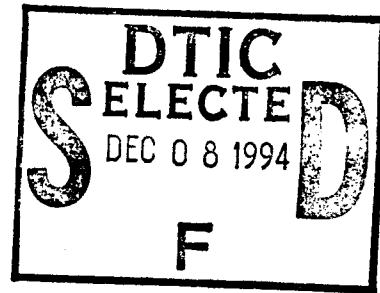


1994  
Executive Research Project  
S24

# Role of the U.S. Government in Industrial Espionage

*Lieutenant Colonel*  
**Phillip Stewart**  
*United States Army*

*Faculty Research Advisor*  
**Mr. George C. Fidas**



This document has been approved  
for public release and sale; its  
distribution is unlimited.



19941201 004

The Industrial College of the Armed Forces  
National Defense University  
Fort McNair, Washington, D.C. 20319-6000

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

## REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified		1b. RESTRICTIVE MARKINGS	
2a. SECURITY CLASSIFICATION AUTHORITY N/A		3. DISTRIBUTION/AVAILABILITY OF REPORT Distribution Statement A: Approved for public release; distribution is unlimited.	
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A		5. MONITORING ORGANIZATION REPORT NUMBER(S) Same	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) NDU-ICAF-94- <i>D 24</i>		7a. NAME OF MONITORING ORGANIZATION National Defense University	
6a. NAME OF PERFORMING ORGANIZATION Industrial College of the Armed Forces		7b. ADDRESS (City, State, and ZIP Code) Fort Lesley J. McNair Washington, D.C. 20319-6000	
6c. ADDRESS (City, State, and ZIP Code) Fort Lesley J. McNair Washington, D.C. 20319-6000		9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8a. NAME OF FUNDING/SPONSORING ORGANIZATION		8b. OFFICE SYMBOL (if applicable) ICAF-FAP	
8c. ADDRESS (City, State, and ZIP Code)		10. SOURCE OF FUNDING NUMBERS	
		PROGRAM ELEMENT NO. PROJECT NO. TASK NO. WORK UNIT ACCESSION NO.	
11. TITLE (Include Security Classification) <i>Role of the U.S. Government in Industrial Espionage</i>			
12. PERSONAL AUTHOR(S) <i>Phillip Stewart</i>			
13a. TYPE OF REPORT Research		13b. TIME COVERED FROM <i>Aug 93</i> TO <i>Apr 94</i>	
14. DATE OF REPORT (Year, Month, Day) April 1994		15. PAGE COUNT <i>33</i>	
16. SUPPLEMENTARY NOTATION			
17. COSATI CODES		18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)	
FIELD GROUP SUB-GROUP			
19. ABSTRACT (Continue on reverse if necessary and identify by block number)  SEE ATTACHED			
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input checked="" type="checkbox"/> SAME AS RPT. <input type="checkbox"/> DTIC USERS		21. ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL Judy Clark		22b. TELEPHONE (Include Area Code) (202) 475-1889	
		22c. OFFICE SYMBOL ICAF-FAP	

### Abstract

You can always find an article in the newspaper about military or political espionage, but only recently have we seen literature on other countries stealing our economic secrets. The fact is that they've been doing it for thousands of years - not just enemies, but allies as well.

What if someone claimed that the American economy loses over \$50 billion each year due to economic espionage by other nations. You don't believe it? Read on!

We must develop and implement intelligence policy to protect America's jobs and economy, while maintaining a delicate balance between government and business. I'll approach how I think this should be done.

## DISCLAIMER

This research report represents the views of the author and does not necessarily reflect the official opinion of the Industrial College of the Armed Forces, the National Defense University, or the Department of Defense.

This document is the property of the United States Government and is not to be reproduced in whole or in part for distribution outside the federal executive branch without permission of the Director of Research and Publications, Industrial College of the Armed Forces, Fort Lesley J. McNair, Washington, D.C. 20319-6000.

Accession For		
NTIS CRA&I		<input checked="" type="checkbox"/>
DTIC TAB		<input type="checkbox"/>
Unannounced		<input type="checkbox"/>
Justification		
By		
Distribution /		
Availability Codes		
Dist	Avail and/or Special	
A-1		

## Abstract

You can always find an article in the newspaper about military or political espionage, but only recently have we seen literature on other countries stealing our economic secrets. The fact is that they've been doing it for thousands of years - not just enemies, but allies as well.

What if someone claimed that the American economy loses over \$50 billion each year due to economic espionage by other nations. You don't believe it? Read on!

We must develop and implement intelligence policy to protect America's jobs and economy, while maintaining a delicate balance between government and business. I'll approach how I think this should be done.

*"There must be no more intimate relations in the whole army than those maintained with spies. No other relation should be more liberally rewarded. In no other relation should greater secrecy be preserved."*

Sun Tzu  
The Art of War

### Introduction

The idea of stealing a country's trade secrets is nothing new. It was almost two thousand years ago when spies from India stole China's highly coveted silk making process.

During the 18th century a french Jesuit, Father Francis Xavier d'Entrecolles visited the secret city of King-to-tchen and stole the secret to the process of making royal Chinese porcelain. He passed the secret back to France in a series of letters. By 1756 the French had established a porcelain factory in the city of Sevres and Chinese domination of the industry was at an end.<sup>1</sup>

It was during the 19th century that Great Britain's process to produce steel was stolen by the German spy, Alfred Krupp. This lead to Germany's development of the Ruhr Valley industries.

Espionage, yes even including industrial espionage, is an age-old art. Apparently many international business executives, their respective governments and intelligence agencies take the words of Sun Tzu very seriously. I can't say the same applies to America's business leaders.

Friends as well as former adversaries have stolen American trade secrets for decades. Only within the past ten or so years have we seen evidence of these thefts in print.

Many world states have shifted national interests since dramatic events beginning in 1989. Since that time, several unpredicted historical happenings have caused world governments to refocus:

- End of the cold war
- Dissolution of the Warsaw Pact and former Soviet Union
- Fall of the Berlin Wall
- Fall of East-European communism

National strategists no longer concentrate on military might and competition. Now they are attempting to provide an improved western lifestyle for their citizens. They now focus on economic prosperity and competitiveness. This competitiveness is not directed only toward former enemies, but toward allies alike. As the number of Democracies grows, elected politicians are becoming increasingly aware that, if they can't improve the daily lives of the populace, they won't be employed following the next election.

As specific examples will specify during latter parts of this paper, former enemy as well as former friendly governments are resorting to technology theft in order to improve the economic competitiveness of their

countries. The natural question which arises is, if allies are stealing our secrets, is it all right for the United States to do the same? Regarding crime rates in the U.S., President Clinton has recently proposed "three strikes and you're out." If the same philosophy held for industrial espionage, we would be conducting it against many "allies" today. The debate has no simple answers. Should we or shouldn't we?

The answer to the issue of whether the United States should conduct offensive industrial espionage is undecided. The issue is indeed controversial, the debate surrounding the issue has been heated. On the one hand, consider the billions of dollars the United States has spent on developing the most technically competent and thoroughly professional intelligence collection system in the world. Consider the billions we continue to spend! What benefit accrues to the average taxpayer from their hard-earned tax dollars? Hey! There's no great Soviet bear out there any more to conquer the good guys, so what are our dollars going for? Consider the thousands of Americans who have lost their jobs because of technology theft and resulting trade imbalances with friendly and former enemy nations. If some clever researcher were able to tie technology theft directly to the loss of specific American jobs, he would become an American celebrity. His study would result in an enraged public and a demand for federal government action.

After a fair amount of research on the subject, I have found that there are more non-supporters of offensive economic espionage than one might think. As a matter of fact, the non-supporters significantly outnumber the supporters of such an effort.

Senior government intelligence officials appear to be unanimous on the subject. They do not support a policy whereby the U.S. would conduct industrial espionage.

The U.S. Congress has provided both supporters and non-supporters on the subject. We find that more supporters surface when a foreign government's espionage attempts become publicized, and resulting congressional hearings take place.

The one population you would presume to support our government's attempts to collect against foreign corporations is American business. Surprisingly enough, this isn't necessarily so. Quite a few American CEO's have publicly stated that they do not support U.S. government interfering into international business relations. Some rationale follows:

- What technology/businesses do you target?
- When information is obtained, which American businesses receive it?
- Today, many businesses are transnational. They're neither owned by or operated in a single country.

- Current trade agreements such as GATT attempt to protect intellectual property rights. U.S. offensive business espionage efforts could thwart the future of such agreements.

For now, at least, policy makers are moving toward a consensus favoring a robust defensive posture. We will attempt to reinforce the security fortress around high-tech American business. This will be accomplished by:

- Reinforcing traditional business counterintelligence methodologies and employee training.
- Forewarning U.S. corporations of foreign technology theft attempts.
- Providing U.S. businesses with lists of "most wanted" technologies.
- U.S. enforcement of regional trade agreements such as GATT and NAFTA.

### **Background - "An Old Art"**

In a perfect world, business competition will exist, each capable worker will be employed, and most nations will prosper because of their economic strengths and natural resources.

However, we don't always have an even playing field. Some governments have been known to cheat. They assist state-owned

enterprises and private corporations with information obtained through government-sponsored espionage. The fact that governments do this is no revelation. We've long known that we must protect against such occurrences. "In 1949, as the cold war set in, the U.S. government passed the Export Control Act, and along with its West European allies established COCOM, the Coordinating Committee for Multilateral Export Controls."<sup>2</sup> The purpose of COCOM was to stop communist acquisition of militarily significant technology and preserve NATO's advantage over the Warsaw Pact. "Although COCOM had no institutional affiliation with NATO, it became known as the economic arm of NATO and was seen to perform a vital function in the West's policy of containment."<sup>3</sup> Although COCOM has had a significant impact in the reduction of technology transfer, much technology has successfully been passed to potential enemies. "CIA and Defense analyses had documented the Soviet military had taken advantage of . . . more than 3500 successful incidents of technology theft over the previous five years (1975-80) and detailed plans for continued activity."<sup>4</sup>

Very few Americans would recognize the potential economic impact of the loss of a few "trade secrets" to other nation's businesses. Based on the various sources that I have found, "the average cost to American business is estimated to be at least \$50 billion annually."<sup>5</sup> Fifty billion dollars represents a tremendous sum when we consider the paring down of

the U.S. budget. What if the loss is greater than this? All evidence suggests that it is. "In the three years since the end of the Cold War, the Department of Justice has prosecuted forty-seven cases involving economic espionage and the export of restricted technology . . . U.S. officials estimate they are detecting only one in twelve cases of economic espionage."<sup>6</sup> If this is true, then the economic impact upon America's annual output is staggering!

More and more evidence points toward greater losses of U.S. business to foreign theft. "In 1991, a survey covering a broad segment of the business community found that sixty-one of the 165 companies responding reported at least one recent incident of actual or attempted theft of their trade secrets."<sup>7</sup> Although many businesses have been reluctant to discuss business losses to foreign competition in the past, I feel that may be changing. The problem is becoming more and more public. Its publicity has made it known that economic espionage means the loss of American jobs and income.

During the Spring of 1993, Secretary of State Warren Christopher listed the United States' six foreign policy goals for the Clinton administration. "The priorities are 'economic security,' reform in Russia, a new framework for NATO, trade relations with the far east, Middle Eastern affairs, and nuclear nonproliferation."<sup>8</sup> The first of these priorities -

economic security - becomes clearer with each newspaper headline. The debates over the North American Free Trade Agreement (NAFTA), the GATT agreement, and others all stress the importance of free trade and economic security. More recently, President Clinton has considered trade sanctions against Japan due to a chronic trade deficit that was about \$60 billion in 1993. The point is that economic prosperity is of significant importance to the United States. Trade policy becomes more equitable each day. Each day illegal trade practices such as economic espionage become less acceptable. Economic competitiveness has become a challenge to national security.

Who's doing it? Quoting Forbes, "More than half of the world's nations are running industrial espionage operations against U.S. firms, according to FBI agents."<sup>9</sup> Although this statement is difficult for me to accept as fact, there are many documented cases of economic espionage directed against American business.

### **Recent Examples**

Ironically, some of the governments most widely known to target the United States are those considered as friends and allies - Germany, South Korea, Japan and France. We even assisted in developing some of these countries' intelligence services.

**France** - The French have been very open with their attempts to steal U.S.

industrial information. Pierre Marion, a former Director of French Intelligence states "In economics, we are competitors, not allies. I think that even during the Cold War, getting intelligence on economic, technological, and industrial matters from a country with which you are allies is not compatible with the fact that you are allies." In other words, being aligned with another country against a potentially hostile threat should in no way preclude your stealing the allied country's economic secrets.<sup>10</sup>

French intelligence collection capabilities changed in April of 1982. At that time, a new division of the government's intelligence structure, the Direction Générale de la Sécurité Extérieure (DGSE), was formed. This new element, formed by Marion, achieved almost immediate success. At that time the Indian government was negotiating with the United States, the Soviet Union, and France for the purchase of two billion dollars worth of fighter aircraft. The DGSE successfully recruited an Indian civil servant in New Delhi who worked in the prime minister's office. The civil servant obtained information on the American bid for the contract, provided it to the French, and France won the contract.<sup>11</sup>

"One of the most flagrant cases of industrial espionage occurred in France in 1987. French intelligence conducted a full-scale operation against the European offices of IBM, Texas Instruments, and other high-technology

American companies."<sup>12</sup> During January of 1987, the DGSE performed a strategic analysis to determine what types of secrets could most benefit French industry. IBM and Texas Instruments were chosen because they were industry leaders in computer technology. Corning was chosen because of its research in fiber optics. DGSE's attempt to obtain information from IBM was tremendously successful. Six employees were recruited to provide the company's sensitive information. Information was brought to DGSE covering everything from strategic business decisions, to financial information, to contract bids and high-tech research. Information from IBM was Funneled to the state-owned, financially-troubled French electronics firm, Compagnie des Machines Bull. IBM's proprietary secrets provided an infusion of prosperity to the firm and allowed it to advance against foreign competition.<sup>13</sup>

DSGE's efforts to steal company secrets at Texas Instruments and Corning also progressed well. Recruited personnel within the two companies provided volumes of material. The French intelligence service had to rent an apartment near the Texas Instruments facility in order to store the stolen information. Exploitation of these three American companies continued for two years. After working on uncovering the network for over eight months, a joint CIA/FBI team succeeded in cracking the conspiracy in November of 1989.

Has discovery of such espionage attempts slowed the French in their attempts to steal American technology? Hardly! During this past April, a "twenty-one page French document listing United States aerospace companies as targets for industrial spying was issued by the French government."<sup>14</sup> Not only were U.S. firms listed, but also "a shorter list of British and Swiss industrial and financial targets caused fresh embarrassment."<sup>15</sup> One of the items listed in the twenty-one page document was the Hughes Aircraft HS 601 communications satellite. Hughes recently lost out to a French company in a competitive bid to provide \$258 million worth of satellite gear to Arab countries. Hughes officials subsequently pulled all representation from the Paris Air Show, stating that the most recent French machinations were the last straw.

In June of 1993, one report provides that two French undercover agents were discovered at the Bell Textron plant in Texas.<sup>16</sup> Bell Textron is the company developing the V22 Osprey special operations aircraft.

Several sources have also indicated that Paris directed DGSE agents to obtain information from U.S. negotiators scheduled to attend the GATT (world trade) talks. Even with the discoveries of French intelligence failures during many espionage attempts, it appears that the intensity of such efforts has not lessened. They may, however, be becoming more clever. During May of 1991 the "French Consul in Houston was photographed by

U.S. agents while he was searching through the garbage outside the homes of executives for high technology companies. He claimed he was only trying to find material to fill a hole in his garden."<sup>17</sup> Sure he was.

Although the French have been stealing most of the headlines, estimates are that the Pacific rim and the Commonwealth of Independent States (CIS) countries are responsible for the bulk of economic espionage. U.S. intelligence officials estimate that "of the 3000 Chinese diplomats and officials in the U.S. and the 1600 from the CIS, some 40% are actually 'economic spies' sent to filch U.S. technology and corporate secrets."<sup>18</sup>

**Japan** - Perhaps the most written about case of industrial espionage in the 20th century is the theft of IBM's crown jewels by a former employee. During November of 1980, a computer scientist named Raymond Cadet resigned from IBM and took employment elsewhere. With him, he took a set of design books called the "Adirondack Workbooks." These books contained the technological secrets for the new series of computers that IBM would market for the upcoming decade. During the summer of 1981 Mr. Cadet sold copies of ten of the IBM workbooks to representatives of Hitachi Corporation. These workbooks assisted Hitachi in capturing large segments of the computer market from IBM, as well as significantly cutting Hitachi's research and development costs.

During the same time that Cadet was selling the IBM workbooks to

Hitachi, the FBI was busy setting up a sting operation in Silicon Valley, California. Mr. Zkenji Hayashi, senior computer planning engineer for Hitachi, unknowingly approached FBI sting personnel in an attempt to purchase information on the IBM 3380 computer. Information the Japanese had obtained from the Adirondack Workbooks would be enormously valuable when combined with the IBM 3380 data. "It would give Hitachi the opportunity to draw even technologically with IBM in the development of personal computers, promising hundreds of millions of dollars in new revenue."<sup>19</sup> On June 21, 1982, FBI sting personnel met with Hitachi to sell secret IBM computer information for a reported \$600,000. Hitachi personnel were arrested and charges were brought against them and Hitachi Corporation. The judge overseeing the trial ruled against jail time for the conspirators, and fined Hitachi only ten thousand dollars at criminal proceedings. In an out of court civil settlement Hitachi paid IBM \$300 million in civil damages.

When pluses and minuses are tallied, Hitachi survived the ordeal fairly well. They've successfully marketed a line of peripheral products to accompany the IBM 3031 computer, earning several hundred million dollars. Additionally, only two months after the sting operation, the U.S. Social Security Administration granted Hitachi a seven million dollar contract over IBM.

Germany - The conduct of friendly government sponsored economic espionage is found in virtually every continent or region. As we know, the United States was instrumental in rebuilding the German government and economy after World War II. This rebuilding effort included the German Intelligence Service, or Bundesnachrichtendienst (BND).

During December of 1989, BND agent Heinrich Stohlze came to the United States. His mission, as tasked by German intelligence, was to collect information on biochip research which was being conducted by high-tech companies within the Boston area. After being stolen, such information would be passed on to the German electronics giant, Siemens Corporation.

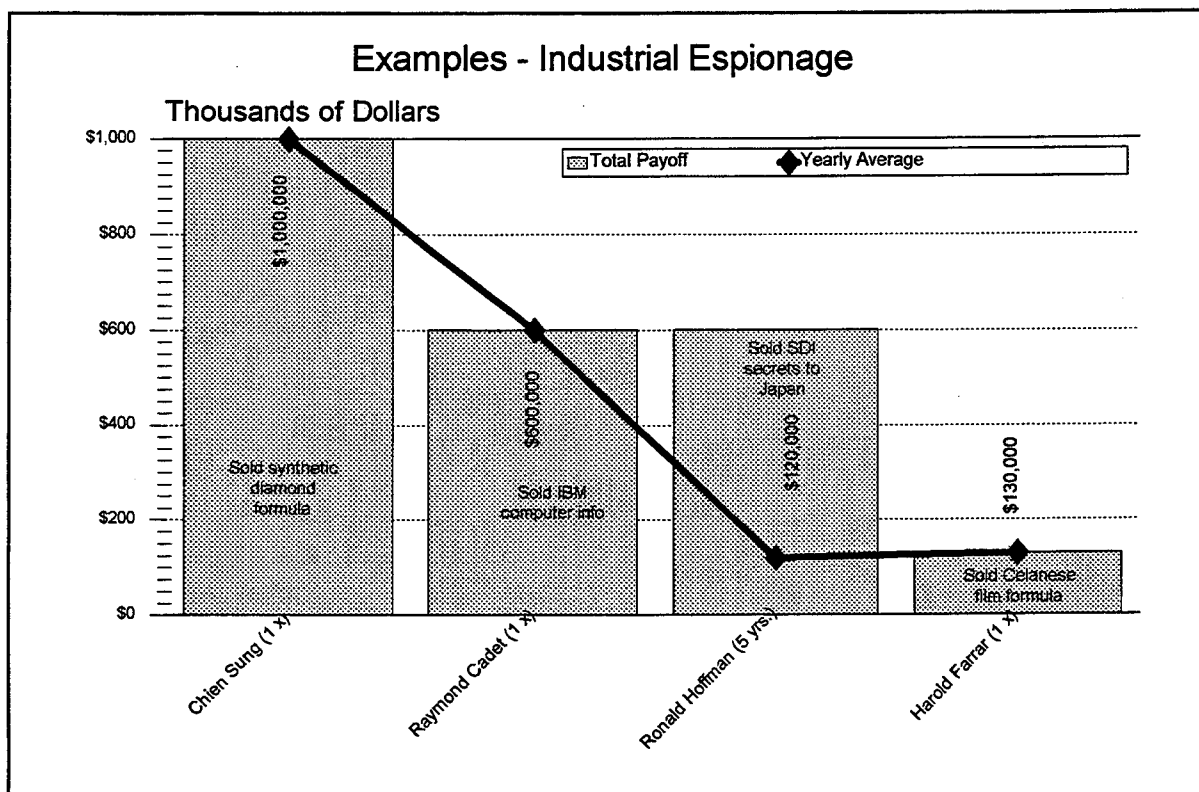
Within a few weeks of his arrival, Heinrich Stohlze managed to meet and seduce a mid-level manager employed by a high-tech company conducting bio-tech research on the east coast. At his request, she began to pilfer company technical documents for him to copy. Unlike the Japanese and French cases, motivation in this particular case was love, not greed. After a couple of months the company employee's disloyalty was discovered by her superiors. The company employee unsuccessfully attempted suicide. Mr. Stohlze escaped back to Germany with several thousand pages of sensitive bio-tech research data. The FBI was notified. However, no charges were ever filed against yet another friendly government.

### "Industrial Espionage on the Rise"

"Business and government leaders are reaching the conclusion that part of the reason U.S. competitiveness has weakened in the past 20 years is because of the loss of exclusive trade secrets and technology to foreign espionage."<sup>20</sup> I've provided examples of how industrial espionage is truly a problem for American industry. What bothers many government and business security professionals is that this form of industrial theft will probably continue. There are two primary reasons why this is so:

- Profitability
- Little fear of prosecution

The following chart illustrates that industrial espionage is, itself, big business:



What about legal reprisal when individuals are caught stealing company secrets? First of all, in order for someone to be convicted of a crime, a law must have been broken. "One of the problems faced by potential targets is that neither purchasing an electronic listening device nor planting a bug in an office is a crime - provided there is no forcible entry or trespass involved."<sup>21</sup> Our laws have not been set up to protect the intellectual property of corporations. Also, as pointed out earlier in a couple of actual cases, United States courts often impose very light sentences. So what do we see here? What is very clear is that the potential to obtain enormous sums of money exists, and the chance of serving jail time when caught is extremely small.

### **Legal Protection**

Believe it or not, there have been few laws or statutes designed to protect against technology espionage between states.

The most talked about international agreements of the 90's, GATT and NAFTA, only address the issue indirectly. "Article 21 of the General Agreement on Tariffs and Trade (GATT) allows individual countries to apply measures necessary - accordingly to their own judgements - to protect their national security interests."<sup>22</sup> This article, although not directive in nature, only permits participant states to enforce such protective measures as they deem necessary to protect security interests.

The North American Free Trade Agreement (NAFTA) doesn't go much further. What it does accomplish is an attempt to protect intellectual properties of the signatory states. Progress in the protection of intellectual property has probably been made due to recent developments in the franchising market in Mexico. A new law for the Promotion and Protection of Industrial Property was published in the Diario Oficial on June 27, 1991. The new law plays an important role in President Salinas' program to liberalize the Mexican economy and protect intellectual property in Mexico. It also makes Mexican standards consistent with the policy of the World Intellectual Property Organization.<sup>23</sup>

One law on the American books would appear to solve all of business' problems. "To declare information a trade secret often is a better option than patenting, since a trade secret need not be revealed to the public after a certain number of years. With the 1979 adoption of the Uniform Trade Secrets Act, unauthorized disclosure of a trade secret became a criminal act."<sup>24</sup> Even though the law is a valid one, we've rarely seen it enforced to the point of prosecution in court.

Why are businesses and governments reluctant to prosecute offenders through the legal system? The debate continues; the reasons are many.

### **U. S. Government and Business Responses**

Circumstances can also be thrown in to make it easier for the foreign

government or corporation to obtain U.S. industrial information. As we have read about foreign corporate policy, it's interesting to note that corporate loyalty is totally ingrained in employees within some countries. Not so within most U.S. corporations. Most employees of U.S. firms do not have this developed sense of corporate loyalty. Mobility is the key here. Employees switch jobs and corporations often - usually moving for raises in salaries or status. Loyalty can often be for sale to the highest bidder.

As you notice, it's only been within the last few years that American government or corporate officials have complained about foreign sponsored economic espionage. Why is this? Did it just begin or did we just become aware of it? The answers here are no and no. According to the former Director of NSA, Adm. Bobby Innman, for the past fifty years our government's "attention has been almost totally obscured by that big Soviet bear and the Cold War."<sup>25</sup> Our previous fears were those of political or military domination. Now, our attention is refocused - economic competitiveness is now key to national survival.

As stated earlier, several other friendly countries' intelligence services have been built based on the American model. U.S. eavesdropping facilities had been built in several of these countries during the Cold War era. Many feel that our government didn't complain of government sponsored economic espionage during the Cold War due to fear of loss of these facilities. If we

had complained of these illegal business practices, we might have lost certain basing rights.

Our State Department has probably downplayed the business of economic espionage due to its complex diplomatic situations. The case of Hitachi and its attempted theft of IBM's secrets created significant diplomatic complaints from the Japanese.

Leaders of U.S. owned businesses have also been reluctant to complain about espionage attempts. Fear of public embarrassment appears to be part of the reason here. Also, some U.S. business have lost contracts in countries who have been named in espionage attempts. Another reason to deter such allegations by U.S. business might be cost. The effort to prosecute cases in civil and criminal courts can run into excessive costs in time and money.

### **Conclusion and Outlook**

"In the end, the compelling reason for protecting American business secrets against espionage is to insure the survival of our economic system."<sup>26</sup> A lot of people would probably agree with these words by Richard Helms, former Director of Central Intelligence. Exactly how we go about protecting American business hasn't been agreed upon by policy makers. A close examination of the subject tells us that we don't even have agreement by business executives on the amount of government assistance that should be

afforded to industry.

Should the U.S. retaliate against other nations who illegally steal American industry's secrets? Our nation's current policy was voiced by Robert Gates, Director of Central Intelligence, in a speech during 1992. He stated "the U.S. intelligence community does not, should not, and will not engage in industrial espionage."<sup>27</sup> So if we aren't going to deliberately spy for American companies, then how are we going to protect our industry?

Our current Director of Central Intelligence is at least recognizing and speaking to the dilemma. "Industrial espionage has become in some ways, the hottest current topic in intelligence policy," Mr. Woolsey said during his Senate confirmation hearings last month.<sup>28</sup>

The current Chairman of the Senate Select Committee on Intelligence may add emphasis to U.S. intelligence's efforts in supporting American industry. Senator Dennis DeConcini, Arizona Democrat, has publicly stated opinions similar to the "three strikes and you're out" policy that President Clinton has suggested for criminal offenders. When considering what to do with economic intelligence that is not vital to national security, he has stated that "My own feeling is we ought to give it to our industry . . . if we find something, not to share it with our people seems to me to be not smart."<sup>29</sup> When considering what to do about other "friendly" countries' attempts to steal U.S. trade secrets, DeConcini stated that "we ought to be

prepared to strike back if we have to, just to demonstrate that if you want to play hardball, we can play hardball, too!"<sup>30</sup>

Apparently, we're seeing a shift, although subtle, in U.S. policy regarding whether our government will assist businesses with economic intelligence. I don't mean to imply that policy is changing to the extent that we'll begin to target human and signals intelligence assets towards economic collection in other countries. As you know, our intelligence agencies continuously prepare economic forecasts for other countries such as Russia, China, Japan, Canada, Mexico and many others. Much of the information collected for these studies comes from open source materials and is entirely unclassified. Some of this information is currently being passed to U.S. businesses through the Department of Commerce. Whenever intelligence officials can protect sensitive sources and methods from discovery by the general public, it may be possible to pass additional economic information to business.

Passing economic intelligence data to U.S. firms brings additional problems which must be solved. Do you provide the data to company A or company B? What changes would have to be made in the Freedom of Information Act? The problem of partial foreign ownership of U.S. firms raises difficult questions as well. These problems are real, but can be overcome with legislation.

The one pill that may be a bitter one for many federal bureaucrats is that, if we are to support U.S. industry with economic intelligence, then U.S. intelligence must become more open, more public and subject to open public controversy. The ability to protect intelligence policy decisions from public scrutiny via the Freedom of Information process will undoubtedly require significant modification of the legislation.

The Congressional Research Service has examined the items necessary to task the intelligence community to support U.S. business with economic intelligence:<sup>31</sup>

- Recruit intelligence analysts with business community experience.
- Encourage increased contact between economic intelligence analysts and private sector economic and science/technical experts.
- Increase liaison between intelligence community and the Department of Commerce.
- Improve dissemination of intelligence products.
- An economic intelligence advisory committee should be established under the direction of the DCI.

Should the Clinton administration make the decision to support U.S. industry with an enhanced technical intelligence product, the five items

above will certainly help to tie together a comprehensive program.

It is this writer's view that we should go ahead and provide key economic intelligence to U.S. business. I do not support an all-out effort against specific businesses, or even the targeting of specific countries.

What is necessary to complement economic efforts is information regarding economic trends and market shortfalls within the world's regions. U.S. business and government officials must work together to protect the American job market. Whenever our intelligence sources reveal vulnerabilities of U.S. business that are exploitable, American businesses must be warned. The American worker must also be educated on the necessity of protecting trade secrets, as workers have been in other countries.

## ENDNOTES

1. Friendly Spies, Peter Schweizer, Atlantic Monthly Press, 1993.
2. Export Controls in Transition, Gary Bertsch, Duke University Press, 1992, p. 1.
3. Ibid., p. 1.
4. Ibid., p. 41.
5. "Industrial Espionage: Reality of the Information Age," Stephen A. Carlton, Research-Technology Management, Vol. 35, Issue 6, Nov/Dec 1992, p. 18.
6. "U.S. Intelligence Retools to Fight New Brand of Espionage," Ronald E. Yates, staff writer, Chicago Tribune, Aug. 30 1993, p. 1.
7. "Industrial Espionage: Reality of the Information Age," Stephen A. Carlton, Research-Technology Management, Vol. 35, Issue 6, Nov/Dec 1992, p. 18-24.
8. "Christopher Lists Six Goals of Clinton's Foreign Policy," Daniel Williams, Staff Writer, The Washington Post, 26 March 1993, p. 1.
9. "The Valley of the Spies," Norm Alster, Forbes, Vol. 150, Issue 10, 26 Oct. 92, p. 200 - 204.
10. Friendly Spies, Peter Schweizer, Atlantic Monthly Press, 1993, p. 9.
11. Military Espionage is Out, Economic In, N.Y. Times, Jack Anderson and Michael Binstein, 14 March 1993, p. 14.
12. Friendly Spies, Peter Schweizer, Atlantic Monthly Press, 1993, p. 34.

13. Allies . . . or Enemies, Security Management (SEM), Daniel P. Scuro, Vol. 36, Issue 1, Jan 1992, pp. 78 - 81.
14. "U.S. Expanding Its Effort to Halt Spying by Allies," Douglas Jehl, New York Times, 30 April 1993, p. A1-10.
15. "Paris Fires Secret Service Chief for Spying on West," Leonard Doyle, The Independent, 7 June 1993, p. 8.
16. "Paris Fires Secret Service Chief for Spying on West," Leonard Doyle, The Independent, 7 June 1993, p. 9.
17. "French Riled by U.S. Claims of Industrial Espionage," Eduardo Cué, Christian Science Monitor, 3 May 1993, p. 8.
18. "U.S. Intelligence Retools to Fight New Brand of Espionage," Ronald E. Yates, staff writer, Chicago Tribune, Aug. 30 1993, p. 1.
19. Friendly Spies, Peter Schweizer, Atlantic Monthly Press, 1993, p. 61.
20. "Industrial Espionage: What You Don't Know Can Hurt You," Michael J. Stedman, Business and Society Review, Issue 76, Winter 1991, p. 25 - 32.
21. "Coming Clean on Dirty Tricks," Tom Nesh, Director, Vol. 45, Issue 13, August 1992, p. 38.
22. "Western Export Controls: An East European View," Technology Markets and Export Controls in the 1990's, Andrzej Rudka, 1991, New York University Press, p. 20.
23. "Business and the Law, The Status of Franchising and Intellectual Property Law in Mexico," Business Mexico Journal, Vol. 1, Issue 10, Dec. 1991, Enrique Calvillo, pp. 60 - 61.
24. "The Spy Who Loves You," ARMA Records Management Quarterly, Vol. 24, Issue 2, April 1990, Carolann Morino, pp. 24 - 26.
25. Friendly Spies, Peter Schweizer, Atlantic Monthly Press, 1993, p. 34.

26. *Speech to the International Security Systems Symposium, Alexandria, VA, 28 Oct. 1991, Richard Helms.*
27. *Speech to the Economic Club of Detroit, April 13, 1992, Mr. Robert M. Gates.*
28. *"Clinton Administration Grapples With New CIA Role," The Christian Science Monitor, Michael Richards, 22 March 1993, p. 6.*
29. *"Senator Suggests CIA Give Business Trade Secrets," Washington Times, Bill Gertz, 13 March 1993, p. A5.*
30. *Ibid.*
31. *"The U.S. Intelligence Community: A Role in Supporting Economic Competitiveness?" CRS Report to Congress, Richard A. Best, #90-571 F, December 7, 1990.*