about.

Intelligence is fundamentally a service required by those who have to make decisions and, because there is nearly always some difficulty in acquiring others' secrets, doubt is an unavoidable element of any intelligence report. The report of a spy may be full of apparently concrete facts, but it is possible he or she may be mistaken or may have been deceived. The question is begged, is the spy entirely reliable? It is a curious fact that often accurate

information of vital importance is rejected or ignored simply because spies are seldom trusted, and also because so many rulers, commanders and business executives are convinced that their own opinion is more reliable than that of a spy — particularly if the spy's information conflicts with their own preconceived ideas. Spies, spymasters and intelligence staffs have frequently discovered that it is one thing to obtain absolutely correct and reliable information, and quite another to persuade people to believe it.

If spies had been trusted, the Russian armies would not have been taken by surprise when the Germans invaded in 1941, and there might have been no American disaster at Pearl Harbor later that same year.

The question of trust and the element of doubt have always been, and no doubt always will be, basic problems. They are also the reasons why intelligence must remain a service and never have executive powers. The executive, whether he or she is a government official, military commander in the field, or on the board of directors of a company or organization, must decide what information is wanted so that a course of action can be determined. This requirement is passed to the intelligence service or security department, which may consist of secret agents, staff officers or a market research team; and this group does its best to answer the questions asked. Since any forecast, particularly of an opponent or competitors' intentions, can be wrong, this intelligence-developing group must always differentiate between the facts and the deductions it makes from them. Realistically, in light of the trust factor, it can and should only give advice, pointing out the possible consequences of alternative courses. The final decision must be taken by the executive and not dictated by its intelligence service. Executive decision-makers must clearly have a background in, or be counseled on, how to separate fact from fiction when intelligence is part of the equation.

As mentioned earlier, espionage is one of the oldest professions and has a rich history from antiquity to the present day. However, for our purposes the recent history of espionage will vividly portray the positive and the negative lessons of this phenomenon and how the techniques apply today to corporate espionage. Having won the "War to End All Wars," the British, French and Americans demobilized their forces and reduced their

(continued on next page)

---

---

## Espionage, Spies, and Industrial Espionage: The Evolving Challenge

(continued from preceding page)

intelligence services to the minimum, leaving the field open to the Russians, the Japanese and in due course, the Germans. The British felt that intelligence was not “playing the game,” while the attitude of many Americans was summed up by the remark made by Secretary of State Henry L. Stimson in 1929, that “gentlemen do not read each other’s mail.” A more recent example is the lack of attention paid to al-Qaeda activities prior to its attacks of America on September 11, 2001.

### World War II

During this period Russia was laying the foundation of what, in wartime, was to become the famous Rote Kapelle, or Red Orchestra — the name given by German intelligence to the Soviet spy rings active in Europe who were recruiting agents that would send a flood of information from Vienna, Brussels, Berlin, Paris, Oslo, Madrid, Switzerland and even London. Headed by Leopold Trepper of Poland, the Rote Kapelle became a nightmare to Admiral Canaris and Reichsführer Heinrich Himmler, the heads of the two main German intelligence services. Among Trepper’s agents was Rudolph Roessler, who lived in Lucerne, Switzerland and had the code name “Lucy.” He was in contact with members of Hitler’s staff who passed him details of practically every undertaking planned by the German High Command — including the date, time, place, and strength of the German invasion of Russia in 1941. Another Soviet spy was the brilliant journalist Richard Sorge who was completely accepted and trusted by the German Embassy in Japan and ran a spy ring that penetrated the Japanese War Cabinet. He gave Stalin — as did the Rote Kapelle — details of the German invasion plans in 1941, only to be ignored.

### The American Experience

America had been slow to develop its intelligence resources. The United States secret service, established in 1865, had nothing to do with espionage; its function was to suppress forgery and counterfeiting. It moved into the world of counterespionage during the Spanish American War of 1898, and following the 1901 assassination of President William McKinley, took on the responsibility for the personal safety of the President and his family.

In 1908, the forerunner of the Federal Bureau of Investigation (FBI) came into being as an investigating agency with federal powers under the Justice Department. During World War I, the FBI added counterespionage and National Security to its responsibilities; however by

the time Pearl Harbor was attacked there was still no central intelligence organization. Although the FBI began to monitor the activities of the German, Italian and Japanese representatives in the Americas, there were as of yet no organized efforts to develop and process intelligence to be forwarded to the executive branch. To fill this gap, General William J. Donovan founded the Office of Strategic Services (OSS) shortly after the Pearl Harbor attack in December 1941 to collect information and intelligence. As early as 1944, General Donovan recommended the creation of a central intelligence agency with dual functions. The Central Intelligence Agency (CIA) came into existence with the National Security Act of 1947 and rapidly became an effective counter to Russian intelligence during the Cold War.

During this period, the Soviet Union had built up an enormous and ruthless apparatus answering only to Stalin, a growth that continued during the Cold War. By 1969, Yuri Andropov controlled an army of approximately 500,000 and had at his disposal an incalculable number of spies and informants all over the world. The KGB and its counterpart, the GRU, or Soviet Military Intelligence, operated a vast network of espionage, largely through Soviet embassies and official establishments throughout the world. The CIA and FBI, in cooperation with friendly intelligence and investigative services, countered the activities of the Russian services around the globe. Consequently, the history chronicling these events involving heroes, tyrants and scoundrels has become the lore of the intelligence confrontations of the Cold War. The majority of these secret battles were fought on the streets and in back alleys of Moscow, Vienna, London, Paris, New York, Washington, D.C. and other cities, but there were also intelligence activities taking place in Asia, Africa and Latin America. Everywhere Soviet operators surfaced, it was necessary to counter their activities to prevent the further proselytizing of communism. The Cold War was fought almost exclusively with intelligence services, and was undeniably responsible for the birth and rapid growth of huge intelligence agencies on both sides of the Iron Curtain.

### Recruitments and Defectors

All espionage systems, no matter how carefully controlled and directed, share a common, fundamental weakness — their security is largely dependent on the loyalties of the individuals who work for them. They are therefore at the mercy of defectors and recruitments-in-

---

place. Double — and triple — agents and high-level spies did incalculable harm to the free-world intelligence community. On the American side most were pathetic alcoholics in financial difficulty while on the Soviet side many cooperated for money, but there were also many who defected or cooperated for altruistic and ideological reasons. The last American spies who helped the Russians for ideological reasons were probably the Rosenbergs, who shared classified information regarding the atomic bomb with Soviet agents in New York and were arrested in 1948. Although Russia is again beginning to assert itself in worrisome fashion, the resources of Western intelligence services were directed elsewhere after the fall of the Berlin Wall and the devolution of the Soviet Union. Currently, terrorism, state sponsors of terrorism and nuclear proliferation are the primary targets of America's intelligence resources.

### **Industrial Espionage**

While nations have a need for intelligence and counterintelligence services, the private sector must also be alert for instances of industrial espionage, sabotage and the security of its intellectual property. Though industrial or corporate espionage is conducted for commercial purposes, it can certainly impact national security. The term "industrial espionage" is distinct from what is called "competitive intelligence" — legal and ethical activities such as examining corporate publications, websites and patent filings to determine the activities of a corporation. In contrast, industrial espionage describes activities such as theft of trade secrets, bribery, blackmail and technological surveillance. Industrial espionage is most commonly associated with technology industries, aerodynamic and satellite companies and the computer industry. Pharmaceutical and heavy industries, particularly the automobile sector, are also targeted; one example involves the secrecy of vehicle testing. Sweden recently proposed a law to protect cold weather vehicle testing in their frigid northern regions. The world's leading auto manufacturers head there every year to see how they can improve vehicles' cold weather performance. Vehicle testing also attracts the prying eyes of those wishing to get a look at the competition or uncover trade secrets utilizing sophisticated spying equipment. Prudence would dictate that effective countermeasures be implemented to prevent the leakage of advanced technologies.

Espionage takes place in many forms and even purportedly friendly foreign intelligence services have been known to assist their homeland industries by

conducting espionage. Keeping this in mind, it is safe to say that foreign counterintelligence services will be carefully examining the business visa applications of American companies. Moreover, surveillance activities on expatriate employees connected to targeted industries will continue. These services will attempt to recruit expatriate and local employees. This surveillance of American businesses may apply not only to corporate offices but to employees' residences. Company executives and other employees may be physically surveilled and their residences subjected to technical surveillance, such as wiretaps and bugs, as well as mail and garbage covers. Domestic workers may also be recruited in an effort to collect information on employees. One cannot escape noticing the number of experienced former intelligence officers from various countries who are working in the security departments of foreign competitors. In addition to the more traditional practices of using electronic surveillance and "black bag jobs" (illegal searches and seizures) on offices and executive apartments abroad, it is not uncommon for recruited agents to infiltrate a competitor to collect proprietary information and identify vulnerabilities that can be used to compromise employees through blackmail. Under these conditions, countersurveillance sweeps are not always effective because the adversary is operating on his home turf.

Corporate espionage is a threat to any business whose livelihood depends on information. The information competitors seek may be client lists, supplier agreements, personnel records, research documents or prototype plans for new products or services. The Economic Espionage Act of 1996 was approved by Congress because the theft of U.S. trade secrets was costing U.S. companies billions of dollars a year in lost sales and costing U.S. workers their jobs. Foreign intelligence services and corporations are with increasing frequency using classical espionage techniques to steal U.S. corporate marketing information, technological advances and proprietary data in support of their national goals. Since the enactment of the Economic Espionage act in 1996, indictments, arrests and convictions have occurred not only in high technology and electrical industries, but also for the theft of products and ideas as diverse as pharmaceutical plant cell cultures, razor blade design, consumer film and self-adhesive technology.

It is clear that in view of the increased activity in the area of industrial espionage, all technology is worth protecting

**(continued on next page)**

---

---

## Espionage, Spies, and Industrial Espionage: The Evolving Challenge

(continued from preceding page)

because of the potential value involved. All entrepreneurs must constantly be on the alert for espionage attempts and intelligence gathering on the part of foreign competitors and intelligence services that are so sophisticated that the victim often has no inkling as to what has occurred until the costly consequences reveal themselves. When the adversary is a foreign intelligence service assisting homeland industries, this presents a unique problem. Intelligence education programs should be instituted to alert various levels of management to this special situation when communicating; technological eavesdropping is almost impossible to prevent when operating abroad. Encryption must be utilized in electronic communications and telephone conversations must be handled with knowledge of the sensitivity involved and the likelihood of eavesdropping. Employee alertness is paramount in light of the fact that unethical and ruthless competitors have in the past authorized all the tools of the intelligence tradecraft to gain illegal access to sensitive information to harm honest and unsuspecting entrepreneurs and their companies.

With all the recent attention paid to hacking, identity theft and computer-related security, it is easy to forget the key role staff plays in corporate security. One of the first steps an organization should take is to ensure that all levels of management receive education on the security implications of the decisions they make each day. This should minimize security breaches brought about by carelessness, such as holding sensitive conversations in public places or over unsecured telephones and sending unencrypted sensitive information by computer. Despite the mounting sophistication of those dedicated to committing industrial espionage, most security leaks are not caused by technology but by insufficiently trained employees violating the most simple security precautions. Firewalls, passwords and high-tech systems are all crucial safeguards, but they cannot stop someone from leaving their laptop unattended, forgetting their documents on a train or lending their access card to a part-time employee who is not properly vetted. The staff must be asked to protect business information as if it is their own personal secret and a culture must be developed that encourages employees to take security personally.

Although most security breaches are inadvertent, others are intentional. There is no hard-and-fast rule for identifying who within an organization might start to

siphon off cash or sell secrets to a competitor. It could be a seemingly trustworthy, long-term employee who finds himself under new financial pressure — a growing risk in today's financial climate — or a new member of staff employed without a thorough background check, who joined with the sole intention of stealing information for a competitor, or infiltrating the company or organization for the purpose of causing harm. Such corporate espionage may sound far-fetched but it is very real. A more common variant is the account manager taking client lists with them when they leave, a scenario that is still considered industrial espionage and is breaking the law. Organizations can improve their security programs by encouraging the staff to offer suggestions on how to improve security and by conducting a wide range of security training and awareness programs.

### A Second Cold War?

*During this period of economic dislocation and stress and with an impending resurgence of Russian assertiveness, never were the aforementioned concerns more germane. In the past, the Russians were very pragmatic. They did not see the need to spend money to develop a technology from scratch when they could steal or buy it for a fraction of the cost and effort. So far, there is no indication the Russians are reinstating this aggressive posture. However, as the price of a barrel of oil drops, the economic situation worsens and tensions increase over geopolitical issues, the newly strengthened Russian intelligence services may return to their old habits. And corporate America, in the face of a shaky economy, deserves to preserve the rewards of its hard work and not be saddled with the added challenge of valuable information siphoned off by foreign competitors. The time for urgency is now®.*



The Lipman Report Editors