Industrial Espionage Today and Information Wars of Tomorrow

Paul M. Joyal
President

To be presented at the

19th National Information Systems Security Conference

Baltimore Convention Center Baltimore, MD October 22-25,1996

INTEGER Security Inc.
Information and Analytic Services

725 15th Street, NW, Suite 908 Washington, DC 20005 Tel: (202) 347-2624, Fax (202) 347-4631

Industrial Espionage Today and Information Wars of Tomorrow.

October 22-25, 1996 Baltimore, Maryland

Paul M. Joyal
President
INTEGER Security Inc.
Information and Analytic Services
725 15th Street, NW, Suite 908
Washington, DC 20005
Tel: (202) 347-2624, Fax (202) 347-4631

<u>ABSTRACT</u>

In this report we review case histories of industrial espionage publicized in the media and in Congressional hearings. The threat to the United States as the world's largest investor in R&D is magnified by the transition from a cold war military confrontation of the super powers to economic competition in global markets. To sustain their market share, France, Japan and Russia have initiated national programs to acquire U.S. technical know-how. Former intelligence staff now distill fragments of sensitive information into meaningful intelligence to guide industrial and national efforts towards dominance. This threat is amplified by the exponential proliferation of global communication networks, like the INTERNET, that reach into corporate America and permit unseen adversaries to probe the vast U.S. data stores for unprotected intelligence. Counter intelligence in industrial espionage by the United States on a national level is virtually impossible because of public scrutiny in our open society.

On the positive side, the upheaval of a rapid transition from the global political <u>high</u>-tension and high stability of the Cold War to the <u>low</u>-tension and high instability of the so-called new world order has prompted increased international collaboration against international terrorism and organized crime. On the corporate level, strategic alliances with foreign firms are expanding in order to sustain competitiveness and innovation in areas of specialty. A national security plan to protect the U.S. information resources is needed; and a viable policy to enable our information highways to operate as safe conduits for electronic business. The well being of our nation or that of the global economy, should not be left to chance and provocation.

<u>KEYWORDS</u>: Industrial espionage, economic espionage, case histories, terrorist attack, disaster prevention, corporate alliances, national collaboration, information warfare.

1. INTRODUCTION

National Competition in Global Markets is well illustrated by the following example: In June, 1990, US intelligence officials learned that Indonesia was about to award a contract for roughly \$100 million to the Japanese electronics firm NEC to modernize its creaky telephone system. Authorities familiar with the specifics say that AT&T's subsidiary in Europe had a more competitive bid and that Tokyo used its \$2.1 billion in foreign aid to Jakarta to sway the decision in NEC's favor. It took the intervention of President Bush in a letter to President Suharto, to have the bid split between the two firms. As David Boren, then Chairman of the Senate Intelligence Committee remarked, "The world has changed ... We have to change with the world.¹

Moreover, one of the reasons that McDonnell Douglas has considered entering into a foreign ownership arrangement with the Taiwanese is that it is becoming increasing more difficult for McDonnell Douglas to compete against the likes of the French *Airbus* passenger plane. The rise of *Airbus*'s share of the world market to 30% has largely come at the expense of McDonnell Douglas. Some company officials claim that if they can't get an industrial policy in the U.S. they must go to where they can get one. McDonnell Douglas recently lost a sale to Singapore Airlines when Airbus sweetened the offer with scarce landings rights at the two airports in Paris.² These are examples of how economic wars are presently being waged.

In his 1987 book **Real-World Intelligence: Organized Information for Executives**, Herbert E. Meyer contends that throughout the world of commerce and industry, "**intelligence**" is on its way to becoming a key management tool for the corporate executive.³ Meyer goes so far as to suggest that the emergence of *business intelligence systems* is the most striking and potentially significant business trend of our time. Here, intelligence becomes the means by which companies chart their future course and are alerted to the strides of their competitors. As economic competition intensifies, and as it redirects the activities of covert agents who were previously focused on military competition, the importance of acquiring information concerning economic plans and intentions will become more acute. Correspondingly, systems and methods for the protection of proprietary information will also be elevated in priority and importance.

Meyer reminds us that successful business enterprises have been collecting and using intelligence for centuries. Examples of the organized use of intelligence can be found as far back as the fourteenth century in the historical accounts of the *House of Fugger*. One of the first European international banks, the *House of Fugger* produced a "manuscript newsletter" for its key officers, what today might be described as a "competitive intelligence" newsletter. This newsletter contained succinct political insight and sensitive commercial information. What differentiates these efforts of the past with those of the present is the organized nature of the correlation of the material. In the past many elements of business intelligence have traditionally been carried out in only the largest and most successful of companies. Today the effort is to integrate that information and to disseminate its analysis and conclusions to those decision makers who are expected to use it as a managerial tool. "It is this new effort within the corporate community to acquire, organize, and coordinate the diverse elements of intelligence that is turning a group of related, but previously separate activities, into a new, and incredibly powerful business management tool." ⁵

Today the world is changing before our very eyes. Some old rivalries are fading while others are coming to the forefront. Today's friend may become tomorrow enemy and visa versa. This is especially true in the rapidly changing world of shifting political alliances and changing boundaries for economic competition. Secretary of Defense William Perry has warned: "We live in an age that is driven by information. Technological breakthroughs....are changing the face of war and how we prepare for war." What are we to do and who are we to guard ourselves against? The French government has been extremely focused on these questions in recent years. Findings of a recent investigative report are gradually becoming revealed.

2. THE FRENCH CONNECTION

Three years ago, in France, a high-level commission was very quietly formed under the office of the Prime Minister. The Commission was headed by Henri Marte, CEO of the French military aircraft manufacturer Aerospaciale. The task of the Commission was to study how a selected number of foreign countries integrate economic information obtained from various governmental and non governmental sources. Among the countries studied were: Japan, Sweden, Germany, the United States, and Great Britain. As the Commission investigated the systems which various countries have developed to integrate commercial, trade, intelligence and *company-proprietary* information with *open-source* information, they found France lacking. They concluded that France, while having many of the desired components, suffered from a lack of focus and failed to integrate the various activities and sources of information towards an effective national course of action.

The Commission for Security and Economic Competitiveness had thirteen official members, including prominent businessmen from defense companies such as Mr. Lagardere of Matra, as well as Professor Montagner at the Pasteur Institute. But the vision and forceful drive of the Commission flowed from its director Mr. Reme

Pautrat. The sixty-ish former head of the French internal security service, DST, Mr. Pautrat brought all the competence and enthusiasm he was known for in his former position; DST is the French internal security service, equivalent to the FBI in the United States. Some prominent members of the distinguished French business organization CNPF have expressed their general uneasiness concerning the efforts of its own government. They, perhaps more so than members of the former socialist government, have failed to accept the notion that economic problems or competitiveness can be anything more than marginally improved through government intervention and involvement. Some French businessmen have even openly expressed their skepticism for this government effort. Their concerns are that any government effort, coordinated through the office of the Prime Minister, will be counterproductive and lead to more suspicious attitudes against French companies in global markets. What distinguishes this planned approach from earlier activities in France is the attempt not only to aid the large French national and strategic companies in their global posture, but also to reach out to the small- and medium-size French companies on a regional basis to promote the export of their goods.

One of the concrete steps undertaken so far by the French government has been the establishment of a DECA-type education program by the DST in 1993. It reaches out to educate companies on the various threats they might face in industrial espionage and economic intelligence. They are also becoming more and more concerned about disinformation and covert action. Some suspect that Coca-Cola was behind the benzene scare that negatively effected the business of Perrier, due to the public reaction and concern about the purity of its widely-favored drinking water. No doubt, the French have many case studies and experiences to draw upon; some of these concern IBM, Texas Instruments, and Corning, as will be noted later. The fact that Mr. Pautrat's old organization is highly active, should come as no surprise. However, not to be left behind is the French *DGSE*: the equivalent of the United States' CIA. DGSE will continue the questionable covert and 'black bag' activities in their department known as 'Service Seven', which has been targeting American business since the 1960s. This has prompted visiting American government officials to tote there briefing books, papers and documents with them when traveling in Paris. One of President Clinton's economic aides commented that he was cautioned "...that this is France we are visiting. When it comes to economic espionage, no one does it better."

In another development of the Chirac government, the DST and DGSE intelligence services have established a liaison committee to work together rather than at cross purposes. This committee will attempt to coordinate information from the Economic and Commerce Departments of the French government. One old mission within the French Foreign Ministry's overseas diplomatic establishments was the "Post Economic Expansion" organization which attempted to help French private businessmen with investment opportunities around the world. When the Commission found that it was largely an ineffective expense for the Foreign Service, with little or no concrete, tangible achievements, the foreign service component was re-focused to feed information back into the new French national structure for information analysis. This activity, represented within the French Embassy in Washington, DC, recently forwarded to the French Finance Minister a 26-page report, dated September 11, 1995, titled The American System to Support Private Business. It describes all the various components of the American government which promote American business overseas, especially the Advocacy Center of the Department of Commerce (DOC). The report even contains a photograph of their "war room". It also reviews, in some detail, the September 1994 "Operation China," when Secretary Ron Brown visited China and the successful use of the CIA to dislodge the Thompson Company from a Brazilian contract on behalf of Raytheon. These initiatives have their roots in economic modeling of the United States by French entities on computers of U.S. firms under contract to the Bureau of Economic Analysis and Labor Statistics, with the latest econometric data.

The outcome of the French study about business in the United States was scheduled to be publicly acknowledged on October 31, 1995, in Essonne, France. There, the first regional national information center was unveiled to help 300 French companies to remain competitive in global markets. The ceremony was conducted by the French Minister for Economy and Finance, Mr. Arthris, by the Chairman of the new Agency, Philip Caduc, and of course by Mr. Pautrat of the SGDN. This new organization has been given a clear focus, a defined mission and will be called the "Agency for Diffusion of Technological Information." This new Agency will become a fusion center for sensitive information in intelligence, business, diplomatic, and ministerial communications that reaches out to French Regional Chambers of Commerce seeking to promote French economic interests. Businesses who wish to avail themselves to this valuable information will be able to subscribe to protected and secured national data banks. While presently located under the Prime Minister office, a real power play is occurring within the French government to see what ministry will ultimately run it—Finance, Economy, Trade?

The French approach goes well beyond what many have attempted to propose as a symbiosis between national and corporate efforts to compete in world markets as well as goes beyond what many believe is appropriate. Some would maintain that only classified national security information should be protected and that only military and political government-vs-government espionage should be formally addressed. The French are attempting to integrate public and private information for offensive and defensive purposes. The presence of the Pasteur Institute on this Commission should make in the United States take a second look at this problem. For example, a U.S. pharmaceutical company that has entrusted to the FDA a \$60 million dollar product of research with all of its proprietary data, could be a tempting target for foreign intelligence collection. This information is as vitally important to a private company as a Top Secret document is to the government. It is simply not true that company proprietary information is less important or valuable than government classified information. After all, the stature of a nation depends upon the well-being of its industry. In fact, much of the technological data that foreign intelligence services target and collect are neither classified nor subject to government control. The challenge of protecting emerging, innovative technology goes to the heart of one of the strategic national security issues of our country: The competitiveness of the United States in global markets. But the French approach is more holistic than has been seen in the past. It is one which must be studied, and possibly emulated, because it is much more significant in the long term as a national strategy than the uncorrelated collection of interesting technical tidbits.

This realization is especially important to countries that find it prudent to form alliances for the gathering and exchange of specific intelligence to counter a common threat, as will be noted later on. Specifically, on May 28, 1990, Jay Peterzell, writing for TIME Magazine in "When Friends Become Moles", cautions us to the troubling reality of friendly governments aiding their domestic companies by funneling to them sensitive information gathered covertly from their allies. In fact, the article asserts that the French actively utilize a special section of their intelligence service to engage in "bag operations" jobs against American and foreign businessman in Paris. TIME reported that Service-7 of French Intelligence (DGSE) was set up in the early 1960's to run recruitment and collection operations against foreign firms in France. L'Express reported that U.S. intelligence had discovered that the DGSE had recruited assets in the European branches of IBM, Texas Instruments and other U.S. companies doing business in Europe. Incidents such as this have now become part of the staple of FBI briefings on DECA. Robert Courtney, a former IBM security official stated in the TIME article: "There's no question that they (The French DGSE secret service organization) have been spying on IBM's communications and have been giving the information to Bull for years." Increasingly, concerns are filtering throughout the contractor community that the threat of espionage is no longer limited to the traditional Soviet Bloc adversaries. Our allies or "friendly' nations must also be viewed with caution, especially when it comes to the protection of technical breakthroughs, financial insight, and corporate proprietary information. The French national initiative to collect innovative technology from competing markets prompts all countries to recognize the value of technical know-how in the emerging information age as a national resource, with the corollary need to defend it - and to acquire it for the common good. However, it follows in many ways the precedent set by Japan.

3. THE JAPANESE HAVE COME AND ARE HERE TO STAY

The Japanese efforts to penetrate U.S. industry, to gather innovative technology and sensitive business information, have made headlines in the past. Although individual corporate officers and companies have been exposed as culprits in the media, the official industrial and economic intelligence gathering is represented by the **Japan External Trade Organization**.

In Bob Woodward's controversial book *Veil*, he reports that in 1982 an investigation was opened to uncover the "leak", when it became apparent that highly classified excerpts from the U.S. National Intelligence Daily (NID) concerning the Iraq-Iran war were being sent from the Washington office of the Japanese Mitsubishi Corporation to Tokyo. ⁸ This investigation eventually lead to the resignation of a United States government official. Mitsubishi, along with Mitsui, Sumitomo and Nissho-Iwai, were identified by Meyer as the closest thing to a superpower conglomerate in the business world, with regards to intelligence capabilities. The Japanese trading companies or **sogo shosha** have become the standard by which others will be judged. Understanding business intelligence as organized information has been mastered by these Japanese trading companies. They have committed the resources and created the system needed to collect, analyze and distribute intelligence to key

executives. Pat Choate, in his equally controversial book **Agents of Influence**, also refers to the intelligence gathering capabilities of Japanese trading companies "as a vast overseas information collection system." Once again, according to Meyer:

"Indeed, every branch office of every trading company operates like a vacuum cleaner, sucking in information, statistics, documents, brochures, articles from technical and current events magazines, reports delivered at industrial and scientific conferences attended by one or another Japanese executive, and even gossip picked up at dinner parties or on the golf course. Some of these trading companies' operations are substantial; Mitsubishi intelligence staff in New York takes up two entire floors of a Manhattan skyscraper."

This raw material is then transmitted back to its headquarters where its senior intelligence and analytic staff transforms it into an intelligence product. Once the information is collated, analyzed, and synthesized, the intelligence is immediately delivered to the key executives who use it via a pre-defined need-to-know system for strategic decision making. This intelligence can then be exploited for tactical purposes. Strategic planners in Japan will also directly benefit from this intelligence product.

According to a 1987 classified CIA report *Japan: Foreign Intelligence and Security Services*, Japanese intelligence service priorities were the following:

- Intelligence regarding access to foreign sources of raw materials, including oil and foodstuffs
- Detailed intelligence on technological and scientific developments in the United States and Europe
- Intelligence on political decision making in the United States and Europe, most specifically, intelligence relating to trade, monetary, and military policy in Asia and the Pacific region
- Intelligence pertaining to internal political and military developments in the Soviet Union, the People's Republic of China, and North Korea

The report concluded that 80 percent of all Japanese-government intelligence assets were directed toward the United States and Europe, concentrating on high technology developments. The CIA report also allegedly explained the critical "intelligence gathering role" played by semi-official organizations, such as the Japanese Ministry for International Trade and Industry (MITI), the Japanese External Trade Organization (JETRO), and Japanese multinational corporations such as Hitachi and Mitsubishi.¹⁰ The CIA has assessed the quality of the intelligence gathering operations of these companies to be every bit as sophisticated as the intelligence services of smaller countries, including technical penetration and collection operations. In 1985, Professor Chalmers Johnson of the University of California at San Diego estimated that JETRO operated seventy-five offices in fifty-nine countries, with twenty-five of the offices located in "key foreign cities". This amounted to a "worldwide intelligence organization" with two hundred seventy agents overseas and twelve hundred analysts in Tokyo.¹¹

The close working relationship between Japanese companies and the Japanese government is illustrated in the famous IBM-Hitachi case, sometimes referred to as JAPSCAM. In 1981 Hitachi acquired a nearly-complete set of the confidential and much coveted IBM *Adirondack Workbooks* from a former IBM employee. These were state-of-the-art design workbooks containing technical secrets clearly marked **FOR INTERNAL IBM USE ONLY.** Eventually, the combined efforts of IBM counterintelligence and FBI personnel led to the dramatic arrest of a number of IBM officials and a reported, out of court settlement of US\$300 million for IBM. What is most interesting to note, is that Hitachi spymasters in Japan, who were supervising the espionage operations, transmitted their instructions to Hitachi case officers in San Francisco through Japanese diplomatic communications. The Japanese consulate had received telex instructions on how to proceed with the acquisition program after meetings between Hitachi and the American agents had occurred in Tokyo. Once communication was received in the consulate, the message was transmitted to the Hitachi man in Silicon Valley by the commercial representative of the Japanese consulate. ¹²

Similarly, in a remarkably candid interview appearing in *Bungei Shunju*, a Japanese monthly, in 1982, chairman of Fujitsu Taiyu Kobayashi described, in calculating detail, how Fujitsu also acquired information on IBM. While criticizing Hitachi for its blatant methods, he also explained how his firm avoided direct runs at IBM for information in order to avoid detection and prosecution. *The Washington Post* reportedly had planned to reprint the

Kobayashi interview in its entirety in a January 1983 issue. However, after *The Post* obtained the rights to do so from *Bungei Shunju*, Fujitsu became aware of it and pressured the monthly to cancel the agreement. The Washington public relations firm of Ruder and Finn, which represents Fujitsu explained that, "Fujitsu suggested that the complete version not be printed in the *Post.*" In another case it is believed that Fujitsu placed a Japanese mole inside Fairchild Semiconductors between 1977 and 1986 which did substantial damage to the company. This may be part of the reason why Fujitsu attempted to purchase Fairchild in 1986, while they were in secret negotiations with Cray Research Corporation for closer collaborations. These few examples are merely the tip of the iceberg when it comes to Japanese industrial espionage prowess. Unfortunately, as with all intelligence operations, the best and most successful often are never publicized or become known.

4. RUSSIA'S COLD WAR CONTINUES

All governments actively seek to acquire significant military technology and equipment. The spy versus spy game has long attempted to acquire technological breakthroughs and to break adversary cryptographic codes. so as to design counter measures that could neutralize a potential adversary. However, it was not until the early 1980's that the extent of such a program by the Soviet Union was fully appreciated. In an extraordinary exchange between President Mitterand of France and US President Reagan in Ottawa, Canada, in July, 1981, the French President briefed his American counterpart on "Farewell." "Farewell" was the cryptonym for a high level Soviet source within the Soviet Intelligence service technological theft program. 14 "Farewell" may be one of the greatest agents the West as a whole has ever run against in the Soviet Union. The man, who was prophetically code-named "Farewell," nevertheless elected to disclose to the West the entire order of battle for the massive Soviet effort to acquire Western technology. It lead to a great number of Soviet KGB and GRU expulsions from France and other Western countries and produced extremely detailed intelligence into the methods of operation of the Soviet effort, their take, and targets. A more recent book, The "Stormbirds," included even more detailed information. 15 It is reported that over 2,000-plus secret and top secret intelligence documents and two personnel lists of secret Russian, agents which he copied directly from the card indexes of Department "T", were initially provided only to the French. This allowed the identification of many KGB Line X officers and their assets. Information was obtained which was so detailed as to include the devastating statistics that 61.5% of all technical information then collected by the Russians came from American sources. Some of that material was declassified and released to the public in 1985 and is available for review.

The trend toward the recognition of the greater role of economic intelligence in our society is displayed most evidently in a series of articles published in *Pravda* beginning in 1990. In *Pravda*, on September 16 of that year, an article appeared entitled "In the Holy of Holies of Security - A Journalist has Crossed the Threshold of the Eighth's Main Directorate of the USSR KGB for the First Time." The significance of this article was embedded in the fact that it showcased one of the more interesting revelations of "glasnost". In an extremely revealing exposé, a new strategic direction was posited for the protection of commercial communications.

"Today, with regard to the changes in the world, new tasks face the cryptographers of the KGB: The amount of work in military directions is being reduced while the work on commercial issues is growing... The need to protect commercial secrets is becoming urgent, especially more recently in connection with the movement of our departments, enterprises and cooperatives into the foreign market... Our secret service will offer all types of aid and consultations to appropriate organizations at all stages in the design, creation, introduction, and use of such cryptographic codes. This has not changed in today's Russia." ¹⁶

This extraordinary article even claimed that U.S intelligence, in particular the National Security Agency (NSA), was actively aiding U.S. businessmen in their negotiations concerning trade in agriculture and oil. This allegation later will be referred to on in this report.

As the former East Bloc countries enter Europe and the world of economic competition, many changes will be thrust upon their societies. Unemployment and inflation are among the first indications of the transition to a free market economy. The question remains—what will they rely upon for their competitive edge? One or more elements will surely be required for success. Price, quality, technical innovation, service, etc. are examples of traditional resources which can provide a competitive advantage. However, a non-traditional edge could be provided by the national intelligence services. As noted earlier, the services set up by the Soviet KGB were

extremely competent. One of their major tasks was the clandestine acquisition of militarily-significant technology. The **"Farewell"** case points to these. As another example, some of the most lethal hemorrhages of technology were run by the Polish and East-German intelligence services. Certainly, privatized intelligence collection efforts on behalf of companies must also be taken into account. Former intelligence officers who were put out of work as governments changed in the aftermath of the cold war could be a source of talent for such private and corporate undertakings. But, the real question remains: Will governments task their present intelligence services, dedicated to military and national security, to gather economic intelligence in order to keep their countries competitive?

In June of this year, a new document entitled <u>"New Approaches to National Security Problems"</u> was obtained by news media organizations in Moscow, which might shed some light on this question. The report, supposedly written by the Russian Security Council before the appointment of General Aleksandr Lebed, but endorsed by him, clearly states that Russia must recreate its state's management system based on the "information highway". It also describes "economic security issues as dominant at this present stage of the country's development." To this end General Lebed is reportedly to have stated:

I believe that it is necessary to adjust the structure and goals of the intelligence services directing their efforts to back Russia's economic interests in the first place. I will demand that more effort be applied immediately in the following specific fields: to ensure an uninterrupted monitoring of the situation on the world markets of armaments, aviation and space equipment and to search for information on existing or developing technologies in the design of new armaments; to search for new designs in commercial technologies, both by state-run and private enterprises; to search for critical information on the plans and activities of the leading international financial institutions, major transnational corporations, banks and investment companies of all countries of the world; to organize information campaigns in foreign countries to attract more investment in the Russian economy. I believe it is necessary to allow the intelligence services to cooperate with major domestic production and financial enterprises of any form of property. The experience of France, Germany, Japan and China has proved the efficiency of cooperation for raising the competitiveness and technological potential of the domestic economy. These are the issues that I want to handle within the Security Council through coordinating the resources that already exist in the key financial and economic structures of the state.¹⁸

Other articles soon followed in the Russian press on the "Future of the Intelligence Community". These included more specifics about Lebed's plans to increase the number of GRU (Russian Military Intelligence) and SVR (Foreign Intelligence Service, former KGB First Chief Directorate) officers stationed around the world specializing in science and technological espionage. Countries specifically mentioned for technology collection include: United States, Great Britain, Japan, Israel, the Federal Republic of Germany, France, Italy, South Korea, and Sweden. Switzerland was also identified for intelligence personnel with higher financial education and directs the curricula of the GRU and SVR intelligence schools to be revised so as to increase the number of subjects in economics and finance. Also mentioned was the need to provide Westerners with access to classified technological information funds in the millions to stimulate growth of those willing to cooperate with the overseas intelligence posts. Lebed will supposedly take personal charge of the effort to support and form financial-industrial groups (FIGs) which might become the symbol of Russia's industrial might in the third millennium. These FIGs will be created mostly out of defense enterprises oriented toward the world market. An example of an emerging FIG is the military-industrial complex supporting the exports of MIG-29 fighter aircraft.¹⁹

5. PROTECTING THE BUSINESS OF THE UNITED STATES

The theft of U.S. proprietary information and technology by foreign companies has long been part of the competitive business environment. But, as former Director of the Central Intelligence Agency Director Gates pointed out in his testimony to the U.S. Congress in April, 1992, it is the increased activities of foreign governments in industrial espionage which is raising the level of concern: "Some foreign intelligence services have turned from politics to economics and the United States is the prime target." President Bush emphasized the same concern by saying that we must thwart anyone who tries to steal our technology or otherwise refuses to play by fair economic rules. Director Gates stated that "Various governments in Asia, Europe, the Middle East, and to a lesser degree, Latin America, as well as some former Communist countries (some 20 countries or governments in all) are involved in intelligence activities that are detrimental to our economic interests at some level." ²⁰

France, Japan, and Russia are by no means the only countries which have established a formidable apparatus for gathering business intelligence. The creation of such business intelligence systems is now recognized as a good national and corporate business decision. Meyer points out that the big American grain houses and large computer companies, to mention a few, have also formed similar units. However, most U.S. companies do not collect information and process it into true intelligence. The competitive world of international trade and finances will more than likely require it as well. However, the Japanese seem to have organized themselves within this capacity and it has become an extremely effective element for their overall competitiveness and success. Much can be learned from the success of the major Japanese trading companies. Acknowledgment of the Japanese achievement in <u>business management</u> should now be extended to that of <u>business intelligence</u>. American business must respond to this challenge not with complaints about the Japanese but with constructive action. "Japan bashing" should have no place in this discussion. The Japanese, French, and the Russians are doing their best to advance their interests - and so should we.

The allegation made in *Pravda* that NSA was actively aiding U.S. businessmen in their negotiations concerning trades in agriculture and oil, and that it would be increasingly involved in economic espionage, also against the USSR, is clearly disinformation designed to justify the Russian program. ²¹ If the truth would be known, there is tremendous trepidation on the part of the U.S. government to do anything this risky. The mere attempt to devise a method by which to disseminate sensitive information, to whom and for whatever reasons, is enough to stop any discussion of this topic right in its tracks. In America's open democratic system it is simply too hard to accomplish and would be contrary to the free market principles espoused by the U.S.. While these charges are clearly meant for internal consumption, it is interesting to postulate that even the KGB seems hard pressed today to justify their existence and still relatively enormous budget.

Although, industrial espionage is not new, the U.S. Federal government's response clearly appears to be changing. On August 10, 1990, FBI agents arrested Bernard Mayles after allegedly turning over micro-organisms and documents to an undercover FBI agent. This is the first major criminal espionage case involving, not classified United States defense documents, but those of a private pharmaceutical company. The undercover agent had offered the huge sum of \$10 million for the trade secrets of two of the nation's largest pharmaceutical companies. In the future, corporate spying may be getting more attention from the FBI financial crimes unit. In 1988, a National Institute of Justice survey showed that 48% of the 150 companies it polled had been victims of trade secret theft.²² A majority of those companies had been victimized more than once. Given the natural incentives of companies not to report the fact they have been victims of such crimes, common sense indicates that percentages are in fact low. However, adverse information, true or false, could send a company's stock plummeting. If the "year of the spy" taught us anything, it is that more people than we would like to admit are ready to compromise their ethics and national alliance for *money*.

American companies spend an estimated \$108 billion in R&D, or roughly one quarter of the world's investment in research. It should be no surprise, therefore, that U.S. R&D are the top target of industrial espionage. Other targets include: new technology, customer lists, program plans and financial data. The Mayles indictment indicates just how vulnerable pharmaceutical companies are. A \$10 million dollar bribe pales in comparison to the enormous amount of time and money it takes to bring a new drug to market. Trade secret experts maintain that pharmaceutical companies spend an average of 12 years and \$231 million to research and market a new drug. Herein lies the economic incentive which will drive a very active industrial espionage business. This all leads to one conclusion: American business faces many threats which in turn challenge our ability as a nation to maintain our economic competitiveness. This is a national security strategic issue since it means opportunities for economic growth. Protection of propriety information must not only be limited to foreign countries or companies, but American competitors within the United States. In my opinion, the most common threat to proprietary information is not from the electronic "bug" but from the open mouth. It is loose lips which can provide a competitor with more than is prudent. Electronic communications and eavesdropping on the national and global information highways can carry an inadvertent or willful sensitive remark near-instantaneously, and irretrievably, into unknown adversary camps.

The protection of propriety information in an increasingly competitive global market may ultimately incorporate the traditional means and procedures developed for the protection of classified government information. Corporate security may become a necessary component for survival, just as sound financial judgment and planning have traditionally been in the past.

6. INTERNATIONAL TERRORISM AS A GLOBAL THREAT

What are the new dangers to our technological society? How vulnerable is our information-dependent society as it evolves into a more efficient multi-faceted society electronically interconnected and responsive? What does the end of the cold war mean to our vulnerabilities and perceived level of threat. Do vulnerabilities and threats require an enemy to be named to survive?

International terrorism is now the emerging global concern. Specifically, in 1976 the Swedish Ministry of Defense published a report on "The Vulnerable Computer Society." This report explores the threat of sabotage and the increasing vulnerability of society as a whole during wartime because of the increasing use and reliance on computers. The resulting economic vulnerability of any society is then underlined in the report with the recent problems involving telephone networks. It is noted that repeated interruption of communications can produce powerful psychological warfare effects on the more technologically advanced societies. Especially affected are societies such as ours which have little, if any preparation to this type of disaster and psychological warfare.

In February of 1989, a series of hearings were held by the United States Committee on Government affairs. Experts from the Office of Technological Assessment who testified indicated that most electrical systems in the United States were not prepared for the advent of multiple serious failures to the system, whether they be inflected by natural disaster or by from a terrorist attack. The results of Hurricane Hugo confirm this. A systematic attack by terrorists upon multiple key electric power plants and their distribution centers, and destruction of the telephone switching stations, could have effects which would last for extended periods of time. Public utility companies just don't seem to conduct serious disaster planning that take into account the simultaneous knockout of multiple facilities. Equipment is not stored or propositioned to be rapidly set up in anticipation of an emergency of this magnitude. And even more surprising is the fact that many key installations do not even offer a moderate level of defensive precautions. To wit, when the high-capacity transformer which provides electric power for the Lawrence Livermore National Laboratory (LLNL) was destroyed by a series of escalating accidental events, a replacement transformer was not readily available. It took several months before the replacement could be found and transported to from the East coast to California to restore electric power at full load.

Another interesting report emerged from those 1989 hearing for the Senate Governmental Affairs Committee. The report was provided by one of our intelligence agencies. I quote from their public statement:

"Virtually all of today's computer systems and networks are susceptible to virus attacks. Protection techniques vary depending on the type of computers and networks in use. Currently, defenses against computer viruses fall into two categories: procedural and technical. Procedural protection consists of those actions taken to restrict access to the system or network. Personnel security, physical security, and administrative security play a major role. Technical defenses are software and/or hardware solutions that prevent, detect, or confine viruses. Because we lack effective technical defenses, we rely heavily on procedural protection. Strict adherence to good computer security procedures and policies is one way to defend against introduction of a virus. However, to provide increased protection, additional research is required to further develop effective technical defenses."

7. THE INVISIBLE WEAPONS of ELECTRONIC WARFARE

Now that we have left behind the cold war as a period of high tensions and high stability, how vulnerable are we? Have we adjusted psychologically and militarily to a world of low tensions but high economic instability? Is the world now a more dangerous place due to unprovoked terrorism and crime that can strike any place? Information Warfare is another area which has captured much of the discussion concerning the changing face of war. In Russia studies of the American effort during the Gulf war have lead to studies and formulations of informatic warfare as the wave of the future. The Rand corporation recent publication of Strategic Information Warfare summarizes its research conducted for the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) on this extraordinary subject. These areas continue to outstrip the imagination as one ponders the ongoing rapid evolution of cyberspace and the information culture of our advanced post industrial society.

Until now, most attacks on computers by terrorists have not been by a hostile virus but with explosive bombs. Let me explain: The EDP Auditors Association of Israel has monitored terrorist attacks on data processing (DP) personnel and facilities since 1969. Between 1969 and 1981 they reported fifty-four documented cases of direct DP terrorism. Twenty-two attacks were directed at United States companies abroad, half of the fifty-four cases took place in Italy and were the work of the 'Red Brigades' and other terrorist groups within their network. The Red Brigades clearly state in their own manifesto that computer targets are a key element of the capitalist technological society and that their vulnerabilities permit devastating destruction. Euro-terrorism has been in the forefront of attacks against computer facilities and companies. In the United States, our technological infrastructure is more vulnerable to a variety of such attacks—both those which are obviously malicious, and those which, while still benign, can be devastatingly destructive. For example: Robert Tappan Morris who unleashed the WORM on the Arpanet system caused a tremendous problem when the speed of the network rapidly replicated the WORM and it shut down much of the nation's digital communications. The government estimated the cost of the Morris experiment gone wrong at about \$160,000. Kevin Metnick, the phone freak depicted in CYBERPUNK, is the epitome of the public's dark-sided computer hacker. This case is only an indication of what is possible by those harm bent on harm could accomplish.

The Middle East certainly has developed an image for originating some nasty computer viruses. The IDF virus, named after the Israeli Defense Force which identified it, is just one example. Another is the PLO virus, and then there is the May 29th virus. These examples point to the vulnerability of computer systems and the prevailing methods of disabling attacks with ingenious viruses as agents of warfare. The result is a relatively low-intensity economic and psychological aggression. In one of the more turbulent areas of the world it could be played out as follows: Israel is a society which is known both for it's technology as well as existing in a hostile ethnic environment. The clandestine placement or activation of a computer virus within Israel by adversaries could become a critical impediment to wartime response and even bring into question survival. A "logic bomb" implanted within a target computer could become activated upon program change. A "time bomb" could launch a virus on a specific date. Strategic placement of viruses, can have a devastating or fatal effect. Such adversary actions must be of prime concern to the security professional because of their devious potential nature. Unlike these hostile viruses, the computer virus called "Brain" had the benign intent to catch computer software pirates, but because it proliferated without bounds many innocent computers were infected and their files destroyed. This virus was developed by two Pakistani brothers and could be viewed as another example of a computer prowl limited to the near East. But it is an omen of impending threat to our society that is much more vulnerable because of its growing dependence upon computers.

In France, new department within the DST has been created. This is the **`DST Protection Department.'** It will attempt to survey, monitor, and provide security for uses of the **INTERNET** by French business. The original idea was for it to somehow control the use of the **INTERNET** in France, but it soon became clear that this was an unrealistic goal. The concern over the **INTERNET** as an uncontrollable, international network was generated after the 1988 crash of the *Airbus*. A French company prepared a confidential internal report on the crash, but soon after is was completed, the most damaging portions of the report, citing design flaws, was distributed freely on the **INTERNET** through a Finnish institute. The French company claims that this leak was fostered by the U.S. competitor to *Airbus*—Boeing.

However, the conscious placement of a virus may also have positive applications. In the August 1995 issue of *Armed Forces Journal*, an article appeared with the following title: "*Virus*" *Implants* "*Go-Signals*" *in Future US Weapons?* The article describes how a virus or software disabling mechanism could be placed in every major new US weapons system—one which could be remotely triggered if the system, and the know-how for its activation, fell into an enemy's hands, or come under adversary control—could determined the outcome of the war without a shot being fired. While the article can be described as speculative at best, the idea of placing a radio receiver, embedded among thousands of other circuits on a key microchip to disable the system is both novel and intriguing, provided that the knowledge about its existence could be protected. The other side of the equation is, what could occur if an enemy was to obtain such a code or ability to activate the disabling program or redirect the compromised weapons upon their original owners. The answer is obvious and troubling; the nation's newest and most innovative weapons systems could be neutralized.

Information Warfare (IW) represents a growing concern among military war planners and Washington policymakers. Cyberspace, with all its promise also represents a growing set of uncharted vulnerabilities and in turn opportunities for both friends and foes. As we move forward as a society and a government which more and more intertwining telephony and computing, the need to better understand and protect the software links between these technologies becomes more and more challenging. As the world become better connected via the Internet and other wireless ways, the ability to reach out and touch a potential adversary increases exponentially. For these reason the United States government, as well as many others around the globe are exploring this new element of warfare. A recent RAND report conducted for the Department of Defense immediately comes to mind, for it moves our understanding from the tactical applications of IW techniques to the strategic level.

The United States has substantial information-based resources, including complex management systems and infrastructures, involving the control of electric power, money flow, air traffic, oil and gas, and other information dependent items. U.S. allies and potential coalition partners are similarly increasingly dependent on various information infrastructures. Consequently, if and when potential adversaries attempt to damage these systems using IW techniques, information warfare inevitably takes on a strategic aspect.²³

Some of the features of Information Warfare (IW) make the threat difficult to truly evaluate. Seven features were identified in the RAND exercise. They include: low entry cost; blurred traditional boundaries, public vs. private interests, criminal or warlike behavior, geographic, etc.; expanded role of perception management; new strategic intelligence challenge; formidable tactical warning and attack assessment problems; difficulty of building and sustaining coalitions; vulnerability of the U.S. homeland. These challenges will require sustained and creative government responses for many years, with the ever changing technological telecommunications and information environments.

8. CONCLUSION

In conclusion, the real issue for the business community is not to construct operatives and organs for clandestine operations and collection, but systems that could help us organize and visualize information in new ways. Business should not expect the United States government to do their job for them, or act as an agent on their behalf for competitive advantages. However, if foreign governments are in fact aiding their own domestic companies, an American policy could address this issue diplomatically and politically. For many businesses much of the information is already being collected by trade organizations or is otherwise within easy grasp. However, the systematic approach and coordination of such effort can transform the bulk of information gathering into succinct information intelligence. A corporate intelligence office, operating as an independent unit of the corporate strategic planning group, could transform an organization's traditional approach to information into a new and powerful business tool. Its formulation will no doubt take many reiterations, but the emergence of intelligence components will surely continue to grow in the business community.

For some businesses, it may suffice to bring to the same table those individuals who had collected information for the company in the past, but had perhaps not worked together in an organized and coherent manner. For others, it will be the establishment of a small group of employees who will collect, synthesize and feed to the top a new and powerful decision making tool. Whether it is called intelligence, or strategic planning, the new business management tool will emerge and increase in importance. Competition will force its existence to become commonplace.

A cogent example of such corporate activity has been practiced and demonstrated by the Phillips Company in Aachen, Germany. There, several hundred lawyers and technical professionals jointly review the global intelligence collected from their field offices, appraise the technical literature, and analyze global patents for their significance to Phillips' strategic business plan. This organization of legal and technical experts, working in part on a rotating basis by assignment from other corporate departments, has been successful not only by advising corporate decision makers, but also by filing a growing number of preemptive patents for Phillips to assure it a leading position for years to come. ²⁴

It should be obvious by now that we must plan to protect our domestic infrastructure and national resources against an information warfare attack and industrial espionage conducted against our

economic and technological base. In some cases we must consider this in alliance with other nations, in others not. The time to establish a viable policy to operate our information highways as safe conduits for electronic business is overdue. The effects such hostile actions could have on companies and our economy would have devastating implications to our inter-dependent global economy. Once certain forces are unleashed, even if in a limited capacity, the consequences are far from predictable and the potential damage is strategic.

REFERENCES

- ¹ U.S. News & World Report, June 3, 1991, "The New Spy Wars", p. 23.
- ² The Washington Post, November 6, 1991, Business section.
- ³ Herbert E. Meyer, *Real World Intelligence*, New York, 1987, p.8.
- ⁴ Ibid, pp. 8-9.
- ⁵ Meyer, Op. Cit.
- ⁶ Strategic Information Warfare, The Rand Corporation, 1996
- ⁷ The New York Times, July 1, 1996, Page one, "Economic Summit Subplot: Do French Walls Have Ears?", David E. Sanger
- ⁸ Bob Woodward, <u>Veil</u>, Simon and Schuster, New York, 1987, pp.368-371.
- ⁹ Pat Choate, <u>Agents of Influence</u>: <u>How Japan's Lobbyists in the United States Manipulate America's Political and Economic System</u>, Alfred A. Knopf, New York, 1990, p.37, from Meter, Op Cit. p. 58.
- ¹⁰ Peter Schweizer, <u>Friendly Spies: How America's Allies Are Using Economic Espionage To Steal Our Secrets</u>, New York, The Atlantic Monthly Press, 1993, pp.71-72. Admiral Pierre Lacoste of the French Intelligence Service further states that MITI and JETRO intelligence operations are massive, sending five hundred thousand messages back to Tokyo each day.
- ¹¹ IBID. p. 80.
- ¹²Op. Cit. p.56.
- ¹³ Op. Cit. p. 68.
- ¹⁴ Thierry Walton, <u>Le KGB en France</u>, Grasset, Paris, 1986, Part 5, The "Farewell" Dossier Scientific and Technological Espionage, p. 241.
- ¹⁵ Gordon Brook-Shepherd, <u>The Storm Birds</u>, Widenfield & Nicolson, New York, 1989, Chapter 17: "Farewell" A French Connection.
- ¹⁶ Foreign Broadcast Information Service, 24 September 1990 (FBIS-SOV-90-185), pp. 64-68, Endfield.
- 17 INTERFAX, Moscow, 26 June 1996; KOMMERSANT-DAILY, (in Russian) 26 June 1996, page 3; ITAR-TASS, Moscow 27 June 1996.
- ¹⁸ "Lebed's National Security Document", INTERFAX, Moscow, June 26, 1996, 1852 GMT
- ¹⁹ Nezavisimava Gazeta (Independent Newspaper), 1 July 1996, page 2, (in Russian)
- ²⁰ Hearings before the Subcommittee on Economic and Commercial Law, Committee on the Judiciary, House of Representatives, "The Threat of Foreign Economic Espionage to Corporations," April 29 & May 7, 1992, Senate # 65.
- ²¹ Reference 10, p. 67.
- 22 This paragraph was excerpted from a reproduction of an article dated September 16, 1990, The Business section of "The Record". This article also provided the information from the National Institute for Justice survey and the data on the U.S. spending in R&D.
- ²³ RAND corporation, Strategic Information Warfare, Washington, 1996.
- ²⁴ Personal communications with Dr. Herbert Newkirk, a chemist at the Lawrence Livermore National Laboratory who spent two years as a guest of Phillips on a sabbatical assignment.