Insider Espionage in Technology Businesses: Lessons from the Military and Government Security Agencies

Nwankama Nwankama

October 18, 2006

Advisor:

Col. Jonathan S. Lockwood, PhD, MSSI (US Army)

American Military University

IN690 – Independent Study – Intelligence

TABLE OF CONTENTS

BACKGROUND

The business world has always learned from the military and government security agencies. For example, the concept of strategic planning, which is taught in business schools and discussed in corporate boardrooms today, was derived from the military. Strategic planning also lays the foundation for operations in the most tactical government agencies. It was also the military (precisely, the U.S. Army) that worked with Bell Labs and major universities in the 1940s (at the heat of World War II), to perfect the statistical sampling techniques that are widely used in business operations today. Again, the concept of scenario planning, which first emerged following World War II, as a method for military and later security and intelligence operations planning is widely applied in business organizations today.

The twenty-first century fierce competition in business, driven by technology and globalization, has given rise to the necessitude of skilled intelligence in present-day business operations. Again, the business world has been learning about intelligence and intelligence analytical methods from the military and government agencies.

Notwithstanding the tremendous benefits business has derived from the military and government agencies, certain negative happenings within the military and government security agencies have also found their way into businesses. There have been an increasing number of cases of espionage by inside participants in businesses. Not surprising, insider participation in espionage has been a problem encountered by the military and government security agencies. In response, the military and government security agencies have conducted several studies towards understanding and dealing with the problem of insider participation in espionage, over the years. Businesses can equally benefit from such studies.

THE PROBLEM

Espionage is a particularly serious problem with American businesses, especially hi-tech companies. Many of the affected hi-tech businesses have lost billions of dollars and some have been forced into bankruptcy as a result of the loss of their competitive advantage due to espionage activities. Trusted technology insiders, who are indispensable in the business operations, have been found to actively participate in perpetrating most of these crimes against their employers.

FOCUS

This study focuses on the technology specialists within American technology companies. From the broad array of employees and associates who have access to computers or other high-technology equipments or systems within these companies, these specialists are the ones who design, maintain or manage the critical systems. Employees and associates in this professional category are of particular concern to the security professional because they possess the necessary skills and access to engage in serious harm if, and when, they choose to do so. Their typical jobs include systems administrators, engineers, systems programmers and operators and networking technicians. They are the high technology insiders.

This study excludes the mass of end-users who utilize computer or other equipment as parts of their jobs but for whom computers and equipments serve as a tool and not as a job in itself. While end-users are associated with their own set and level of risks (some of which may be similar to those of their h-tech counterparts), this study is specifically concerned with technology specialists, whose job functions elevate them well above the average end-user in terms of skill, access and potential for damage.

Furthermore, this study dwells only on the willful participation of the technology insiders whether or not the information stolen or otherwise compromised was subsequently sold; or whether the insider had been recruited prior to the theft or compromise; or whether the crime may have been committed for monetary gain or simply out of malice. This study does not attempt to deal with actions of the technology insiders due to their own carelessness in innocence, or where the circumstance of the breach or compromise was beyond their control, or that of the business or organization that hired them.

THE GOAL

Having received terrible blows to their operations over the years, the military and government security agencies have conducted several studies on insider participation in espionage. However, while it has been difficult or impossible to accurately predict who would eventually engage in espionage (in spite of rigorous screening and monitoring), some of the characteristics of the assailants, and their modes of operation have emerged over the decades.

This study examines some espionage cases within the military and government security agencies, and findings by the military or security establishments on the characteristics and modes of operation of those insiders who have engaged, or attempted to engage in espionage activities. It is hoped that this study will contribute to improvements in security related to the technical personnel within American technology companies; and to aid in the development of counterintelligence policies and practices within the technology businesses as it relates to insiders.

This study, while it is not exhaustive, has the potential to provoke specific commonsense applications for improving screening, selection, monitoring and management of technology specialists.

METHODOLOGY

Much has been written and said about how espionage criminals operate and the havoc they wreck. A lot of information can be heard from the news and derived from books and reports, but even from such news, books and reports, learning the specifics of actual cases (and not simply experiencing the sensation or knowing about the statistics) present one of the best opportunities for businesses to understand their own security needs, vulnerabilities and methods of intervention.

Data for this study was gathered using very low profile research methodologies. No interviews, fieldwork, surveys or focus groups was utilized. Sources of information were primarily from declassified military and security agency documents that are available to the public. This study also explores previous work by authors, academics, consultants, law enforcement agencies, research organizations, journalists and professional organization publications.

As an emerging area that hasn't been subjected to expansive study by business researchers or practitioners, considerable materials were gathered from the Internet, newspapers and other journalistic articles. Much information also came from government data and reports. However, wherever possible, serious attempts were made to explore supporting theories and other relevant information which might be available in published text.

BEGINNINGS OF INDUSTRIAL ESPIONAGE: HISTORICAL HIGHLIGHTS

Industrial espionage (though not as organized and sophisticated as it is today) is not new. It's quite true that the Elizabethan Age in Europe was one of the most remarkable moments in industrial espionage, but industrial espionage far predates the Elizabethan Era. The

history of the Silk fabric presents perhaps the first case of industrial espionage which is on record.

Industrial Espionage in the Development of the Silk

According to Emperor Confucius (551-479 BCE), the development of the silk started when Chinese princess Xi Ling Shi (sometimes spelled Si-ling-chi) in 2640 B.C. reeled a cocoon of silk which had dropped into her cup of tea. Confucius, founder of the Ru School of Chinese thought[1], is regarded as a great thinker, political figure, historian and educator. Ames & Hall (1987), Lau (1979), Nivison (1996) and Schwartz (1985) suggest that the work of Confucius is authoritative enough to present an authentic account of historical events in China.

Having reeled the cocoon of silk, princess Xi Ling Shi's husband, the great prince, Hoang Ti, directed her to examine the silkworm and test the practicability of using the thread. Thereafter, Xi Ling Shi discovered not only the means of raising silkworms, but also the manner of reeling the silk, and of employing it to make garments. Through this accidental event, the Chinese discovered the life cycle of the silk worm, how to cultivate the worms and make fabrics out of the silk. For the next 3000 years the Chinese were said to have kept their monopoly of silk fabrics.

Gradually, Chinese silk fabrics found their way throughout the whole of Asia (including Japan) and then to Europe. The trade was so profound that those long routes became known as the "silk roads." The silk fabrics greatly fascinated the Europeans (Romans, as they were known at the time, of which present Britain was a part) but they knew nothing of first their origin, and later how they were made.

---

[1] See "History of the Silk/The Silk Road" available at http://www.silkroadfoundation.org/artl/silkhistory.shtml, http://www.asianartmall.com/silkarticle.htm, http://www.travelchinaguide.com/silkroad/history/ and http://www.ess.uci.edu/~oliver/silk.html. Also see "Sericulture" at http://www.insects.org/ced1/seric.html; "Emperor Confucius (551-479 BCE)" at http://plato.stanford.edu/entries/confucius/) and http://www.newadvent.org/cathen/08578b.htm (see http://plato.stanford.edu/entries/confucius/). Internet. Retrieved February 24, 2006

Roman Emperor Flavius Anicius Julianus Justinianus (527-65) was to get the secrets of the silk by foul means, if necessary. He was born about 483 at Tauresium (Taor) in Illyricum (near Uskup) and died in 565. His 38 years of reign are regarded as the most brilliant period of the empire. He was full of enthusiasm and achieved the task of reviving Rome's glory. His accomplishments included a wave of military triumphs, development of bright legal systems, the promoting of religion and arts (especially the development or perfection of Byzantine architecture), and an aggressive trade and (as at that time), "industrialization." The Chinese fervently protected the secrets of silk production in order to maintain the lucrative monopoly. But, Emperor Flavius Anicius Justinian Justinianus's determination to understand how the silk was made, led him to embark on the first highly organized and State-sponsored industrial espionage scheme.

In 552 A.D., the emperor sent two Persian monks on a mission to Asia. Persia was under the Roman Empire and the monks (much like priests in our present civilization) were trusted and respected all over Asia. Maybe, the emperor's reasoning was that these monks would draw less attention than regular people. These monks were ordered to smuggle the worms, but the worms died en route but they left eggs. So, they went back to Byzantium with silkworm eggs hidden inside their bamboo walking sticks. Incidentally, Byzantium figured out how the silk was made.

This emperor's deceptive tactics is regarded as the earliest known example of industrial espionage. From then on, sericulture spread throughout Asia Minor and Greece. Thus, the emperor Flavius Anicius Julianus Justinianus gained the secrets of sericulture for the Roman Empire with the smuggling of the silk worm eggs from China by the monks. With China's monopoly on sericulture broken, silk importations from China drastically and progressively reduced.

The global production of silk has approximately doubled during the last 30 years with China and Japan being the two main producers. Together they manufacture more than 50% of the world production each year. American attempts on silk production have largely been unsuccessful. During the late 1970's China, the country that first developed sericulture thousands of years earlier as we saw above, has dramatically increased its silk production and has again become the world's leading producer of silk, but not the only producer. Although the silk production technique would have spread sooner or later, Emperor Flavius Anicius Julianus Justinianus's thievery was their undoing.

Industrial Espionage and England

England flourished during the period associated with the reign of Queen Elizabeth I (1558–1603). This period is often considered to be a golden age in English history - the height of the English Renaissance. This period is considered so highly partly because it contrasts so much with the periods before and after it. It was a brief period of largely internal peace between the English Reformation and the battles between Protestants and Catholics.

During this period, England was also well-off compared to the other nations of Europe and the world. But, this prosperity was not achieved by only fair means, of which slavery was just one reason. Spies like Christopher Marlowe and Walsingham (two of the pioneers of human intelligence – HUMINT) epitomized the human heartlessness in the pursuit of wealth and glory. They employed treachery, deceit, lying and other vices that would be considered despicable even in modern espionage.

British companies' ability to gather intelligence propelled the empire into a great industrial power even into later centuries. During the 18th and 19th centuries, ideas and information flowed in Britain. The ideas landed them in a formidable position in the industrial revolution. But with the free market system so created, Britain was not only a magnet for

information, but also became a source for information (a position America and especially America's hi-tech companies are all too familiar with today).

In the 18th century, Britain's textile, hardware, steel, coke-iron, steam power and glass industries were subjects of espionage from other countries. England developed the production of glass, but the French stole the English technology and improved on it. However, England between 1773 and the 1790s, in turn stole the improved French method that produced less distortion. Eventually, the French technology reached America. In many cases, insider technical personnel made the espionage more possible.

Steam engine technology was also believed to have been stolen from Britain. The British Science Museum[2] gives an account of the invention of the steam engine. There was a string of spying within Britain in the 18th century. Eventually in 1791, a young German mechanic named Georg Reichenbach bribed an insider with the British Boulton & Watt's steam engine pioneers. The Boulton & Watt's insider let Reichenbach view the 'Lap' engine - one of Boulton & Watt's steam engines installed in Boulton's works, and let him sketch it. Upon returning to Germany, Reichenbach then designed several similar engines even though Reichenbach experienced some initial technical problems. Nonetheless, the technology had been stolen.

Britain's textile industry also fell victim to the soon-to-be American industrialist Francis Cabot Lowell through espionage. Lowell wangled through insiders, who enabled him to copy British Cartwright textile factory designs and processes while "touring" their textile factories. Upon returning to America, Lowell built his own highly successful textile factory in Lowell, Massachusetts. It was this stolen British technology that brought the Cartwright loom to America, revolutionalizing the textile industry in America.

[2] See "Makings of the Modern World: Centres of Excellence: Engineering Pioneers" at http://www.makingthemodernworld.org.uk/stories/manufacture_by_machine/03.ST.01/?scene=5&tv=true. Internet. Retrieved October 16, 2006

Industrial Espionage During the Cold War – a Sketch

During the Cold War, much scientific and technical information passed from West to East (and vice versa) through the hands of scientists and engineers induced to act as spies and sometimes conniving with their counterparts on the other side. Macrakis (2000) provides a case study of Gorbachev Rehder - a scientist and high-ranking employee of *AEG/Telefunken* in West Berlin. Rehder was however, an artful spy for East Germany. He successfully performed his deeds for nearly two decades.

For his work as a spy, Rehder received several medals and awards in recognition of his "active participation and good results toward developing scientific-technical cooperation between the German Democratic Republic and the Soviet Union." Rehder's clandestine activities succeeded even though West Germany ran a large anti-industrial espionage operation, which was sometimes brought to naught because of insiders generating and/or entrusted with the secret information. Macrakis concludes however, that the strategy of developing technology by stealing it, rather than investing in research and development, turned out to be short-sighted.

Industrial Espionage and the US – a Sketch

The US has been well acquainted with incidents of espionage. For example, whereas the US can't be said to have clean hands, being a collector of extensive intelligence from other nations and organizations (and even from its citizens and citizen organizations), sometimes using surreptitious means, Petersen (1992, pp.152-211) shows that there were over 1,000 major cases of spying in and against the United States between 1775 and 1990. Moreover, the free market severely weakened or eliminated some old physical boundaries. The fall of the

Berlin Wall in 1989 created another epoch in industrial espionage against the US. So has the Internet, in fact to an unprecedented and unmatched degree.

Industrial espionage has been increasingly getting more sophisticated and clandestine especially with the removal or weakening of physical and governmental or administrative barriers that used to be there for the US. Spying is now more digitalized and the US has borne the brunt of it. At the same time, insiders in US firms are transferring decades of research, hard work and billions of dollars in investment, simply by hitting a “send’ button on a computer keyboard. Indeed, for the US, “the connectivity of the Internet has made the concept of borders and jurisdictions an incredible challenge” (Nasheri & Blumstein, 2005, p.1)

An Office of the National Counterintelligence Executive (ONCIX) Foreign Economic Collection and Industrial Espionage Reports to Congress, which were a 10-year compilation (1995 - 2004) of industrial espionage against US companies, show that the number of countries targeting the US has increased every year. For example, in the 2002 report, 75 countries were said to have been the perpetrators. By 2003 the number was 90 countries and in the 2004 report, over 100 countries were reported to have targeted US secret security and commercial information.

Very striking in the ONCIX reports were that the countries that were featured prominently were Algeria, Armenia, Azerbaijan, Belarus, Canada, China, Cuba, Germany, Georgia, India, Iran, Iraq, Israel, Kazakhstan, Kyrgyzstan, Libya, Moldova, Pakistan, Russia, Syria, Taiwan, Turkmenistan, Ukraine, and Uzbekistan. These countries have sought to steal or actually stolen information worth several billion dollars from US companies, agencies and the military. They have sought critical US military secrets (which cannot be quantified in dollar amounts),

information technologies, agricultural technologies, genetic engineering, chemicals, or business strategy and bidding strategies.[3]

Collection of US secrets by nations that are antagonistic to the US does not shock anyone. However, nations do not engage in espionage out of malice or to punish the source. They collect for their own advantages. Thus, countries that collect from the US have an interesting mix of nations - rich and poor; friend and foe, as seen from the ONCIX reports. Indeed, Schweizer (1993) notes that France has been one of the most aggressive collectors of economic intelligence in the world and that America is target number one, in spite of all France and the US have been through together. Indeed, Nolan (1999) reports that a top French government official once openly advocated that espionage against American firms was necessary to make French firms more competitive. Yet, France follows the precedent set by Japan – another US ally, in many ways.

Thus, Paul M. Joyal advises:

> *"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."*[4]

As already noted, notwithstanding the efforts of the outside collectors, there have been many sobering cases where Americans have proactively engaged in espionage and sold their motherland to the enemy, even during the cold war. They have included trusted people within and outside America's businesses and security agencies.

---

[3] See the Office of National Counterintelligence Executive Report and Speeches at http://www.ncix.gov/publications/reports_speeches/index.html

[4] Speech by Paul M. Joyal, president of Washington, DC based INTEGER Security Inc during the "Industrial Espionage Today and Information Wars of Tomorrow" conference - the19th National Information Systems Security Conference held in Baltimore, Maryland on October 22-25, 1996. For full speech, see http://csrc.nist.gov/nissc/1996/papers/NISSC96/joyal/industry.pdf

AN OVERVIEW OF US INTELLIGENCE AND SECURITY AGENCIES

The US Intelligence and Security Agencies comprise of sixteen agencies which formally comprise the U.S. Intelligence Community (IC). The IC encompasses:

1. Air Force Intelligence
2. Army Intelligence
3. Central Intelligence Agency
4. Coast Guard Intelligence
5. Defense Intelligence Agency
6. Department of Energy
7. Department of Homeland Security
8. Department of State
9. Department of the Treasury
10. Drug Enforcement Administration
11. Federal Bureau of Investigation
12. Marine Corps Intelligence
13. National Geospatial-Intelligence Agency
14. National Reconnaissance Office
15. National Security Agency
16. Navy Intelligence

In essence, the IC includes those agencies responsible for security responses to transnational threats, to include terrorism, cyber warfare and computer security, covert employment of weapons of mass destruction, narcotics trafficking, and international organized crime.

The US Military

The US military, which is clearly the most advanced in the world, is officially known as the United States Armed Forces. They consist of the Army, the Marine Corps, the Navy, the Air Force and the Coast Guard.

The US military is ranked second largest in the world. With its army alone approximately 3 million strong, China has the largest military in the World.[5] The US military has troops deployed around the globe. Its personnel in each service, as of 2004 are shown in Table 1, which follows:

Service	Total Active Duty Personnel	Percentage Female	Enlisted	Officers
Army	500,203	15.2%	414,325	69,307
Marine Corps	180,000	6.0%	157,150	19,052
Navy	375,521	14.5%	319,929	55,592
Air Force	358,612	19.6%	285,520	73,091
Coast Guard	40,151	10.7%	31,286	7,835
Total	**1,450,689**	**14.9%**	**1,196,210**	**254,479**

[5] Although China has the largest military in the world, many analysts see little reason to fear from China's military: Its personnel are reportedly poorly trained and equipped and its 8,500 tanks are slow, small and out-of-date.

The 4,000 fighter planes in the Chinese air force are mostly from the 1960s and 1970s and lack modern avionics. China's navy's 61 submarines and 54 surface ships are capable of little more than coastal patrols. "It's a very large military. It's a very old military," says Tom McNaugher, a China analyst for the Rand Corp. "In fact, two scholars recently referred to it ... as the world's largest military museum." To modernize, China is trimming its ground forces and using the savings to pick up high-tech bargains from the Russian arsenal. As of 1999, it had already purchased a squadron of Su-27 fighter planes, with a second squadron on order. And it's taking delivery of two of four quiet and fast Russian Kilo class diesel submarines. But progress has been slow. "They aren't buying in a number that will lead to any kind of immediate increase in combat capability," Montaperto said. "Reports are they are having trouble maintaining the submarines and the aircraft," McNaugher said. "The pilot training isn't all that effective. It's going to take a long time to absorb these weapons." The assessment at the Pentagon is that China could not project a sustained military force any distance from its borders. American military officials also believe that China, for all its size, could not even successfully invade tiny Taiwan. See "World's largest army not necessarily the strongest" at http://www.cnn.com/WORLD/asiapcf/9905/28/china.military/. Internet. Retrieved October 16, 2006

Table 1: US Military Personnel in Each Service as of 2004
Source: Wikipedia Free Encyclopedia

Every arm of the US armed services is under the command of the President. All arms of the armed forces, except the Coast Guard are part of the Department of Defense (DoD), which is controlled by the Secretary of Defense. In peacetime the Coast Guard is part of the Department of Homeland Security, while in wartime responsibility is transferred to the DoD.[6]

As seen from Table 1, over 1.4 million personnel were on active duty in the military as of 2004, with an additional 1,259,000 personnel in the seven reserve components (456,000 of which are in the Army and Air National Guard).[7] The US armed forces currently have no conscription requirements into the services. Rather, they compete with other employers, or opportunity-providers within the job market and larger society. However, the military continues to run behind its recruiting goals, leading to enormous pressure on recruiters. Indeed, there have been numerous cases of military recruiters going overboard and adopting outright illegal and deceptive practices in order to meet recruitment quotas.

Women are not allowed to serve in combat positions within the US armed forces. This practice has raised significant controversies especially among women rights groups. On the other hand, women are allowed to serve in a non-combat MOS.[8] Nonetheless, due to the realities of war many of these non-combat positions see combat regularly.[9]

---

[6] The United States Coast Guard has both military and law enforcement functions. Title 14, United States Code, Section 1, states "The Coast Guard as established January 28, 1915, shall be a military service and a branch of the armed forces of the United States at all times." In peacetime it is part of the Department of Homeland Security, but in wartime falls under the operational command of the United States Navy. Coast Guard units, or ships of its predecessor service, the Revenue Cutter Service, have seen combat in every war of the United States since 1790, including the U.S. occupation of Iraq.

[7] Additionally, both the Coast Guard and the Air Force have volunteer civilian auxiliaries: the United States Coast Guard Auxiliary (Coast Guard) and the Civil Air Patrol (Air Force).

[8] MOSs are Military Occupational Specialties, such as medical staff, educationists, psychologists, etc.
[9] See “Go Army. Careers & Jobs.” Available at http://www.goarmy.com/JobCatList.do?redirect=true&fw=careerindex&bl=. Internet. Retrieved on October 12, 2006.

The US military has many tactical military intelligence and outright security agencies and offices. They include the offices of Assistant to the Secretary for Intelligence Oversight, the Under Secretary of Defense for Intelligence, the Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Networks and Information Integration, the Defense Information Systems Agency, the Defense Advanced Research Projects Agency, the Defense Protective Service, the Defense Security Service Official and the US Special Operations Command.

The US Army has the offices of Army Deputy Chief of Staff for Intelligence, and that of the Intelligence and Security Command. The US Navy has the Office of Naval Intelligence, the Naval Security Group Command and the Naval Criminal Investigative Service. The US Air Force has the office of Air Force Technical Applications Center and the Air Intelligence Agency.

Director of National Intelligence

The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC). The DNI also acts as the principal advisor to the President; the National Security Council, and the Homeland Security Council for intelligence matters related to the national security. The DNI also oversees and directs the implementation of the National Intelligence Program.

The President appoints the DNI with the advice and consent of the Senate. The DNI is assisted by a Senate-confirmed Principal Deputy Director of National Intelligence (PDDNI), recommended by the DNI and appointed by the President.

National Intelligence Council (NIC)

The National Intelligence Council (NIC) is best known as the organization that produces National Intelligence Estimates, which are Intelligence Community-wide forecasts of issues and

challenges facing the security of the United States. Intelligence Estimates are ready to be delivered to top policymakers in reports. Unlike other intelligence reports, which focus on current intelligence, National Intelligence Estimates, as espoused by Dr. Sherman Kent, are forward-looking assessments. Such estimates have been considered by many to be the best analysis of specific issues of national importance or of national crisis situations.

The NIC reports to the Director of National Intelligence (DNI) in his capacity as head of the Intelligence Community (IC).

In an attempt to engage creative thinking from outside the Intelligence Community's classified bunker, the NIC has increasingly participated in joint sponsorship of conferences with non-governmental institutions and has produced a number of unclassified publications.

National Counterterrorism Center (NCTC)

The National Counterterrorism Center (NCTC) serves as the primary organization in the United States Government (USG) for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism (CT) and conducts strategic operational planning by integrating all instruments of national power. In December 2004, Congress codified the NCTC in the Intelligence Reform and Terrorism Prevention Act (IRTPA) and placed the NCTC in the Office of the Director of National Intelligence. The NCTC is a multi-agency organization dedicated to eliminating the terrorist threat to US interests at home and abroad.

The stated mission of the NCTC is to inform, empower, and help shape the national and international counterterrorism effort to diminish the ranks, capabilities, and activities of current and future terrorists. The NCTC is envisioned to become the nation's center of excellence for terrorism and counterterrorism issues, orchestrating and shaping the national and international counterterrorism effort to eliminate the terrorist threat to US interests at home and abroad.

The NCTC brags about ensuring precision, objectivity, integrity, and timeliness in pursuing their mission; developing the expertise of its employees, and ensuring their professional development and growth.

National Counterintelligence Executive (NCIX)

The National Counterintelligence Executive (NCIX) serves as the head of national counterintelligence (CI) for the US Government. It is directly responsible to the Director of National Intelligence (DNI).

The NCIX facilitates and enhances US counterintelligence efforts and awareness by:

1. Enabling the CI community to better identify, assess, prioritize and counter intelligence threats from foreign powers, terrorist groups, and other non-state entities.
2. Ensuring the CI community acts efficiently and effectively.
3. Providing for the integration of all US counterintelligence activities.

The NCIX chairs the National Counterintelligence Policy Board (NCPB), the principal interagency mechanism for developing national CI policies and procedures. The NCIX also heads the Office of the National Counterintelligence Executive.

Central Intelligence Agency (CIA)

The Central Intelligence Agency (CIA) was created in 1947 with the signing of the National Security Act by President Harry S. Truman. The act also created a Director of Central Intelligence (DCI) to serve as head of the United States intelligence community; act as the principal adviser to the President for intelligence matters related to the national security; and serve as head of the Central Intelligence Agency.

The Intelligence Reform and Terrorism Prevention Act of 2004 amended the National Security Act to provide for a Director of National Intelligence who would assume some of the roles formerly fulfilled by the DCI, with a separate Director of the Central Intelligence Agency.

National Security Agency (NSA)

The National Security Agency/Central Security Service is America's cryptologic organization. It is tasked with coordinating, directing and performing highly specialized activities to protect U.S. government information systems and to produce foreign signals intelligence information. The National Security Agency (NSA) is a high technology security organization. It claims to be on the frontiers of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the government.

National Reconnaissance Office (NRO)

The National Reconnaissance Office (NRO) designs, builds and operates the nation's reconnaissance satellites. It oversees the production of equipment and tools provided to an expanding list of customers like the Central Intelligence Agency (CIA) and the Department of Defense (DoD). Its products can warn of potential trouble spots around the world, help plan military operations, and monitor the environment. The NRO plays a primary role in achieving information superiority for the U.S. Government and its Armed Forces.

National Geospatial-Intelligence Agency (NGA)

The National Geospatial-Intelligence Agency (NGA), formerly the National Imagery and Mapping Agency (NIMA), is a combat support agency of the Department of Defense (DoD). It supports the Secretary of Defense, the Director of Central Intelligence (DCI), and other national-level policymakers in the areas of imagery, imagery intelligence, and geospatial information.

NGA is the single entity upon which the U.S. Government relies to coherently manage the disciplines of imagery and mapping.

Defense Intelligence Agency (DIA)

The Defense Intelligence Agency (DIA) is charged with providing timely, objective, and cogent military intelligence to war fighters, defense planners, and defense and national security policymakers. It relies on the integration of highly skilled intelligence professionals with leading edge technology to discover information and create knowledge that provides warning, identifies opportunities, and delivers overwhelming advantage to US war fighters, defense planners, and defense and national security policymakers.

Federal Bureau of Investigation (FBI)

The Federal Bureau of Investigation (FBI) is a law enforcement and intelligence agency of the US, under the office of Attorney General.

The mission of its intelligence program is to optimally position the agency to meet current and emerging national security and criminal threats by:

1. Aiming core investigative work proactively against threats to U.S. interests
2. Building and sustaining enterprise-wide intelligence policies and capabilities, and
3. Providing useful, appropriate, and timely information and analysis to the national security, homeland security and law enforcement communities.

The FBI attempts to create a common approach to intelligence work through enterprise-wide doctrine, policy, and production standards.

The State Department's Bureau of Intelligence and Research (INR)

INR is one of the smaller components of the Intelligence Community but is widely recognized for the high quality of its analysis. INR is strictly an analytical agency. Its diplomatic reporting from embassies, though highly useful to intelligence analysts, is not considered an intelligence function (nor is it budgeted as one).

Department of Homeland Security (DHS)

The Homeland Security Act provided the Department of Homeland Security (DHS) responsibilities for fusing law enforcement and intelligence information relating to terrorist threats to the homeland. The Information Analysis and Infrastructure Protection Directorate in DHS participates in the inter-agency counterterrorism efforts and, along with the FBI, has focused on ensuring that state and local law enforcement officials receive information on terrorist threats from national-level intelligence agencies.

The Department of Energy

The Energy Department analyzes foreign nuclear weapons programs as well as nuclear non-proliferation and energy-security issues. It also has a robust counterintelligence effort.

The Department of the Treasury

The Department of the Treasury collects and processes information that may affect US fiscal and monetary policies. The Department also covers the terrorist financing issue.

The Drug Enforcement Administration (DEA)

The Drug Enforcement Administration is the agency responsible for enforcing the controlled substances laws and regulations of the United States.

CRITICISM OF THE US INTELLIGENCE COMMUNITY

The terrorist acts of September 11, 2001 (9-11, as it is commonly called) marked holes that existed within the US Intelligence Community. The FBI reportedly had some of the perpetrators of the terrorist acts on their watch list. However, FBI's surveillance of those individuals was unknown to the Immigration authorities, as well as the essential local and other Federal security agencies, who let them go around without any hindrance whatsoever.

The terrorists later hijacked airplanes with which they blew up the NY World Trade Center, attacked Pentagon and were supposedly on their way to blow up the White House. They took thousands of life and caused billions of dollars in damages. Many businesses went bankrupt and many lives were permanently shattered.

Many analysts believe that the US, with its network of well-equipped security agencies should have been able to pick up the terrorist acts at their planning stages. Others charge that the US government was actually informed of the plots, but downplayed or didn't understand its magnitude. Either way, the Intelligence Community has been given a resounding "F" with regard to the 9-11 plot and attacks. Some attribute the intelligence failure to US's over-reliance on technology and inadequate use of human intelligence (HUMINT).

Several years after the resulting sweeping government reorganization began; the agencies charged with protecting the United States against terrorist attacks remain troubled by

high-level turnover, overlapping responsibilities and bureaucratic rivalry. Thus, many people argue that the pre-9-11 security holes still exist in the present day.

In his remarks during a hearing on the President's Proposal for a Terrorism Threat Integration Center, which was a part of the reorganization of the IC, the Senate Governmental Affairs Committee ranking member Joe Lieberman, noted on February 14, 2003:

> *"The disastrous disconnects among our intelligence agencies - the culture of rivalry rather than cooperation, turf battles rather than team work - that have plagued the intelligence community."* [10]

The Senator further noted that the disconnects and rivalries have been well-documented, and were well known. Most IC officials say that progress has been made toward the critical goal of the sharing of security threat information from all agencies. But, many people are adamant. They argue that the biggest restructuring of intelligence agencies in half a century has bloated the bureaucracy, adding boxes to the government organization chart without producing clearly defined roles.

Many people insist that the nation has not been provided sufficient evidence about how the intelligence community will overcome the institutional rivalries to information sharing that has already hindered the efficiency of the intelligence agencies. It worries many citizens that as of today, the US still do not have a truly all-source or an efficient intelligence organization capable of meeting 21st century security challenges.

Another criticism is that the US government has been steadily depriving or advocating policies that would deprive people of their fundamental human rights, using security and the 9-11 attacks as excuses. Countless citizens worry that the US Government is increasingly attempting to spy on their own citizens while many international events of national security importance are overlooked, not picked up on time or at all, or are handled improperly. Not only the inability of the US to detect the full extent of the 9-11 terrorist attacks at its planning stages,

[10] The full text of Senator Lieberman's remarks is available at http://www.senate.gov/~govt-aff/021403lieberman.htm

but India's and Pakistan's nuclear programs have been cited as gross security failures. The Iraqi intelligence debacle while Iran and North Korea have turned out to present bigger threats to the US and international community than Iraq or Saddam Hussein ever did have also been cited as evidence of US intelligence ineptitude. The Government's inability to properly respond to the Katrina calamity has also been cited. It typified the unpreparedness of the US government to handle major national disasters. These have all been described as shameful security failures in spite of the bloated and big-budget US Intelligence Community.

The failure of the IC to detect and handle truly critical cases on timely bases, but rather focus on the wrong people or nations has indeed, worried many people. Some citizens suggest that this is mainly because sometimes, some high-ranking CI officials or politicians are sidetracked by their rather ill-informed crusades, sometimes motivated by personal political goals or vendetta.

There continues to be speculations that the president invaded Iraq because he and his intelligence chiefs preferred to see Iraq as an easy target in order to put him in the annals of history as a war president, or to complete the job started by his father (Bush 1) who has been criticized in some quarters as not finishing the Saddam problem. Others suggest that the Intelligence Community tailored the Iraqi intelligence to suit what the president, his few international allies, and his top men and women wanted to hear. This suggests lack of independence of the IC – a very serious security problem if true. The "intelligence" which were presented to US citizens, government officials and the international community to sell the war, suggested that Iraqi weapons of mass destruction was so advanced they presented a "clear and imminent danger." The UN and much of international community who presented a different picture of the Iraqi weapons program – the official basis of the invasion, were snubbed and ridiculed. It turned out they were right and US "intelligence" was wrong. Some top officials US government officials have also rescinded their earlier claims that Saddam Hussein clearly had

links to the 9-11. The linkage of Saddam Hussein to the 9-11 terrorists was also based on US "intelligence" and was used to further sell the war.

Pre-attack US military and economic intelligence suggested a quick victory for US forces in Iraq, the heralding of US troops as liberators on Iraqi streets, and Iraqi oil fully paying the cost of the war christened "Operation Iraqi Freedom." But, since after the president's "Mission Accomplished" landing on the USS Abraham Lincoln on May 1, 2003, the world has witnessed thousands of military casualties, tens of thousands of Iraqi deaths, untold mayhem and destruction of property in Iraq, and billions of dollars spent on the war efforts while vital services and educational funding are cut at all levels at home. Worse, whereas the US invaded Iraq to clean it up of the oppressive and subversive regime of Saddam Hussein and terrorists, Iraq has actually become the hottest breeding ground for terrorists with no pragmatic end in sight. The ill-conceived war has made American to quickly lose the goodwill of much of the International community, which it garnered after the 9-11 attacks.

Crucial security agencies like the FBI have been criticized for their ineptness. For instance, CBS News[11] recounts that the FBI, had for two-and-half years earlier, ignored numerous warning signs about Robert Hanssen, a 22-year veteran of the bureau, who was later convicted selling sensitive information to Russia. Senior FBI officials later described Hanssen as the worst spy in US history and called the mole hunt that nabbed him a major triumph. They paid tribute to the skill, judgment and dedication of their agents. But it turned out that for years, the FBI had targeted the wrong man when they focused on Brian Kelley, an undercover officer at the CIA. He became the focus of an FBI-led investigation that nearly destroyed his life, not to mention his career.

[11] See "To Catch A Spy" CBS News, Aug. 24, 2003. http://www.cbsnews.com/stories/2003/01/30/60minutes/main538650.shtml. Internet. Retrieved October 16, 2006

Kelley's lawyer, Moustakas observed that in the matter of Kelley, the FBI had some solid clues, but when they connected the dots, they came up with the wrong picture.

Moustakas continued:

> *"This was a poorly run investigation, where the conclusion was foregone from the beginning …. what this bureau doesn't do well is it doesn't account for its own blind spot. It has a huge blind spot."*

There have also been charges of hypocrisy, frame-up and scapegoating against the US intelligence community. Whether such charges are valid or not, the mere mention or suspicion of double-standards, setup or entrapment is bad enough for such otherwise highly esteemed agencies such as the CIA. A year before Jonathan Pollard was arrested and charged with spying for Israel, CIA was suspecting a mole in certain operations relating to the Soviet Union. As it turned out, serious acts of espionage were going on within CIA, which led to the virtual collapse of the American espionage network in the Soviet Union. The collapse lasted until the dissolution of the Soviet Union in 1991. This collapse of the American intelligence network was a bitter humiliation to the CIA heads in Washington.

Incidentally the CIA heads put Alrich Ames, who was later arrested, charged and sentenced for spying for the Soviet Union in charge of investigating Pollard for what many think was a damage assessment. Thereupon, Ames reportedly began fabricating a secret file that cast blame on Israel for selling to the KGB the data it had received from Pollard. Then Ames leaked to the press allegations that the information Pollard fed Israel included the secret codes for American agents working in the Soviet Union, thus endangering their lives. As a result, Jonathan Pollard was indicted on passing classified information to an ally (Israel). He received a life sentence, which Appellate Court Justice Steven Williams called "a fundamental miscarriage of justice" (Dershowitz et al, 1999, p.A19).

AMERICA'S TECHNOLOGY BUSINESSES

As of the end of 2005, the United States had over 95,000 major high-technology companies (CorpTech, 2005). Current estimates exceed 100,000. These entities include companies with interest and exceptional capabilities in advanced materials, biotechnology, chemicals, computer, hardware, computer software, defense, energy, environmental, factory automation, manufacturing equipment, medical, pharmaceuticals, photonics, subassemblies and components, test and measurement, telecommunications and Internet and transportation.

Because of the extremely aggressive competition both at national and international levels, innovation is an ongoing process within these US technology companies. Such innovations require tremendous amounts of dedication and are often very time consuming. Also, they are usually very expensive – and exceptionally risky.

The risk of these technologies becoming obsolete within a short period of time is particularly high in the PC industry. For example, given the rapid advances in PC processor speed and memory, and improvements in network topology that are likely to occur every couple of months, most industry watchers expect many new PC products to become obsolete within one year (sometime less, or even before actual product launch). Thus, many high-technology companies are weary of investing in the requisite Research and Development (R&D) and would rather take a shortcut by unclean means. They'll rely on others' ideas or even engage in outright industrial espionage.

Many technology companies whose innovative products survive rapidly becoming obsolete do not reach their payback periods, which is the time they are expected to recoup their huge investments and which are usually three and half years, before their ideas are stolen (Kotler, 2003, p.365). Indeed many innovative projects do not completely get off the drawing tables before they are found in the hands of rivals – both local and foreign.

Losses from these thefts or information misappropriation within the technology industry have been difficult to calculate. The US Trade Commission estimates that over $300 billion is lost annually to theft of business secrets (Minieri, 2004, p.6). However, most industry watchers believe that total losses exceeds $500 billion annually. This is because many cases of industrial espionage are not reported as many companies fear the added problems negative publicity would wreck on their stock values.

In a bid to protect their proprietary information, upon which their success or failure depends, these high technology companies go to extraordinary lengths to shield themselves from attack. Paradoxically, they usually think of the technically sophisticated outside intruders when they try to protect their information. They envisage outside hackers, burglars or their competitors bugging their offices, boardrooms or corporate airplanes, or sending spies with sophisticated recording devices to their locations. For these reasons, they install sturdy firewalls, virtual private networks and secure phone or Fax lines. In addition, they mount robust locks, keys and very powerful security cameras and alarm systems. They hire well-trained and equipped security guards and implement stringent guidelines for visitors. They also employ the best technology gurus to set up and maintain their state-of-the-art security systems. Indeed, many of these companies go to extra lengths of installing powerfully built vault doors in their server rooms and other rooms containing their most sensitive information.

In spite of the vast security systems these American high technology companies put in place, their secret information is frequently stolen or compromised. Industrial espionage has hit US technology companies more than any other industry. Just like the US military and defense systems are the best in the world and always attract prying eyes, US technology firms are also the best in the world. Consequently, they are constantly under the threat of espionage activities not only by technology spies, software moles, but by subversive agents too (Allen, 1986; Allen & Norman, 1988).

When incidents of espionage occur within the US technology companies, many of the companies spend even a lot more money and resources pursuing the culprits or towards the recovery of the lost or compromised information. Yet, most times, it is too late. Even when the criminals are caught and damages are awarded by the courts, it comes several years down road and are hardy enough for the victim companies to recoup their losses. More troubling is that as mentioned above, most thefts are not reported, not only because of fear of negative publicity, but because or fear of their competitors using the information to their advantage. Some firms choose civil remedies over criminal prosecutions, and some are unaware of law enforcement interest in these types of crime (CSI/FBI, 2005).

CASES IN US MILITARY AND GOVERNMENT AGENCY INSIDER ESPIONAGE

The US Military and Intelligence Community possess the best technology and processes of any other country in the world. These agencies adopt very stringent hiring and security clearance and monitoring processes. Nonetheless, much sensitive information has been stolen and a lot of operations compromised over the decades, costing substantial loss of assets and human life. While many foreign security agencies may have succeeded in infiltrating US military and security agencies, there has been a lot of betrayal by insiders who were entrusted with the very information they compromised.

A snapshot of such cases (chosen at random) is presented underneath.

The Case of Alrich and Rosario Ames

Alrich Ames was a former CIA Insider, who with his wife, Rosario Ames was convicted in April of 1994 of several espionage-related offenses. Ames had spied for the Soviet Union/Russia for nine years, during which period some 30 CIA operations against the Soviets

were compromised, and at least 10 Russians and East Europeans were executed as a result of his espionage. According to Wise (1995), Ames received about $4.5 million from the Soviets for his espionage activities for the KGB, which (with his wife as an accessory) dealt a heavy blow on the US. Their activities were reportedly responsible for the loss of virtually all of CIA's intelligence assets targeted at the Soviet Union at the height of the Cold War.

CIA Director General and several news organizations gave an account of Ames's espionage activities.[12] Ames completed full processing for staff employment with the CIA in June 1962. He entered on duty as a GS-4 document analyst in the Records Integration Division (RID) of the Directorate of Operations (DO). Within RID, Ames was an insider, who read, coded, filed, and retrieved documents related to clandestine operations against an (undisclosed) East European target. He remained in this position for five years until he applied and was accepted as a Career Trainee (CT) in December 1967 after completing his BA in history at George Washington University with a lackluster B- average. Later, he was assigned to an SE Division branch. He remained there for several months before beginning Turkish language studies.

Ames had some unsuccessful overseas postings between 1969 and 1972. Thereafter, Ames spent the next four years, 1972-1976, at Headquarters in SE Division. Ames won generally enthusiastic reviews (PARs) from his supervisors. One payoff from this improved

[12] The Ames espionage case was well-publicized by both security agencies and the media. See the following examples:

a) CIA's Abstract of the Ames Affair, by the Inspector General titled "The Aldrich H. Ames Case: An Assessment of CIA's Role in Identifying Ames as an Intelligence Penetration of the Agency" available at http://www.totse.com/en/politics/central_intelligence_agency/amesig.html
b) Washington Post, 15 September 1999, p. A7. "Ames Seeks to Renegotiate 1994 Guilty Plea Over Spying for KGB"
c) CNN National Security Correspondent David Ensor interview with Richard Haver, former Executive Director of the CIA's Community Management Staff titled "CIA Spy Hunter Talks to CNN about Notorious Turncoats" on 29 May 2000 available at http://www.cnn.com/2000/US/05/29/cia.spy.02/index.html.

performance was the decision in September 1974 to name Ames as both the Headquarters and field case officer to manage a highly valued Agency asset.

Ames was later assigned to the New York Base of the DO's Foreign Resources Division from 1976 to 1981, where he received the strongest PAR of his career. These strong PARs led Ames to be promoted in May 1982, having been sent on a tour in Mexico City 1981. This assignment, like his earlier tour and his later tour in Rome, was unsuccessful. Furthermore, while in Mexico City, Ames became involved in an intimate relationship with the Colombian cultural attaché, Maria del Rosario Casas Dupuy.

Ames soon returned to CIA Headquarters in 1983, from Mexico City and was appointed as Chief of a branch in an SE Division Group. This position gave him access to the Agency's worldwide Soviet operations.

In 1986, Ames got a field assignment to Rome. He was Chief of a branch where he had access to information regarding many operations run or supported from that post. Despite his unbecoming conduct, Ames was successful in managing liaison relations with U.S. military intelligence units in Italy and also registered few other achievements.

Ames retuned to CIA Headquarters in mid 1989 to head a branch of an SE Division Group. Here again he had access to many sensitive cases. When that position was eliminated in a December 1989 reorganization of SE Division, Ames became Chief of another SE Division branch, where he remained until late 1990.

Ames moved to a position in the Counterintelligence Center (CIC) in October 1990. In the CIC, where he remained until August 1991, he prepared analytical papers on issues relating to the KGB but also had access to sensitive data bases. Discussions between Ames and the Deputy Chief, SE Division, resulted in Ames's temporary return to SE Division as head of a small KGB Working Group between August and November 1991.

In 1991, Chief SE Division requested that a counternarcotics program be established through liaison with the states of the former Soviet Union. Thereafter, Ames began a rotation to the Counternarcotics Center (CNC) in December 1991. At CNC, where Ames remained until his arrest on February 21, 1994, he worked primarily on developing a program for intelligence sharing between the United States and cooperating countries. Ames was sentenced to life in prison and his wife, Rosario received 5 years.

The Case of Samuel Loring Morison

Weiss (1999) gives an account of Samuel Loring Morrison's espionage activities. Samuel Loring Morison worked at the Naval Intelligence Support Center in Suitland, Maryland. He was an Intelligence Analyst specializing in Soviet amphibious and mine-laying vessels from 1974 to 1984. He was the grandson of the famous naval historian Samuel Elliot Morison.

Alongside his job at the Naval Intelligence Support Center, Morison worked as a part-time contributor and editor of the American section of Jane's Fighting Ships. Jane's Fighting Ships was an annual reference work on the world's navies and was published in England. Morrison reportedly earned about $5,000 per year from this part-time job. There were repeated complaints about Morison using office time and facilities to do his work for Jane's and he received warnings about conflict of interest between the jobs.

In 1984, conflicts with his supervisors led Morison to seek a full-time position with Jane's in London. At this time, Morison began overstepping the boundary of permissible information that could be sent to Jane's. The case came to a head when Morison took three classified photographs from a neighboring desk. These were aerial surveillance photographs showing construction of the first Soviet nuclear-powered aircraft carrier. Naval intelligence missed the photographs very badly. Soon thereafter, they appeared in Jane's Defense Weekly and were traced back to Morison.

Morison was accused, arrested and subsequently sentenced to two years in prison for espionage and theft of government property. Morrison was pardoned by President Clinton in 2001, raising a big uproar in some quarters. Nonetheless, as a result of the Morison case, policy guidelines for adjudicating security clearances were changed to include consideration of outside activities that present potential conflict of interest.

The Case of Marino Faget

Faget was a naturalized citizen who migrated to the US in 1959. He was a high-ranking Immigration and Naturalization Service - INS (now US Citizenship and Immigration Services - USCIS) official in Miami, Florida. Faget's espionage case was prominent in the news in 2000 and 2001[13]. Faget was arrested on 17 February 2000 and convicted of providing classified information to the Cuban intelligence service. At the time of his arrest he held a Secret security clearance and had access to sensitive INS files.

Faget first became a suspect in 1999 when technical and physical surveillance indicated that he was making unauthorized contacts with known Cuban agents. His arrest the following year was based on an FBI sting operation in which Faget was shown (bogus) information that a Cuban diplomat was about to defect. A few minutes later, Faget was recorded passing this information by phone to a business contact with ties to Cuban intelligence.

It was not known how much information Faget may have provided the Cuban intelligence service during his years with the INS. Nonetheless, on 30 May 2000, Faget was convicted of disclosing classified information, converting it for his own gain, lying to the FBI about contact

[13] Like other espionage cases, the Faget case was well written-about. See the following examples:
a) The Miami Herald, 12 Mar 2000, "Faget: 'Spy' Talk Was Only Business"
b) The New York Times, 31 May 2000, "I.N.S. Official is Convicted on Charges of Espionage")
c) The Miami Herald, 30 Jun 2001, "INS Official Gets 5 Years in Spy Sting", the Sun-Sentinel - Saturday South Broward Edition - June 30, 2001
d) Washington Post, 19 Feb. 2000, "FBI Sting at INS Found an Unlikely Cuban Spy Suspect."

with a Cuban official, and failing to disclose foreign business ties on his security clearance application. He was sentenced to five years in prison.

The Case of Timothy Steven Smith

Smith was a civilian employee serving as an ordinary seaman on the USS Kilauea. The USS Kilauea was an ammunition and supply vessel attached to the Pacific Fleet. While the ship was moored at the Bremerton Naval Station in Bremerton, Washington on 1 April 2000, an officer surprised Smith as he was removing computer disks from a desk drawer. [14]

A scuffle ensued, but Smith was subdued. Whereupon, 17 computer disks were retrieved from Smith's clothing. Furthermore, his quarters were searched and five stolen documents marked "Confidential," including one describing the transfer of ammunition and handling of torpedoes on US Navy vessels were found.

Smith was charged with two counts of espionage and two counts of theft and resisting arrest. Smith pled guilty after prosecutors dropped espionage charges. Pursuant to a plea agreement reached in August 2000, he pleaded guilty to one count of stealing government property and one count of assaulting an officer. He was sentenced in December 2000 to 260 days' confinement (to include time served). Smith was released on 22 December 2000.

The Case of George Trofimoff

George Trofimoff was a retired US Army Reserve officer, whose arrest on 14 June 2000 in Tampa, Florida featured prominently in the news[15] of the day, and was eruditely discussed in

---

[14] The case of Timothy Steven Smith featured in:
a) Seattle Post-Intelligencer, 14 Apr 2000, "Seaman Admits Stealing Defense Secrets, FBI Says"
b) National Counter-Intelligence Executive, News and Developments, Vol. 1, March 2001

[15] The following publications/press organizations, among many others, carried the Trofimoff spying news:

Byers (2005). Trofimoff, who was 73 at the time, was charged with spying for Russia for 25 years. His arrest concluded a seven-year investigation by the FBI and German authorities. As a Colonel, Trofimoff was the highest ranking US officer ever accused of spying.

According to the FBI, Trofimoff provided classified information to the Soviets/Russians while employed in a civilian job in Nuremburg, Germany, from 1959 to 1994 following his military retirement. Trofimoff was allegedly paid $250,000 for documents he provided to KGB, and later, to SVR agents. According to the indictment, Trofimoff, who was raised in Germany by Russian émigré parents, was recruited by Igor Susemihl, a Russian Orthodox priest and Trofimoff's boyhood friend. Susemihl died in 1999.

Trofimoff enlisted in the US Army in 1948 after his family moved to the United States. He became a US citizen in 1951 and received a commission in the Army Reserve in 1953. It was in 1987 that he retired with the rank of colonel.

During Trofimoff's military and civilian careers, he held Secret or Top Secret security clearances. In his civilian position with the Army 66th Military Intelligence Group, he had access to a wide variety of classified materials including US intelligence needs and objectives.

In or about 1969, Trofimoff was recruited into the service of the KGB by Susemihl, who at the time served as archbishop of Austria. Trofimoff allegedly removed classified documents from the US Army Interrogation Center in Munich, photographed and returned the originals, and then passed the film to Susemihl or KGB agents during several meetings in Austria or southern

---

a) The Associated Press, 14 June 2000, "Top Military Man Alleged to Be Spy"
b) New York Times, 15 June 2000, "Ex-Army Employee Charged With Spying for Russia for at Least 25 Years"
c) Miami Herald 21 June 2000, "Spy Suspect Bragged of Deeds, Prosecutor Says"
d) Orlando Sentinel, 15 Jun 2000, "Brevard Retiree is Accused of Espionage"
e) Stars and Stripes, 15 June 2000
f) St. Petersburg Times, June 6, 2001 "Trofimoff Spy Trial Promises Intrigue" and "Trofimoff Denies He Spied for Soviets"
g) Washington Post, 6 Jun 2001, "Espionage Trial Begins for Retired Army Colonel"
h) Miami Herald, 25 Jun 2001, "Historic Spy Trial in Tampa Nears End"
i) The New York Times, 27 Jun 2001, "Retired Army Employee is Found Guilty of Spying"

Germany. It is believed that Trofimoff turned over more than 50,000 pages of classified documents.

Trofimoff and his accomplice Susemihl had been arrested by German authorities for suspected espionage in 1994, but the case was dropped because the statute of limitations had expired. The investigation, however, was continued by US officials.

In late 2000, Trofimoff, who had since retired to Florida, was approached by an FBI agent posing as a Russian officer who offered a “special payment” for additional information. Before his arrest at a Tampa hotel, Trofimoff met with undercover FBI agents several times and was videotaped fully admitting his past involvement in espionage.

Although the retired Army employee pleaded not guilty, Trofimoff was convicted in June 2001 for his role in the 25-year espionage conspiracy after a four-week trial. He was sentenced to life imprisonment.

The Case of Robert Philip Hanssen

Hanssen was an FBI agent for 27 years. His espionage case dominated the news in early 2001. Perhaps Hanssen’s case was the most sensational case of national betrayal in recent history, attracting the widest coverage of any known case of espionage in the US.[16]

[16] The Hassen case was really a national frenzy. The following papers/press organizations were just a few of the sources of news articles about Hanssen’s espionage activities in February and March 2001 alone:

a) Washington Post, 10 February, 2001 "Virginia FBI Agent Arrested on Espionage Charges."
b) New York Times, 21 February 2001. "F.B.I. Agent Charged as Spy Who Aided Russia for 15 Years."
c) New York Times, 21 February 2001. "From Dour 'Mortician' of F.B.I. to Suspected Russian Superspy."
d) New York Times, 22 February 2001. "F.B.I. Never Gave Lie Test to Agent Charged as Spy."
e) Washington Post, 22 Feb. 2001. "Russia Says FBI Agent's Arrest Shouldn't Hurt Relations."
f) New York Times, 22 Feb. 2001. "The Prosecution Case: Zigs and Zags of Spy Cases Put a Damper on Predicting."
g) Washington Post, 22 February 2001. "Spy Suspect Had Deep Data Access, Ex-Associates Say."
h) New York Times, 22 Feb. 2001. "The Spymaster: Spy Handler Bedeviled U.S. in Earlier Case."

Hanssen was charged on 20 February 2001 with spying for Russia for more than 15 years. He was arrested in a park near his home in Vienna, Virginia, as he dropped off a bag containing seven Secret documents at a covert location.

For most of Hanssen's FBI career, he worked in counterintelligence, and was said to have made extensive use of what he learned in his own espionage career. Hanssen was charged with espionage and conspiracy to commit espionage.

Specifically, Hanssen was accused of providing first the Soviets and then the Russian government over 6,000 pages of classified documents and the identities of three Russian agents working for the United States. Two of these sources were tried in Russia and summarily executed.

According to court documents, Hanssen provided information on some of the most sensitive and highly compartmented projects in the US intelligence community as well as details

---

i) Washington Post, 22 Feb. 2001. "FBI Faulted For Rejecting Warnings."
j) New York Times, 23 Feb. 2001. "U.S. Had Evidence of Espionage, but F.B.I. Failed to Inspect Itself."
k) Washington Post, 23 Feb. 2001. "CIA Officer Had Been Focus of Spy Probe."
l) Washington Post, 24 Feb. 2001. "To Russia, With Longing."
m) Washington Post, 24 Feb. 2001. "Bush to Speed Clinton Spy Changes."
n) New York Times, 24 Feb. 2001. "Spy-Hunt Team Followed Trail to F.B.I. Agent."
o) Washington Post, 28 Feb. 2001. "FBI Left Hanssen an Opening as His Debts Mounted."
p) New York Times, 28 Feb. 2001. "Accused Spy Suspected Loss of Access to Secrets, Prosecutors Say."
q) Washington Post, 1 Mar. 2001. "Hanssen Carried Secrets Between FBI, State Dept."
r) New York Times, 4 Mar. 2001. "U.S. Thinks Agent Revealed Tunnel at Soviet Embassy."
s) New York Times, 7 Mar. 2001. "F.B.I. Spy Case May Explain Arrest of a K.G.B. Agent."
t) Sun-Times (Chicago), 11 Mar. 2001. "FBI Scandal Leaves CIA Gloating."
u) Washington Post, 13 Mar. 2001. "Webster Begins Probe of FBI Security Measures."
v) New York Times, 18 Mar. 2001. "My Friend, the Spy."
w) Washington Post, 18 Mar. 2001. "Hanssen Case May Be Linked to Defector."
x) New York Times, 22 Mar. 2001. "Russian Diplomats Ordered Expelled in a Countermove."
y) New York Times, 23 Mar. 2001. "News Analysis: In Espionage Game, Get Caught, Lose Players."
z) Washington Post, 24 Mar. 2001. "Spies and Other Ego-Trippers: Psychiatrist Jerrold Post Weighs the Personality in Politics."
aa) New York Times, 24 Mar. 2001. "Russia Expels 4 Americans and Vows 'Other Measures.'"
bb) New York Times, 21 Feb 2001, "F.B.I. Agent Charged as Spy Who Aided Russia for 15 Years"
cc) Washington Post, 25 Feb 2001, "'A Question of Why,' Contradictory Portrait Emerges of Spying Suspect"
dd) Washington Post, 6 Jan 2002, "From Russia With Love", and Los Angeles Times, 7 May 2002, "U.S. Authorities Question FBI Spy's Candor"

on US nuclear war defenses. In return, the Russians paid him $1.4 million over the period of his espionage activities, including over $600,000 in cash and diamonds and $800,000 deposited in a Russian bank account.

Hanssen was identified after the US authorities obtained his file from a covert source in the Russian intelligence service. However, the Russians never knew Hanssen's true name. To them, he was known only as "Ramon" or "Garcia." It is believed that Hanssen was involved with the Soviets beginning in 1979, broke off the relationship in 1980, but again volunteered to engage in espionage in 1985 by sending an unsigned letter to a KGB officer in the Soviet Embassy in Washington. The letter included the names of the three Soviet double-agents working in the United States.

Hanssen exploited the FBI's computer systems for classified information to sell and keep tabs on possible investigations of himself by accessing FBI computer files. In July 2001, Hanssen pled guilty to espionage and in accordance with his plea agreement, cooperated with investigators and avoided the death penalty. On 11 May 2002, the former FBI agent was sent away for life.

The Case of Ana Belen Montes

Montes was a senior intelligence analyst at the Defense Intelligence Agency (DIA). Several news articles in 2001 and 2002[17] reported how Montes transmitted sensitive and

[17] The case of Ana Belen Montes was carried by many papers/press organizations, including:
a) Associated Press, 21 September 2001, "Woman Charged with Conspiracy to Spy for Cuba"
b) Miami Herald, September 22 2001, "U.S. Intelligence Analyst Charged with Spying for Cuba"
c) New York Times, 30 Sep 2001, "Intelligence Analyst Charged With Spying for Cuba"
d) Miami Herald, 21 Mar 2001, "To Catch a Spy"
e) Miami Herald, 28 Mar 2001, "Cuban Spy Passed Polygraph at Least Once"
f) Miami Herald, 16 Jun 2002, "She Led Two Lives—Dutiful Analyst, and Spy for Cuba"
g) The New York Times, 17 Oct 2002, "Ex-U.S. Aide Sentenced to 25 Years for Spying for Cuba"

classified military and intelligence information to Cuba for at least 16 years before she was arrested on 21 September 2001.

Montes was a 44-year old, unmarried US citizen of Puerto Rican descent. She was employed by the Justice Department when sometime before 1985 she began working with the Cuban Directorate of Intelligence. It was not revealed whether she volunteered or was recruited by the Cuban Directorate of Intelligence. Surveillance on her activities was curtailed in response to the terrorist attacks of 11 September 2001 and concern that Cuba could pass on intelligence to other nations. Nonetheless, the Cuban Directorate of Intelligence encouraged Montes to seek a position with better access to information, and in 1985 she transferred to a job at DIA.

From her office at Bolling AFB in Washington, DC, Montes focused on Latin American military intelligence. In 1992, she shifted from her initial work on Nicaragua and became the senior DIA analyst for Cuba.

Montes met her Cuban handlers every three or four months either in the United States or in Cuba to exchange encrypted disks of information or instructions. The Cubans also kept in contact through encrypted high-frequency radio bursts that she received on a short-wave radio. She would enter the sequences of coded numbers coming from the radio into her laptop computer, and then apply a decryption disk to them to read the messages. She used pay phones on Washington street corners to send back encrypted number sequences to pager numbers answered by Cuban officials at the United Nations.

By not following their strict instructions on how to remove all traces of the messages from her computer hard disk, Montes left behind evidence of her activities. Over her years of espionage, she gave the Cubans the names of four US military intelligence agents (they escaped harm), details on at least one special access program, defense contingency planning for Cuba, and aerial surveillance photos. She reportedly passed at least one polygraph test while engaged in espionage.

Montes had access to Intelink[18] and the information contributed to that network by 60 agencies and departments of the Federal government. Pursuant to a plea agreement to reduce her sentence, she cooperated in debriefings by various intelligence agencies. She was sentenced on 16 October 2002 to 25 years in prison and five years' probation.

The Case of Brain Patrick Regan

Regan was a former Air Force intelligence analyst. He was arrested on 3 August 2001 at Dulles International Airport, near Washington, DC as he was boarding a flight for Switzerland.[19] On his person he was carrying missile site information on Iraq and contact information for embassies in Switzerland.

---

[18] The IntelLINK is a classified Web network for the intelligence community. It links information in the various classified databases of the US intelligence agencies (e.g. FBI, CIA, DEA, NSA, USSS, NRO) to facilitate communication and the sharing of documents and other resources. Intelink components include Intelink-U (formerly known as the Open Source Information System (OSIS), Intelink-S, Intelink-SCI, Intelink-P, Intelink-C, Intelink-S (and C2-link) Intelink-S, the secret-level variant of Intelink, has begun to expand rapidly in scope and reach. As the intelligence support medium for GCCS [Global Command and Control System] and law enforcement activities, Intelink-S is expected to become the principal growth area for intelligence products and services. Its customer base will be extraordinarily diverse, eventually encompassing all areas of U.S. government operations that can benefit from integrated intelligence support and collaboration. Intelink URLs take the form of (for example): http://www.nrad.navy.ic.gov and http://www.server.daro.ic.gov

[19] Regan's case was well-covered in the news. The following are a few examples:

a) Washington Post, 24 August 2001, "Retired Air Force Sgt. Charged With Espionage"
b) Washington Post, 25 Aug. 2001, "Air Force Retiree Charged as Spy: Secret Documents Passed, U.S. Says."
c) Washington Post, 25 Aug. 2001, "Satellite Agency Has Tradition of Secrecy; Joint Defense-CIA Enterprise Uses Many Contract Employees Such as Alleged Spy."
d) New York Times, 25 Aug. 2001, "Employee of U.S. Contractor Accused of Conspiracy to Spy"
e) Washington Post, 24 Oct. 2001, "Spy Suspect Had Missile Site Coordinates."
f) Washington Post, 15 Feb. 2002, "Indictment Says Suspect Tried to Sell Defense Secrets."
g) Washington Post, 11 Feb. 2003, "Jury Opens Deliberations in Federal Espionage Case; Regan Could Face Death if Convicted of Spying Charges"
h) Washington Post, 21 Mar. 2003, "Convicted Spy Accepts Life Sentence: Sudden Sentencing Deal Will Prevent Prosecution of Ex-Air Force Analyst's Wife"
i) Washington Post, 28 Apr. 2003, "Coded Messages Add to Mystery of a Failed Spy"
j) Washington Post, 31 Jul. 2003 "Convicted Spy Led FBI to Papers Buried in Parks."

By virtue of his position as an intelligence analyst, Regan was a US Air Force technical insider. He had enlisted in the Air Force at age 17 and began working for the National Reconnaissance Office (NRO) in 1995 where he administered the Intelink. Following his retirement from the military as a Master Sergeant in 2001, he was employed by defense contractor TRW and resumed work at NRO where he was employed at the time of his arrest.

Regan had held a Top Secret clearance since 1980. Computers searched in Regan's home led to the discovery of letters offering to sell secrets to Libya, Iraq, and China. In the Iraq case, he asked Saddam Hussein for $13 million. The documents, classified at the Top Secret SCI level, concerned the US satellite program, early warning systems, and communications intelligence information.

Regan was charged with three counts of attempting to market highly classified documents and one count of gathering national defense information. On 20 February 2003, he was convicted of all charges except attempting to sell secrets to Libya, and on 21 March, pursuant to a sentencing agreement, he was sent away for life without parole. Information provided by Regan after sentencing led FBI and NRO investigators to 19 sites in rural Virginia and Maryland where he had buried over 20,000 pages of classified documents, five CDs, and five videotapes that he had stashed presumably for future sales.

CASES IN THE TECHNOLOGY INSIDER PROBLEM

Just like the US armed forces and security agencies, US technology firms have suffered tremendous losses to espionage activities. Although many outside individuals and organizations have indeed violated many American technology companies and stolen their valuable secret information, numerous cases exist where the very people entrusted with the design of the company technology secrets or the running of the security systems that protect them have

betrayed their employers and willingly stolen, compromised, sold or otherwise divulged company trade secrets. Indeed, most corporations (domestic and foreign) that illegally ended up with trade secrets belonging to US technology companies do not instigate the espionage activities themselves. They are solicited by people that have stolen, or who are privy to the potentially profitable secret information.

US technology firms have made serious attempts – most by building physical shields, to secure their proprietary information. But, Nolan (1999, p.242) was not surprised about the failure of the physical defenses erected by many of the companies: “Clearly, the weakest points were not solely – or even primarily – related to physical security.” It was people. It’s those people inside the businesses that cause espionage. Nolan is adamant: “stronger locks or bigger guards would have no influence” over the real security of these companies without the people factor (p.243).

Most of the insider perpetrators are high technology people who like their military and government security agency counterparts, occupy trusted positions in their places of work – the very entities that they rob and betray. They are the very people who design, install and man the systems. This heartbreaking collusion or instigation by trusted insiders to steal, sell or compromise proprietary information belonging to their employers has been a major concern for many security professionals.

A snapshot of such cases is presented underneath. Please note that in some cases, the names and identities of the individuals were not available from the sources.

The Case of Mr. Shin-Guo Tsai

Tsai was a design engineer with Volterra - a semiconductor company in Fremont, California. He was Taiwanese.

Tsai reportedly gave notice of his resignation on February 15, 2005 in order to go get married in his native Taiwan. But, the story was a smoke screen, according to the FBI which alleged that Tsai had downloaded information on Volterra's products.

Tsai was accused of using a private e-mail account to send some of the information to a Taiwanese startup company that was recruiting him for a job. Nonetheless, Tsai assured his colleagues at the office that he didn't have a job lined up either in Taiwan or elsewhere, or in the United States when he came back. Suspicious, Tsai's co-workers informed a manager that he had been downloading secret technical data. Whereupon, the FBI was alerted and upon confronting him, Tsai admitted to stealing and sending the proprietary data to CMSC, Inc. which was a Volterra's competitor based in Taiwan.[20]

On September 6, 2005, Mr. Tsai was arraigned on a charge of transporting a stolen data sheet containing his employer's proprietary information in foreign commerce in violation of 18 U.S.C. § 2314. He pleaded guilty to this charge pursuant to a plea agreement he entered into with the United States attorneys. According to the plea agreement, Tsai admitted that he sent the stolen data sheet for Volterra's VT1103 product to his contacts at CMSC, Inc. in Taiwan. Tsai also admitted that he stole the data sheet and that the value of the proprietary information contained in the datasheet is worth no less than $120,000.

Tsai's lawyer, John Robertson of Los Angeles, insisted his client's actions did not involve industrial espionage. Tsai's charge carried a maximum statutory penalty of 10 years imprisonment and a fine of $250,000, but on January 23, 2006 US District Judge Ronald M. Whyte gave Tsai less than 10 years, according to the applicable sentencing guidelines.

[20] TechNews (2005). Retrieved February 20, 2006 from http://www.technologynewsdaily.com/node/1405

The Case of an Energy Processing Plant Engineer

The US Department of Defense reports of an engineer at an energy processing plant, who had a wife that was terminally ill. This engineer had a series of angry and disruptive episodes at work and was placed on probation. A new supervisor took charge of his department and after one his violent outbursts, the engineer was fired.

Days later, the engineering staff discovered that the former employee had made a series of eccentric modifications to plant controls and safety systems. Thereupon, the fired engineer was confronted. The angry former employee withheld the password and threatened the productivity and safety of the plant (US Department of Defense, 1998).

The Case of an International Energy Company MIS Contractor

The US Department of Defense reports of a Management Information Systems (MIS) contractor at the regional headquarters of an international energy company, who had been notified that he was being terminated in part for his chronic tardiness. A week later while he was in his last days of work, he effectively captured and closed off the telephonic switching system for the entire complex.

Upon investigation, the contractor was found to have two prior felony convictions. It was also discovered that he was a member of a notorious hacker group which was as of that time, under investigation by the FBI. Additional investigation revealed that this contractor was the second convicted hacker hired at this site. An earlier case involved computer intrusion at a local phone company. Neither individual had disclosed their criminal histories or had been subjected to background checks sufficient to discover their past criminal activities (US Department of Defense, 1998).

The Case of William Holden Bell

Bell was a senior radar engineer with the Radar Systems Group at Hughes Aircraft in El Segundo, California – a defense contractor. Marian Zacharski was the president of the Polish American Machinery Corporation (POLAMCO). In 1981 during the cold war, Bell was having financial problems and Zacharski – a trained Soviet spy who was posing as a salesman uncovered Bell's financial troubles and took advantage. Whereupon, Bell provided to Zacharski secret drawings and data on the US F-15 Look Down-Shoot Down Radar, TOW anti-tank missile, Phoenix air-to-air missile, and quiet radar. Bell was paid more than $150,000 for facilitating this espionage activity.

This secret technical information neutralized some US military advantages and saved the Soviets approximately $185 million in technological research. It also advanced Soviet technology by about 5 years by permitting them to implement proven design concepts.[21]

The Case of Michael Lauffenberger

The US Department of Defense reports of Michael Lauffenberger, who was a computer programmer for the General Dynamics Atlas Missile Program. He reportedly complained about being unappreciated for his programming work on a parts-tracking system. Determined to make a mark, Lauffenberger planted a "logic bomb" in the system.

Disgruntled Lauffenberger's logic bomb, also called *slag code*, and which is a complex programming code, was designed to execute (or "explode") under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. In effect, it was a delayed-action computer virus or a *Trojan horse*. This logic bomb, when "exploded," was designed erase critical data after he resigned. Lauffenberger reportedly

[21] Vidoefact (2001). Videofact International Documentary Press. Retrieved February 22, 2006 from-http://www.videofact.com/english/zacharski.html

anticipated that he would be called back to rescue the company as a highly paid and valued IT consultant (US Department of Defense, 1998).

The Case of Steven Louis Davis

Davis had been employed by Wright Industries, a Tennessee designer of high technology fabrication equipment which the Gillette Company had contracted to assist in the development of a new high-technology shaving system. Davis was originally assigned as the lead process control engineer for the project but was removed from this position at Gillette's request.

Subsequently, disgruntled Davis sent confidential engineering drawings for the new Gillette shaving system to Gillette's competitors, including Warner-Lambert, BIC (a foreign-owned company) and American Safety Razor Company. Those secret drawings were under the custody of Davis as his duty required. The FBI also learned about another competitor in Sweden who had seen the drawings of the new Gillette system. It wasn't exactly clear who Davis' sponsor was, or if he had one. Davis's 1997 indictments included fraud by wire, theft of trade secrets, stealing and disclosing trade secrets. (PRNewswire, 1997).

The Case of Jay Beaman

Beaman was the Regional PC Manager for King Soopers. Beaman conspired with two other employees to manipulate the computer accounting system to funnel certain purchases into a dummy account. At the end of the day, the perpetrators of this high technology theft would take the amount funneled into the dummy account right out of the cash registers and then delete the account thereby erasing any trace of their scheme. They did this successfully for two years.

Beaman was the spearhead of the scheme and their motives were described by investigators as beginning with financial necessity as illustrated by Beaman's personal financial problems. However his financial necessity quickly escalated into greed and ego. Their hi-tech

fraud cost the company over two million dollars over the two years it took before they were caught. While this was not a case of theft of trade secrets or industrial espionage, it is a hi-tech theft all the same – instigated by a trusted technology insider. There is no doubt that Beaman – a technology expert with access to critical technical operations, and having financial problems, was vulnerable to espionage activities if the opportunity presented itself (US Department of Defense, 1998).

The Case of Zhangyi Liu

The US Department of Defense reports of Zhangyi Liu, a Chinese computer programmer, who was working as a subcontractor for Litton/PRC Inc – a company located in McLean, Virginia. Litton/PRC provided IT and system based solutions for outsourcing, e-businesses, and security programs. Litton/PRC Inc. had been hired by the US Air Force for some technical work. Liu used his insider capacity and computer know-how to illegally access sensitive Air Force information on combat readiness.

Liu also copied passwords, which allowed users to create, change or delete any file on the network. Liu's case was so brazen that he posted some of his escapades on the Internet. The extent of loss in investment dollars or the breach of national security caused by Liu's activities could not be ascertained. Also, what else Mr. Liu did or attempted to do with the secret sensitive technical and defense information could not be determined (US Department of Defense, 1998).

The Case of an Ellery Systems Computer Programmer

Ellery Systems was a small, entrepreneurial company in Boulder, Colorado. They were at the forefront of building the much-heralded information superhighway in the early 1990s. Ellery Systems' specialty, called *distributed computing technology*, provided a link between major telecommunications technologies and computing.

Ellery's innovative ideas were so promising that the US Department of Defense funded the early development of Ellery's technology for intelligence and C3I applications. Ellery was also providing specialized software to NASA and working on developing a library of innovative applications for business and other markets.

On the programming staff of Ellery Systems was a Chinese national. With the knowledge of Ellery's management, this employee went to China to "visit his sick mother." Within days of his return, the Chinese programmer submitted his resignation. The following day, this technical insider transferred, via the Internet, Ellery's entire proprietary source code to another Chinese national working in the Denver, Colorado area. Thereupon, the software was transferred to Beijing Machinery - a Chinese company. The Chinese employee allegedly received $550,000 from a Chinese government-controlled export-import corporation to set up his own software development firm here in the United States to compete with Ellery Systems.

According to Mr. Geoffrey Shaw, former CEO of Ellery Systems, the company could not recover their investment money and was subsequently driven to bankruptcy by foreign competition (even though the foreign competitor physically set up their company here in the US). Mr. Shaw directly attributed the demise of Ellery Systems to the loss of their high-priced source code. Effectively, this act committed prior to the passage of the Economic Espionage Act of 1996 "robbed the U.S. of a competitive advantage in an emerging high-tech industry"

(Keating, 1994). There were no prosecutions.

The Case of Donald Burleson

The US Department of Defense reports of Donald Burleson, who was a computer programmer for USPA & IRA Co - a Fort Worth, Texas securities trading firm. After being reprimanded for storing personal letters on his company-issued computer, Burleson designed a virus in retaliation. He designed the virus to erase portions of the company's mainframe and then repeat the process if a predetermined value was not reset in a specific location. After eventually being fired, Burleson used a duplicate set of keys he had made to return to the facility at 3 o' clock in the morning. Thereupon, he employed an unauthorized backdoor password to reenter the system and unleashed the devastating virus (US Department of Defense, 1998).

INFORMATION SECURITY AND THE PEOPLE FACTOR

The above real (sad) cases are among the thousands of cases over the decades, which demonstrate that sensitive information is vulnerable to compromise by those tasked with their design, maintenance and operation. These inside technology specialists—operators, programmers, networking engineers, and systems administrators. In the military and government security agencies, the perpetrators have included agents and employees. All these are people held positions of unprecedented importance and trust. Malevolent actions on their part have had grave consequences.

It is therefore clear that insider problems already exist within the critical infrastructure of the US Armed Forces, security agencies and technology dependent companies. Furthermore, these government and security organizations, businesses and organizations are at risk from repeat offenders, as perpetrators migrate from job to job; and from position to position. No one knows how many cases have gone undetected.

The military and government security agencies are more thorough in their screening process, but in the business world, the perpetrators are often protected by the lack of in-depth or any background checks at all, constraints upon employers in providing references, and the lack of significant consequences for their offenses. Even the Economic Espionage Act of 1996 has many hurdles in its formulation and dispensation that make prosecution of certain cases to be difficult.

In some of the cases, the perpetrators used their technical expertise, or their insider positions, and access to a critical system or operations to steal or create crises, which would enrich them or magnify their feeling of importance and worth within their organizations.

In response to the increasing recognition of the dangers posed by the insiders in American technology businesses, are looking into espionage cases in military and security agencies with a view to improve their understanding of the personality, motives and circumstances which may make a technology insider vulnerable to stealing or compromising their employers' trade secrets or security. By understanding the basic profiles of the perpetrators and by charting their interactions with the organizational environment as they move over time toward the commission of their crimes, the security professional will have improved understanding of how to deal with the human factor in protecting American technology businesses.

THE ESPIONAGE DATABASE

An unclassified espionage database maintained by the Defense Personnel Security Research Center (PERSEREC) released in the 1990s, provides information on cases going back to 1940. Out of this database, Richards J. Heuer, Jr. of the PERSEREC, and Katherine Herbig of TRW Systems examined 150 cases of U.S. citizens who committed espionage against

the United States since the beginning of the Cold War in the late 1940s. The individuals examined were convicted or prosecuted for espionage or attempting to commit espionage, or there was clear evidence of espionage by the individuals which were available in the public domain even though they were not prosecuted. This latter category included people who defected or fled to another country before they were prosecuted, died or committed suicide before they could be prosecuted. Some of them plea-bargained for lesser charges, or were given immunity from prosecution in return for providing evidence on others.

Five types of information were coded in the database: biographic information, employment and clearance status, the spy's motivation, the espionage act itself, and the consequences of the espionage. Included were details of the espionage offenders' personal and professional lives, their access to classified materials, how they became involved in espionage, and how their careers as spies evolved and ended.

Characteristics of Spies

The PERSEREC contained reasonably complete information on the significant demographic variables for most of the 150 espionage offenders. However, some of the older or more obscure cases were not well reported. Demographic characteristics of the publicly known espionage offenders were as follows.

Gender

Ninety-three per cent (93%) were males and 7% females. Information was available for all 150 cases.

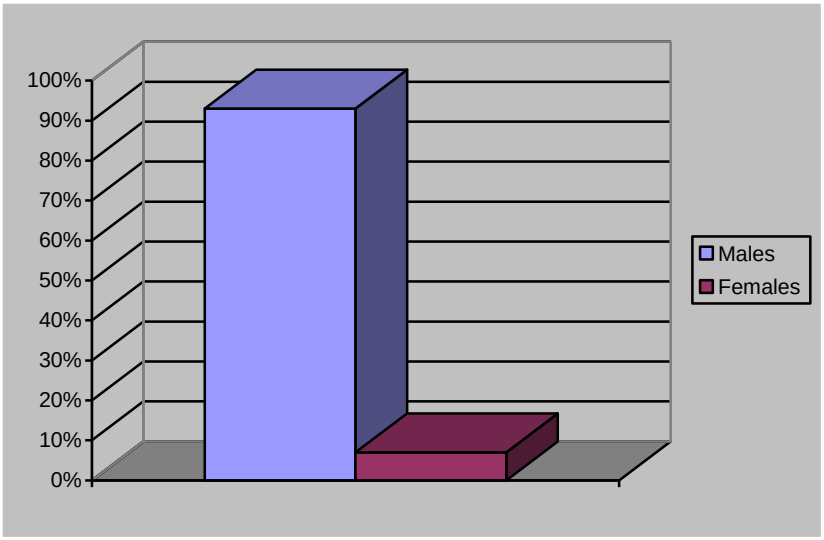

Figure 1: Gender of Spies

Age when Espionage Began

Six per cent (6%) were under 20 years; 40% were 20 to 29 years; 27% were 30 to 39 years; and 27% were 40 years or over. There was a significant difference in ages between civilian and military spies. For the civilians, 44% were age 40 or over at the time they began their espionage. For the military, 57% were 20 to 29 years old when they started. Information was available for 147 cases.

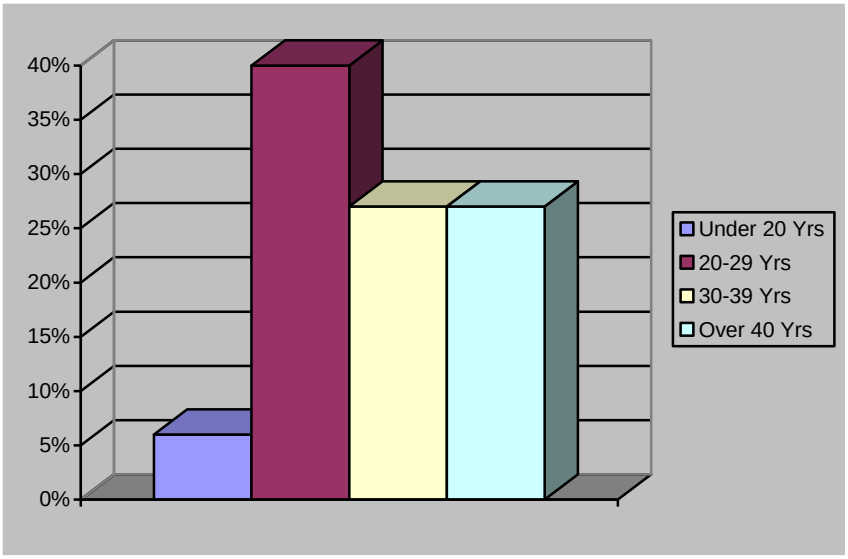

Figure 2: Age When Espionage Began

Marital Status when Espionage Began

Fifty-seven per cent (57%) were married, 33% were single, and 10% were separated or divorced. Information was available for 141 cases.

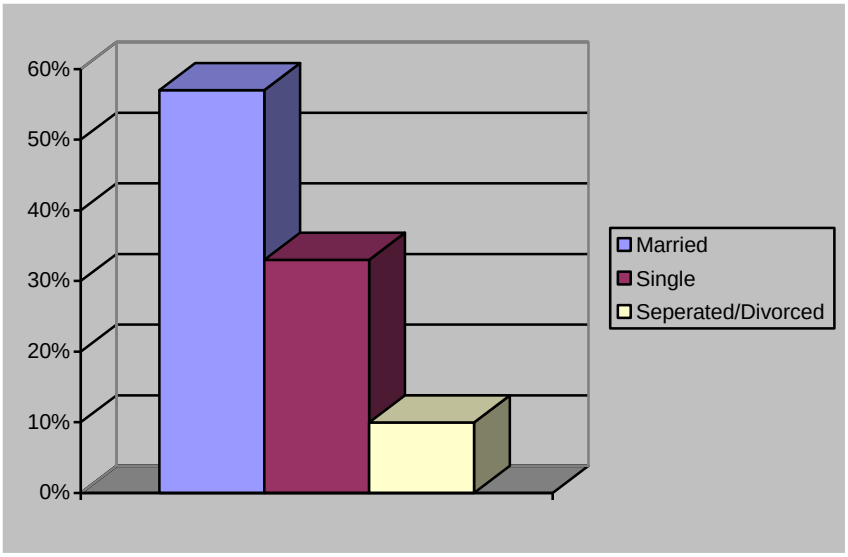

Figure 3: Marital Status When Espionage Began

Race or Ethnicity

Eighty-four per cent (84%) were white, 6% were black, 5% were Hispanic, and 5% belonged to other racial groups. Information was available for 141 cases.

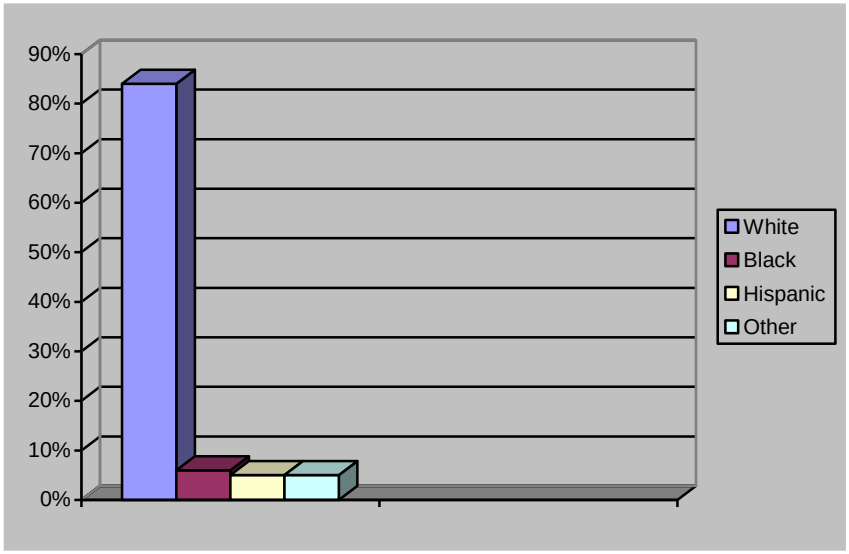

Figure 4: Race and Ethnicity of Spies

Sexual Preference

A majority (95%) was heterosexual and 5% were homosexual. Information was available for 116 cases.

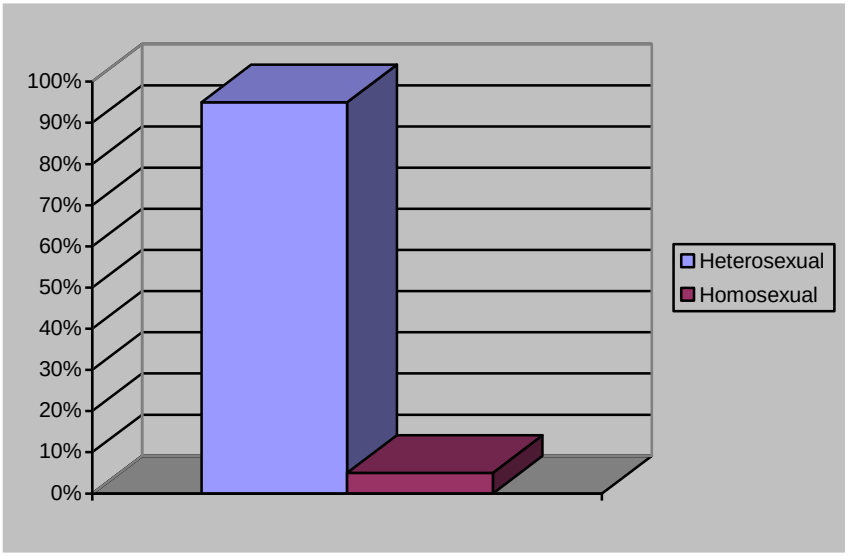

Figure 5: Sexual Preference of Spies

Citizenship

Eighty-three per cent (83%) were born in U.S. and 17% were naturalized US citizens. Most (77%) of the naturalized citizens who became spies were civilians rather than military personnel. Twenty-six percent (26%) of all the civilian spies were naturalized citizens as compared with 8% of the military spies. Information was available for 148 cases.

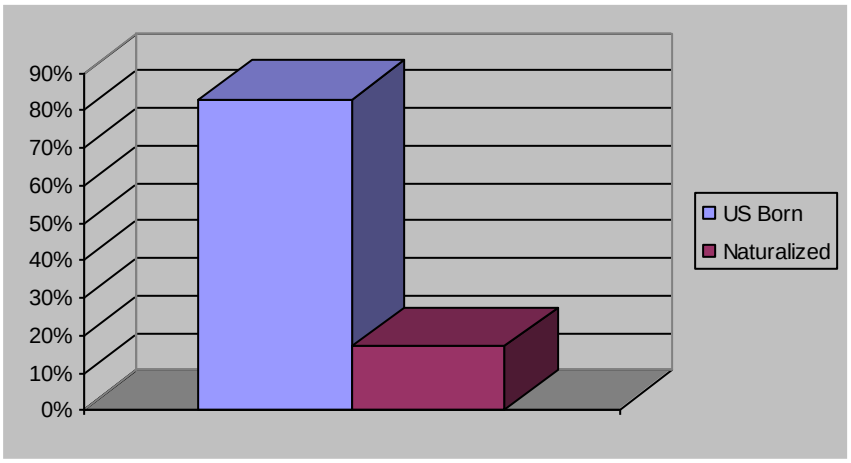

Figure 6: Citizenship of Spies

Education

Seven per cent (7%) had less than high school; 39% were high school graduates; 20% had some college; 20% were college graduates; 14% had at least some work toward their Masters or PhD. Information was available for 133 cases.

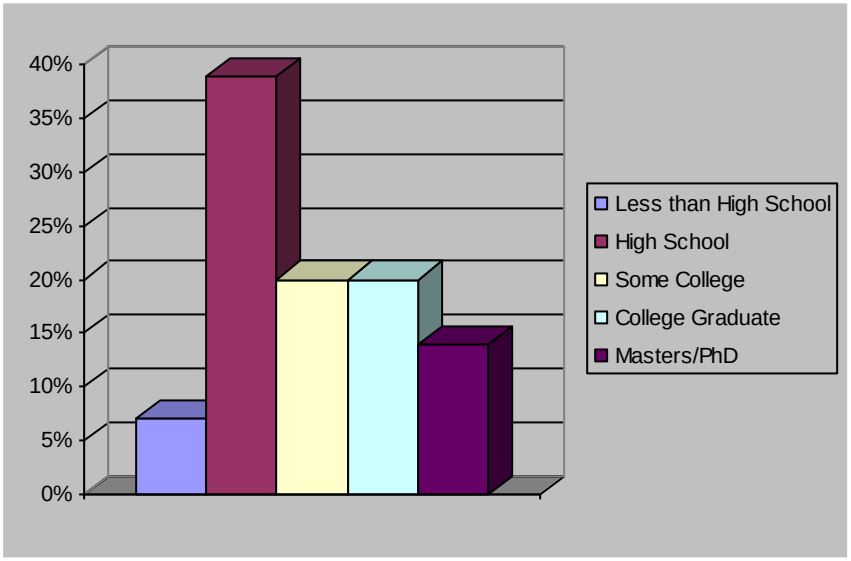

Figure 7: Education Levels of Spies

Type of Employment when Espionage Began

Forty-nine per cent (49%) were uniformed military insiders, 18% were government civilian, 24% were government contractors, and 9% had already left government service or their job was unrelated to their spying. Information was available for 148 cases.

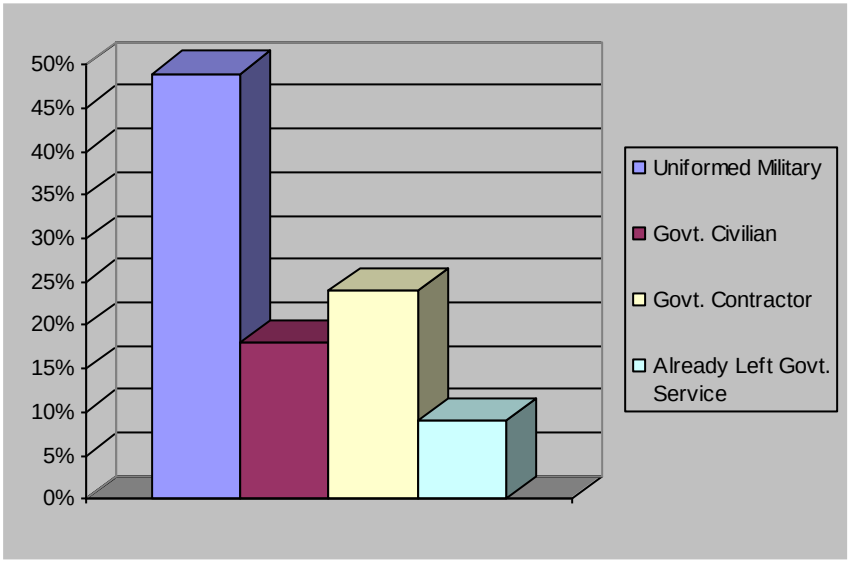

Figure 8: Types of Employment When Spying Began

Rank of Uniformed Military

Nineteen per cent (19%) were E1 to E3; 51% were E4 to E6; 19% were E7 to WO; and 11% were Officers. Information was available for 67 cases.

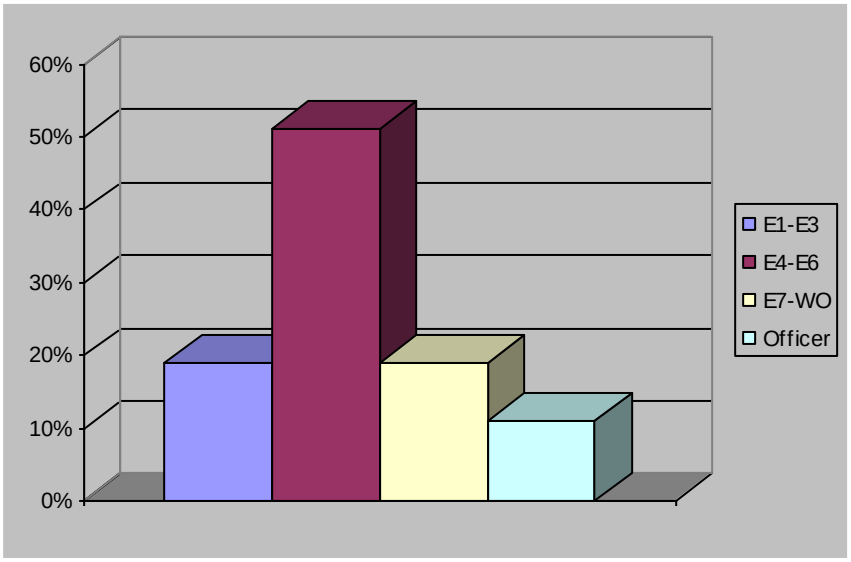

Figure 9: Military Ranks of Spies

Characteristics of the Espionage Activity

The PERSEREC study revealed the following information about the espionage activity. Data was available for most of the cases.

Recruitment

Sixty-four percent (64%) of the spies took the initiative in volunteering their services to a foreign intelligence service. Fifteen percent (15%) were recruited by a friend or family member, most of whom had themselves volunteered, while only twenty-two per cent (22%) were recruited on the initiative of a foreign intelligence service. These percentages differed for different groups. For example, 71% of all military offenders were volunteers, versus 57% for civilians. Seven of the 12

women spies i.e., 58% were recruited by a spouse or boyfriend. Information was available for 148 cases.

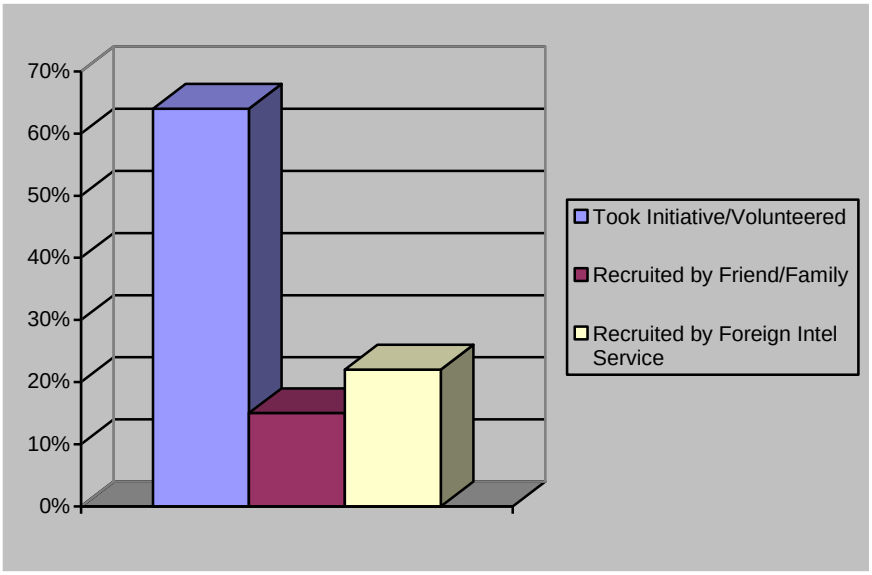

Figure 10: Recruitment of Spies

Motivation

Information on motivation was broken down by categories commonly used when describing espionage offenders, although it is always difficult to know what was really going on in a person's head. One individual may have more than one motivation, so the percentages did not add up to 100%.

Money (either need or greed) was a motivating factor in 69% of the cases, and it was apparently the sole motive in 56%. Disgruntlement or revenge toward employer or some other person or situation was a motive in 27%, and ideology was a motive in 22%. Ideology included beliefs and sympathies resulting from cultural affinity (common ethnic or national background).

A desire to please a friend or family member was a motivating factor in 17% of cases; many of them were cases in which the spy was recruited by the friend or family member. Twelve

percent (12%) were attracted by what they perceived as the thrills or excitement of becoming a spy, while 4% were drawn by a compelling need to be recognized and to feel important. Only 5% were coerced. Thrills or excitement and need for recognition were, in most cases, supporting rather than primary motivations. Information was available for all 150 cases.

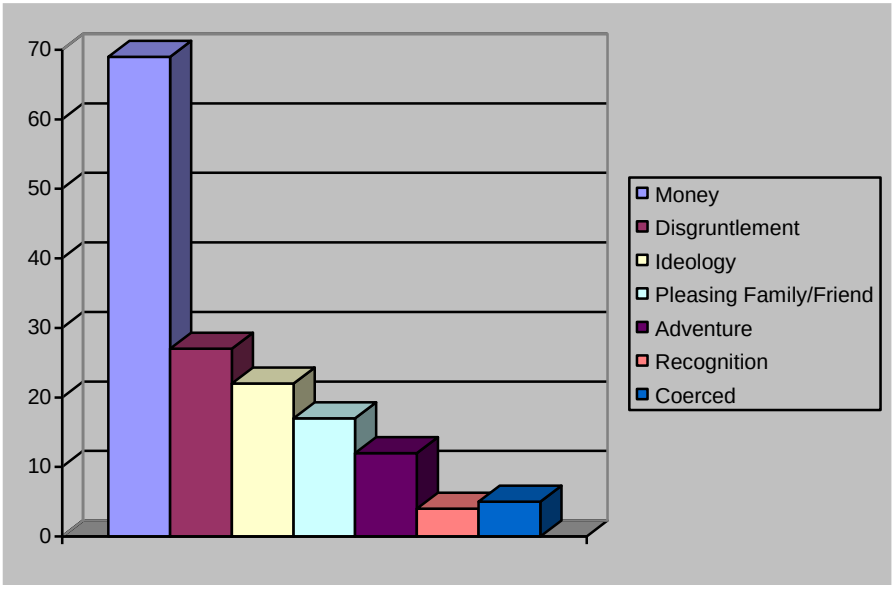

Figure 11: Motivation of Spies

Unsuccessful Spies

Thirty-nine offenders (26% of all those who attempted to commit espionage) were unsuccessful.

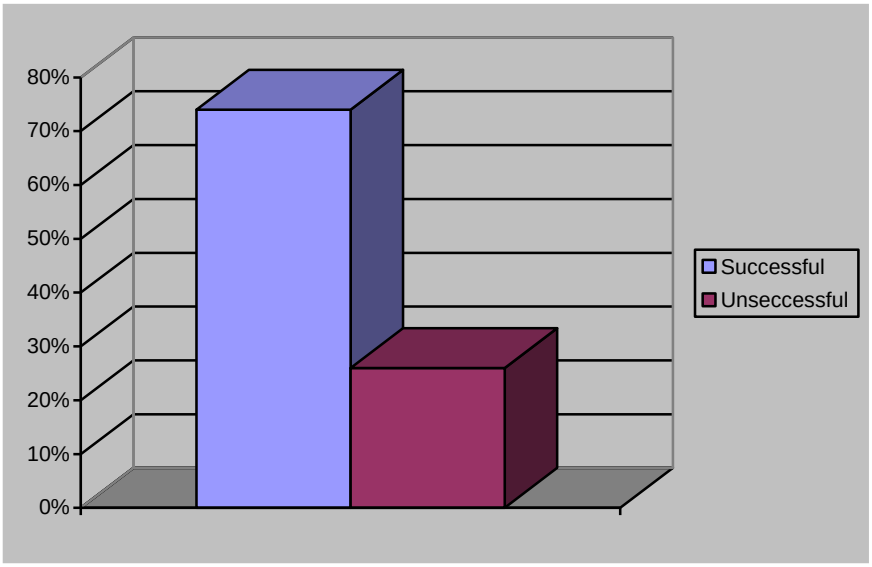

Figure 12: Success of Spies

The unsuccessful spies were arrested before they succeeded in passing classified information to a foreign country. Of the 39 would-be spies who were caught before they could do any damage, 69% were military personnel, mainly young, unmarried, enlisted personnel with no more than a high school education. All were native-born American citizens motivated mainly by the simple idea that selling secrets would be an easy way to get some money. Interestingly, over 60% of the military personnel in this category were in the Navy.

Length of Espionage

Of the 111 spies who succeeded in passing information to a foreign country, 27% were caught in less than one year. Forty-four per cent (44%) lasted more than one year but less than five, while 29% remained undetected for five years or more.

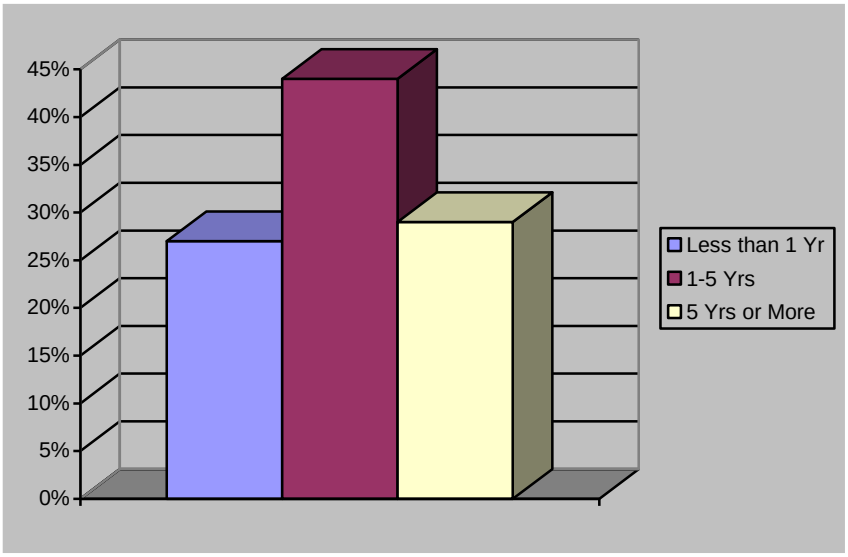

Figure 13: Duration of Espionage Activities

Security Clearance when Espionage Began

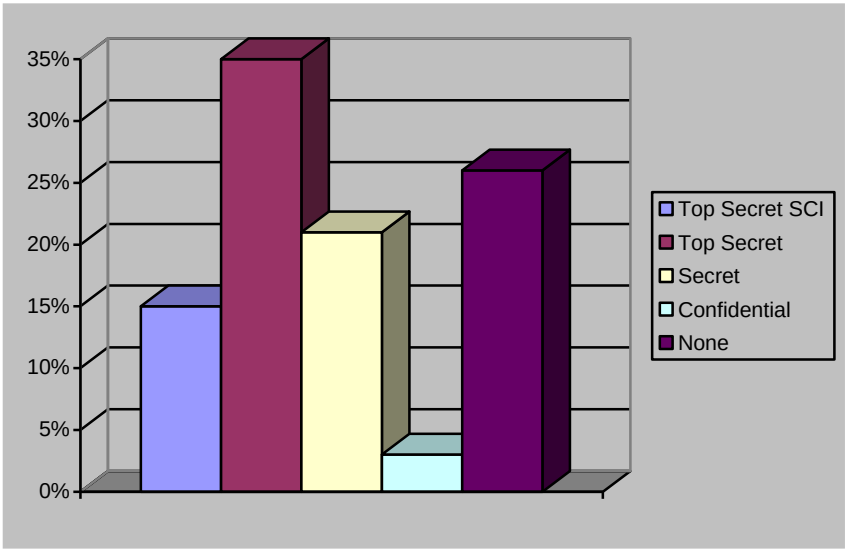

Figure 14: Security Clearance When Espionage Began

Fifteen per cent (15%) of the spies held a Top Secret SCI clearance at the time they began committing espionage. Top Secret clearances were held by 35%, Secret by 21%, and Confidential by 3%. Twenty-six per cent (26%) held no clearance at all. Those with no clearance included accomplices, witting spouses, those who provided classified information obtained during a previous job when they did have a clearance, and those who provided sensitive but unclassified information. Information was available for 141 cases.

Where Espionage Began

Sixty-six per cent (66%) of espionage cases began in the United States, with a large majority of those on the East Coast. Of the 34% that began outside the United States, 66% began in Western Europe (mainly West Germany). This equates to 22% of the entire espionage cases. Twenty (20%) of the 34% of cases originating outside the US originated in Asia or Southeast Asia. This equates to 7% of the entire espionage cases. Five per cent (5%) of the case originated elsewhere. Information was available for 146 cases.

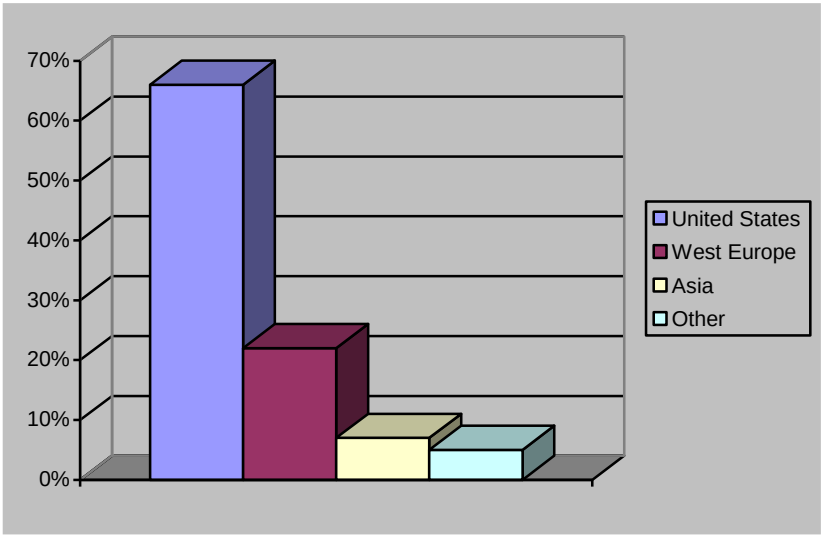

Figure 15: Where Espionage Activities Began

Country Receiving Information

During the Cold War, most espionage was conducted by the Soviet Union and associated Communist countries in Eastern Europe. The surprising thing was that many other neutral or allied countries – rich and poor, friend and foe alike were also involved in espionage against the United States. American citizens were arrested for conducting espionage on behalf of South Korea, Taiwan, Philippines, Israel, Netherlands, Greece, Saudi Arabia, Egypt, Iraq, Jordan,

Ghana, Liberia, South Africa, El Salvador and Ecuador. Information was based on the 111 cases in which offenders succeeded in passing information.

Espionage Target

Information from the following organizations was compromised, or, in the case of unsuccessful espionage attempts, was intended to be compromised. The number after each organization was the number of offenders who targeted that organization. Navy, 38; Army, 32; Air Force, 22; CIA, 16; Defense contractors, 15; NSA, 7; State, 7; FBI, 4; Marines, 4; DoD civilians, 4; DIA, 2; INS, 1.

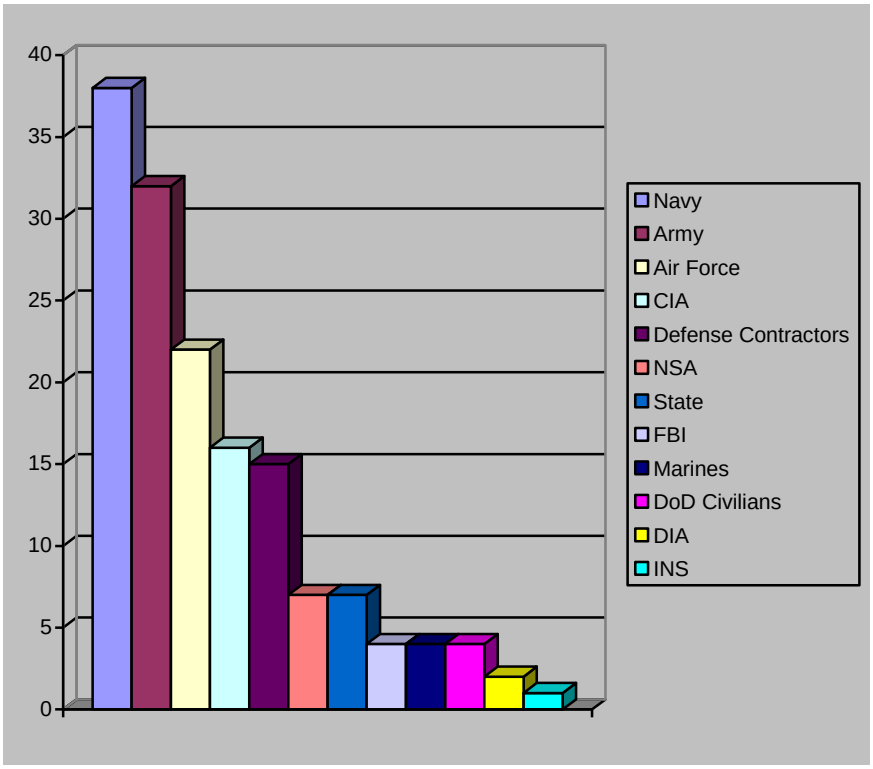

Figure 16: Targets of Espionage

Six offenders compromised materials from more than one agency and were, therefore counted more than once. Information was available for 146 cases.

Payment Received

Although money topped the list of motivations for espionage, as shown in Figure 17, it was interesting to see how few spies received significant payments. Most foreign intelligence services were obviously mistrustful of volunteers and were tight with their money, except in the most important cases.

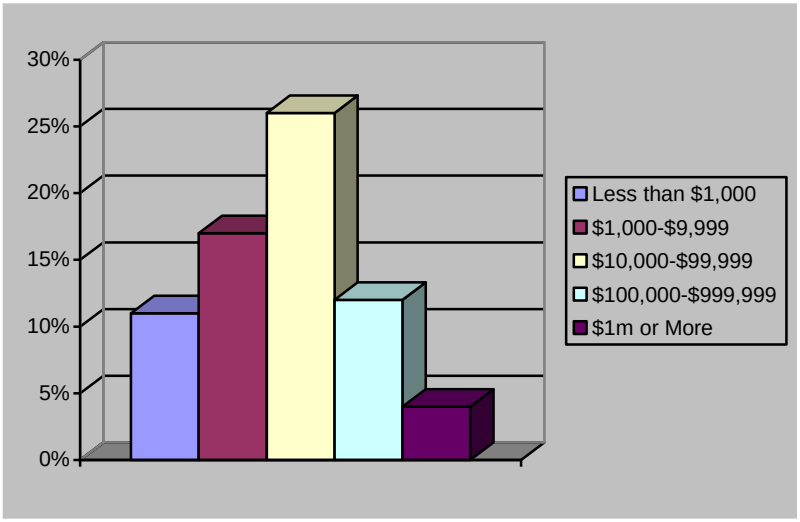

Figure 17: Payments Received for Espionage Activities

Most spies received relatively little, despite the high risk of getting caught and the monumental cost of espionage to the nation. Of the 111 cases in which spies succeeded in passing information to a foreign intelligence service, information on payments was available for 92 cases. Sixty-four of those received some monetary payment, while 28 were believed to have received no monetary payments.

Offenders who received no monetary payment included those who provided information after defecting to the other side, women who helped their husbands or boyfriends, some who appeared to have been motivated only by a desire to help the other country, and others who

sought some non-monetary quid pro quo such as help for a local business, post-retirement employment in the country that received the information, or release of a spouse from prison.

Of the 64 spies known to have received cash payments, 11% received less than $1,000; 17% received $1,000 to $9,999; 26% received $10,000 to $99,999; 12% received $100,000 to $999,999; while 4% received $1,000,000 or more.

It is noteworthy that some of these payments were made as long as 66 years ago, and that the payment figures were not, and have not been, adjusted for changes in the value of the dollar over the years. The numbers also represent only the amount that the spy was known to have received. Most observers believe that after their arrest, spies often try to minimize the amount of money they received in an effort to minimize their crime.

Length of Sentence

The percentages for each initial sentence length were as shown in Figure 18:

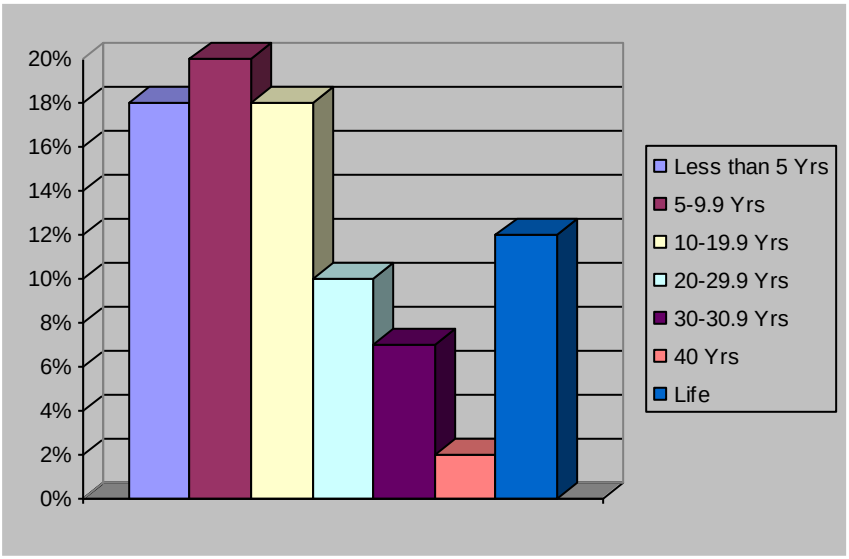

Figure 18: Length of Sentence for Espionage Activities

Sentences for 18% were less than 5 years; 20% received 5 to 9.9 years; 18% received 10 to 19.9 years; 10% received 20 to 29.9 years; 7% received 30 to 30.9 years; 2% received 40 years; and 12% were sent away for life (some without the possibility of parole). Sentencing information was available for 127 cases. Twenty cases were known to have had other outcomes such as defection, suicide, or immunity from prosecution.

Date Arrested or Exposed

Five spies were arrested or otherwise publicly exposed during the decade of the 1950s. This increased to 13 in the 1960s and 13 in the 1970s. Arrests and other public exposures mushroomed to 56 in the 1980s and remained at a high level, with 29, in the 1990s. Information was available for all 150 cases.

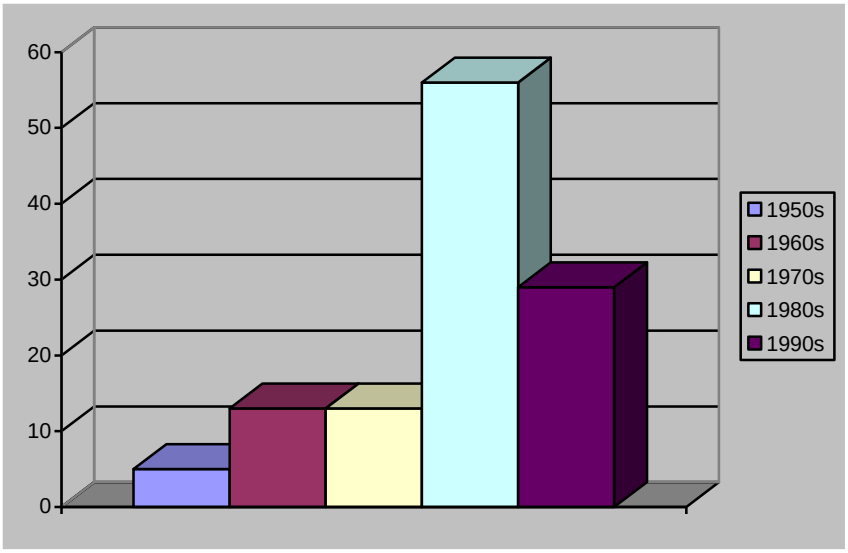

Figure 19: Dates Arrested or Exposed

Large variations in the number of arrests from one time period to another may be determined more by the nature of the counterintelligence sources and tools that were available during a given period than by changes in the prevalence of espionage.

The 1980s have been called the Decade of the Spy (Allen, 1996; Lynds, 2006). This is because of the high number of successful spies exposed during that period. However, it was also the decade of the *unsuccessful* spy. Many young, unmarried military enlisted personnel were caught before they succeeded in selling any secrets. Of the high number of cases in the 1990s, many were successful spies exposed by sources that became available after the end of the Cold War.

Indicators of Security Risk in Espionage Against the US Military and Security Agencies

The Defense Personnel Security Research Center (PERSEREC) analyzed past espionage cases to determine the prevalence among spies of behaviors or circumstances often considered indicative of potential security risk. This was essential because, government decisions to approve or disapprove security clearances for access to classified information are normally based on a set of thirteen Adjudicative Guidelines.[22] These guidelines cover behaviors commonly associated with security risk, such as alcohol and drug abuse, criminal behavior, emotional or mental problems, financial problems, and vulnerability to foreign influence.

Behavioral information was reported in the publicly available sources only if its presence or absence was particularly noteworthy, or if the case was an important one that received in-depth media coverage. As a result, information on behavioral indicators of potential security risk was available for only a portion of the cases.

[22] On April 6, 2006, the testimony of Harold J. Kwalwasser (Deputy General Counsel for Legal Counsel of the Department of Defense (DoD)) before the Senate Armed Services Committee hearing to review procedures and standards for the granting of security clearances at the Department of Defense, which discussed various issues raised by the senate regarding the personnel security process at DoD raised serious questions rather than provide answers to the consistency of application of adjudication guidelines by DOD's adjudication facilities, particularly at the Defense Office of Hearings and Appeals (DOHA); and the implementation of peer review to assure consistent application of the guidelines throughout the DoD adjudication facilities.

Alcohol Abuse

An offender was considered to have engaged in "excessive alcohol use" if he/she was described in one or more open sources as having an alcohol problem, being a heavy drinker, or having been under the influence at the time of first contact with a foreign intelligence service.

Forty offenders from the PERSEREC study reportedly used alcohol to excess. This was 27% of all offenders or 51% of the 79 cases for which information was available about alcohol use. These were minimum figures. It is quite possible that some of those for whom no information was available on alcohol use actually had an alcohol problem.

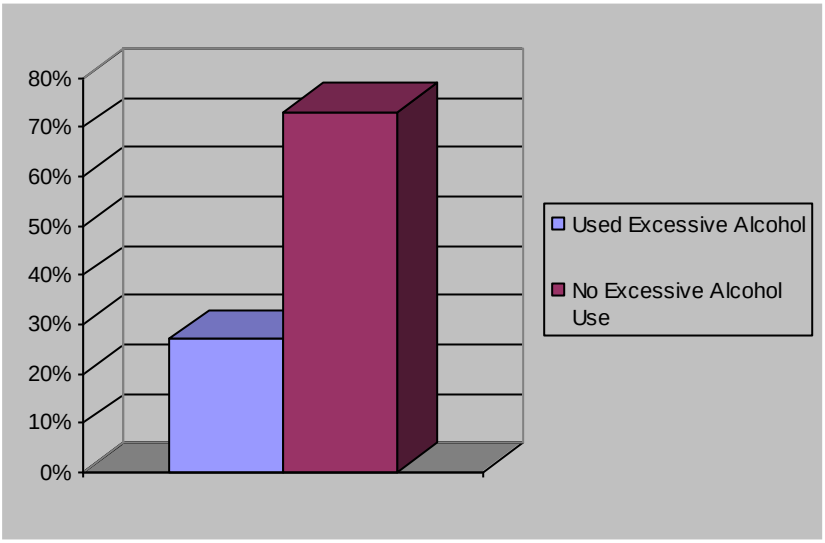

Figure 20: Alcohol Abuse Characteristics of Spies

Drug Abuse

The numbers on illegal drug use were similar to those for excessive alcohol use. Information was available for 76 of the 150 cases. Of those cases for which information was available, 53% of the subjects engaged in illegal drug use while 47% reportedly did not. The current relevance

of such statistics on drug use is uncertain, as the prevalence of drug use, especially within the military, has varied greatly over the years.

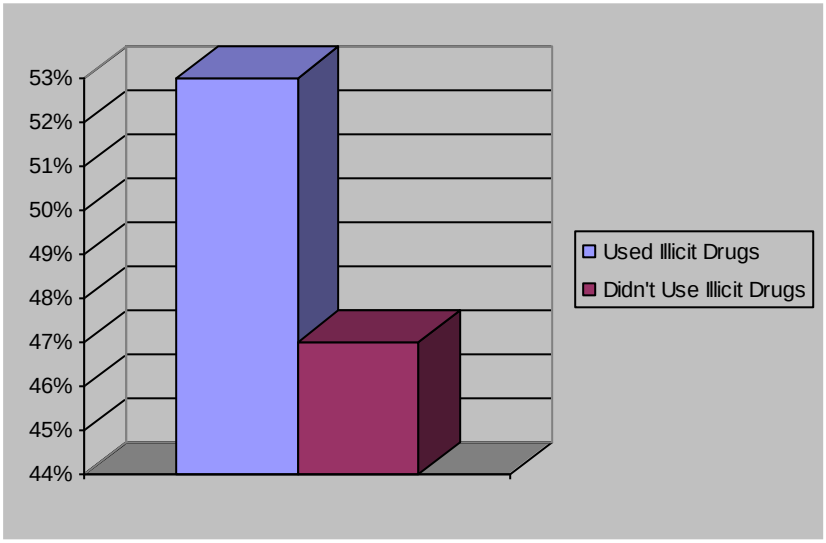

Figure 21: Drug Abuse Characteristics of Spies

Spending Inconsistent with Known Income Level

Spies who obtain significant amounts of money may be tempted to spend their illegal income in ways that attract attention to their unexpected or unexplained affluence. To examine this subject, the PERSEREC study looked at the 64 cases in which payment was received. In 23 of these cases (i.e., 36%), the offenders were reported to have demonstrated financial affluence not consistent with their known income.

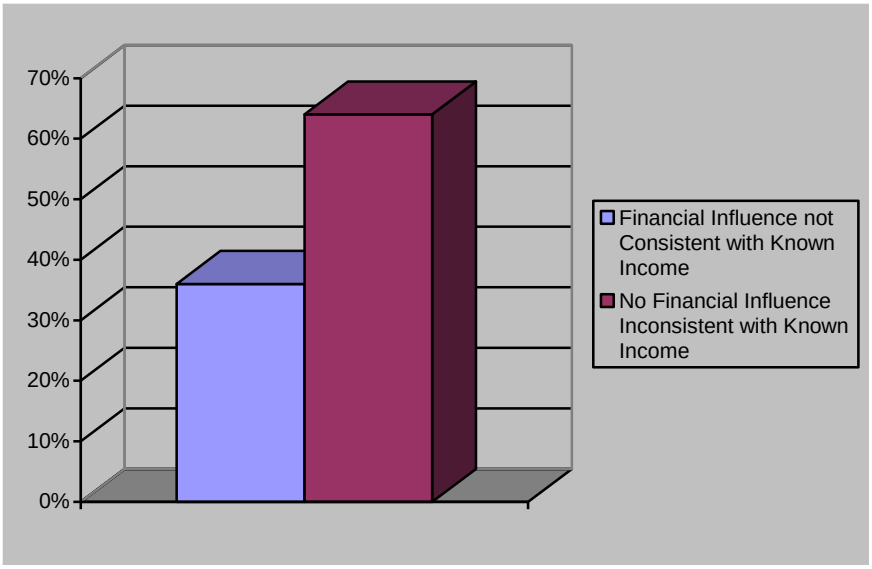

Figure 22: Spending Characteristics of Spies

For the 26 cases in which the spy was paid $40,000 or more, unexplained affluence was reported in 20 cases (i.e., 77%). As usually happens, unfortunately, this information was not known until after the offender was arrested.

Foreign Interests

The national guidelines governing adjudication of security clearances required consideration of any foreign relationships that may make an individual potentially vulnerable to coercion, exploitation, or pressure. This included foreign attachments such as family ties, other emotional attachments or obligations to foreign persons, and financial, business, or professional interests abroad.

In security management, there is concern that conflicting loyalties or conflicts of interest can make a person vulnerable to foreign pressure. A large percentage of offenders had foreign backgrounds or connections as follows (note that many offenders belonged to more than one category. Thus, the numbers did not add to 100%):

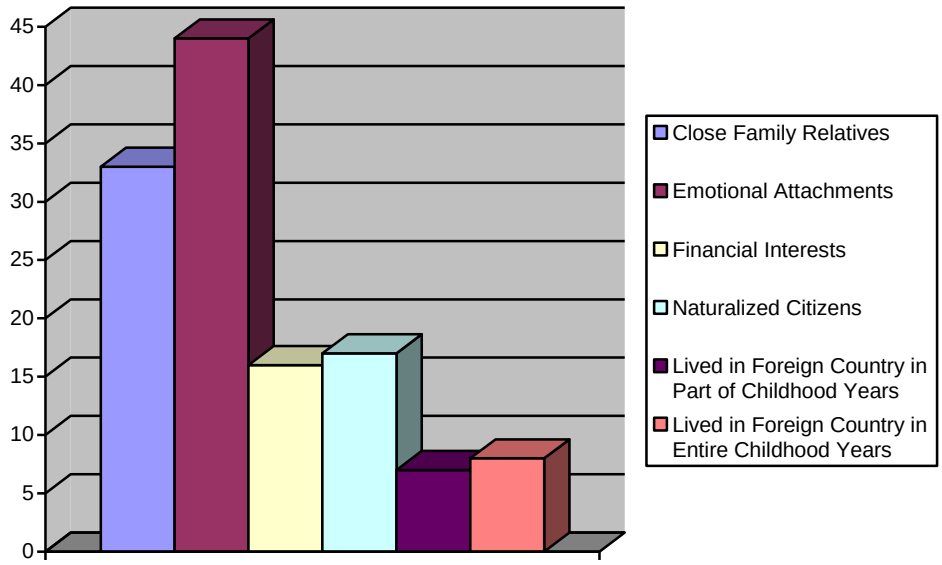

Figure 23: Foreign Interests of Spies

At least 33% had close foreign relatives. In many cases, the relative was a relative of the spouse, not of the offender. At least 44% had emotional attachments to foreign persons such as spouse, fiancée, lover, friend, or relative other than a parent or sibling. At least 16% had foreign financial, business, or professional interests. At least 17% were naturalized citizens. At least 7% lived in a foreign country during part of their formative childhood years, and an additional 8% during their entire childhood.

For analytical purposes, offenders with foreign relatives, foreign emotional attachments of various types, and foreign financial, business, or professional interests were combined as a group called offenders with foreign interests. This group included 76 (51%) of the offenders.

These offenders with foreign interests can be compared with offenders who had no such interests. Those with foreign interests were more likely to have been recruited directly by a

foreign service than those without such background or connections (41% versus 32%), and less likely to have volunteered their services to a foreign intelligence service (59% versus 66%). Of the 76 offenders with foreign interests, foreign relatives played a role in recruiting 26% of them.

Offenders with foreign interests were significantly more likely than other offenders to have been motivated by ideology (34% versus 10%). Recall that in this context the term ideology included a set of beliefs based on common ethnic or national background. On the other hand, they were less likely to have been motivated by money (61% versus 78%).

EXPLORING INSIDER PERSONAL AND CULTURAL VULNERABILITIES OF IT INSIDERS

The PERSEREC studies indicate that many military and security personnel have used their positions to both commit and cover up their espionage activities. So also, many technical experts in American IT companies have used their positions to both commit and cover up their fraud or espionage activities. This emphasizes the vulnerability of technology organizations to trusted technical employees. The fact that only a handful of cases are uncovered and/or reported (or declassified) makes this more worrisome.

Some of the cases also illustrate the problems posed by poor screening measures and the vulnerability of organizations that outsource their technology functions. The cases also demonstrate the espionage threat posed by IT contractors, though the motivations of some of these perpetrators may not be very clear.

Some of the cases also emphasize the complex issues of loyalty in an international environment. Ellery Systems was killed by a Chinese national who allegedly had Chinese government support. Mr. Shin-Guo Tsai, the former design engineer with Volterra transferred secret data to a Taiwanese competitor. He was from Taiwan. Whereas many US technology

companies have benefited greatly by employing foreign talents, these sample cases nonetheless illustrate the fact that foreign connections of IT specialists can increase their vulnerability to recruitment, manipulation, or independent hostile action.

Other cases involve employees who take advantage of their position of trust for financial gain. They demonstrate hackers who were employed within the critical technology infrastructure caught engaging in unauthorized explorations. Other perpetrators included individuals who entered the technology organizations with the explicit intent to commit espionage, fraud or embezzlement. Overall, observers and investigators report that the number of technology-related offenses committed by insiders is rising rapidly each year.

Finally, just as in organizations outside the critical technical infrastructure, the range of potential perpetrators and their motivations is broad. In many cases, as in the cases of Mr. Donald Burleson, the computer programmer for USPA & IRA Co. and Mr. Steven Louis Davis of Wright Industries, acts of computer sabotage and extortion have been committed by disgruntled employees who are angry about lay-offs, transfers, and other perceived grievances.

The Defense Personnel Security Research Center (PERSEREC) study shades substantial light into the characteristics of spies. No doubt, this can be very beneficial to US technology firms in dealing with industrial espionage, in which insiders are participants.

Analyses of the previous cases in American technology companies also show that there is a subset of technology specialists who are especially vulnerable to emotional distress, disappointment, disgruntlement, misplaced loyalties and consequent failures of judgment. These traits or conditions can lead to an increased risk of damaging acts or vulnerability to recruitment or manipulation by industrial spies. Moreover, there are characteristics of the so-called "information culture" which enhance this vulnerability.

It is not, and was never, the purpose of this study to cast suspicions on an entire professional category of professionals whose role in the modern technology-based economy

has become so critical. The majority of these technology professionals are honest. It is always the dishonest few that cause the big havocs. Nonetheless, it is crucial to understand the motivations, psychological makeup, and danger signals associated with those technology insiders who pose a threat to American businesses and security. This will be crucial in addressing the problem of theft of trade secret, industrial espionage or mischief.

As seen form the Defense Personnel Security Research Center (PERSEREC) research, and by logical reasoning, there can be a reasonable conclusion that there are several characteristics which, when found together, increase this vulnerability of a technical insider toward illegal or destructive behavior. Major among the characteristics include substance abuse, excessive introversion, unbecoming activism, financial difficulties, social problems and personal frustrations, flirtation, grandiosity, moral elasticity, reduced loyalty, having a sense of entitlement, lack of empathy, having a history of previous dangerous acts, and revenge.

Substance Abuse

Computer programmers, systems analysts and IT insiders are no different from other employees or associates with regard to their susceptibility to illicit drug use or alcohol abuse leading to loss of judgment and destructive acts. Some employees who quietly suffer alcohol abuse or drug dependence may never compromise security, but this should never be left to chance.

The PERSEREC studies show that substance abuse can be a serious security risk. Twenty-seven per cent (27%) of all cases with substance abuse data abused alcohol and 53% used and abused illicit drugs. For example, Ames’s uncontrolled behavior while under the influence of alcohol was, at least in retrospect, a clear indication of potential security problems. The list of alcohol abuse incidents by Ames was significant not so much for what it told about Ames' alcohol use, as for what it told about Ames as a person -- his irresponsibility and lack of

self-control. His record of alcohol abuse certainly indicates that he should have failed the official criteria for a security clearance -- that he be "stable; trustworthy; reliable; of excellent character, judgment, and discretion."[23]

Although no information was available for the IT espionage or related cases examined in this report, drug and alcohol abuse cannot be ruled out. Only one breach can bring down a whole company.

Excessive Introversion

Computer programmers, systems analysts, programmer trainees, and computer science students are overwhelmingly represented by introverts (Pocius, 1991). They are oriented toward the inner world of concepts and ideas rather than the outer world of people. These IT people enjoy being alone. They find solace with their computers and e-mail. On their vulnerability to e-mail elicitation, Nolan (1999, p.236) observed: “they appeared to have little else in the way of a life” other than e-mail.

They prefer their own thoughts to conversation with others and may be socially unskilled. Peter Cullins, the director of the Management Information Systems (MIS) department at the Retired Officers Association in Alexandria, Virginia admits it: "Most of the people in my department are introverts, myself included. People that crave conversation and human interaction don't last long programming computers. You need people that want to crawl inside a program and not come out until it's working" (Livingood, 1995, p8). They also tend to be over-conscientious and secretive. They are pessimistic and as the scientists they are, extremely critical.

[23] See “Personnel Security Standards”, #5(d) of the Director of Central Intelligence (DCI) Directive 6/4: Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI); July 2, 1998. Retrieved from http://www.fas.org/irp/offdocs/dcid6-4/index.html on October 14, 2006

In a nut shell, the particularly introverted among this subset of people have a special preference for individual intellectual pursuits as opposed to interpersonal activities. This means that the signs of employee disaffection which would be apparent for other employees may not be so readily visible in these excessively introverted employees – the group to which most technology experts belong. Their expressions of displeasure may only occur, in fact, on-line. So, a particularly introverted technology professional poses serious challenges to security management.

Unbecoming Activism

The antithesis of excessively introverted IT specialists and/or insiders is those that become spirited IT activists. Quite often, disagreements occur over how an organization designs and runs its IT infrastructure or that of a client. The IT professional may feel one way and management may have a different idea. Egos may be challenged or personal beliefs or preferences may be required to be trounced. Loyalty to ethical, political or social beliefs and allegiances may be threatened. The IT insider may cause disruptions as revenge or to prove his or her point.

A lesson can be leaned from the Case of Morison, the former worker at US Naval Intelligence Support Center, convicted of espionage and theft of government property in 1985, and pardoned by President Clinton in 2001. Morrison was reportedly motivated not only by a desire to curry favor with Jane's to increase his chances of being offered a job, but who also had a political motive for passing classified information to the media -- to influence American public opinion in favor of a stronger defense posture. He reportedly believed that the new nuclear-powered aircraft carrier, the photos of which he passed on to Jane’s, would transform

Soviet capabilities, and that "if the American people knew what the Soviets were doing, they would increase the defense budget."[24]

Also consider the Case of Ana Belen Montes, who was a senior intelligence analyst at the Defense Intelligence Agency (DIA) and spied for Cuba. Her lawyers claimed she spied from sympathy toward Cuba and that she received no money for her espionage other than travel expenses and the cost of her laptop. At the sentencing hearing she reportedly made a defiantly unrepentant statement condemning US policy towards Cuba. One may wonder if none of her colleagues ever heard her express sympathy for Cuba.

Financial Difficulties

An employee, let alone a technology specialist who has access to critical information and who is obviously having financial troubles is a cause for worry for the security manager. This is especially so if that specialist is losing work time due to online gambling or he is gambling to obtain money for debts or is borrowing money to finance gambling.

Whereas, one individual may have had more than one motivation to steal trade secrets, money (rising out of either need or greed) was a motivating factor in 69% of the cases examined by Herbig (2005). Financial difficulties may also emanate from divorce, ostentatious living or tragedy in the family.

In the PERSEREC studies, money (either need or greed) was a motivating factor in 69% of the cases, and it was apparently the sole motive in 56%. Consider the Case of Regan, the former US Air Force technical insider. Regan was thought to have been motivated not only a sense of disgruntlement, complaining frequently to former coworkers and neighbors about his job and station in life, but by money (he had very heavy personal debts).

---

[24] See “Samuel Loring Morison” at Wikipedia Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Samuel_Loring_Morison on October 14, 2006

Also consider the Case of former FBI agent Hanssen. Although Hanssen's motives were unclear, they seemed to have included not only ego gratification and disgruntlement with his job at the FBI, but a need for money. He and his wife reportedly struggled to provide for his large family on an agent's salary. By 1992, Hanssen had incurred debts of over $275,000. Friends and coworkers were reportedly at a loss to explain how this supposedly deeply religious father of six and ardent anti-communist could have been leading a double life. A large part of his illegal income was believed to have been used to buy expensive gifts and a car for a local stripper.

The Case of Faget, the former high-ranking Immigration and Naturalization Service (now US Citizenship and Immigration Services), who was convicted of providing classified information to the Cuban intelligence service also shades light into money as a major motivator for espionage. Prosecutors reportedly stated that Faget's motives were financial gain rather than political. Faget was said to have expectations of engaging in a lucrative trading business with Cuba once the US embargo is lifted.

Ironically the technology specialist undergoing financial difficulties may suddenly become a workaholic: never taking vacations and unusually working late into the night and at weekends. He may become very protective of his domain and get startled whenever someone approaches his desk. These may be additional danger signs. Routine credit checks of their technology insiders (if not for all employees) may be a good idea for US technology firms. This is because credit checks reveal financial pictures of individuals.

Social Problems and Personal Frustrations

Technology specialists can feel frustrated and angry with friends or co-workers due to conflicts and disappointments in their lives or at home. Shaw et al. (1998) report a 1993 study by Professor R. Coldwell where technology specialists preferred the predictability and structure of work with computers to the lack of predictability and frustrations of relationships with others.

These experiences appeared to leave them with a propensity for anger, especially toward those in authority and the entire organization.

These traits create an increased vulnerability to feelings of alienation, disgruntlement, and disappointment on the job. Not only are such technology specialist employees more likely to have inherent bitterness towards their jobs or supervisors, but they are less likely to trust and to deal directly with authorities when problems arise. In turn, these characteristics may also make some of these technology employees more vulnerable to recruitment and manipulation by industrial spies. Substance abuse may exacerbate these tendencies.

Flirtation

One of the major weaknesses of men is sex and there is a specific type of espionage that uses sex as its primary tool. Once the potential source has succumbed to the sexual manipulations of the collector, he or she is trapped. Blackmail and intimidation may follow. The operation is called the "honey pot."

Those who encounter a "honey pot" are tempted by the seemingly irresistible sweetness of sex. They are often ensnared in the sticky web of sin – the lust of the flesh. Indeed, many successful espionage activities have been pulled off using sex. Russia and China are frequently reported to be targeting American (and Japanese) technology companies (and even their national intelligence officers and diplomats) using sex frequently.

A technology professional who is seen to be flirting and womanizing especially with foreign women (or men, if the IT specialist is a woman, or is gay) is a cause for concern for the security manager. Such a technology professional can easily be wooed and trapped by sex. What makes this problem especially difficult to combat is that people feel reluctant to disclose that they made a mistake out of personal embarrassment, not realizing the security implications that are associated with their decision making.

Grandiosity

In the IT culture, there appears to be a feeling by some, that they are above the rules, that security and other mundane procedures followed by others did not merit their attention since they are the ones who design and maintain the programs. These are more of cases of grandiosity than stealing or engaging in espionage. Nonetheless, this poses substantial security risks.

Lessons can be learned from the Case of Ames. In 1976, while on his way to meet a CIA source in New York, Ames reportedly left a briefcase of classified materials identifying the source on a subway train. Although the briefcase was ultimately recovered by the FBI, it might well have compromised the source. In 1980 he left Top Secret communications equipment unsecured in his office.

In Mexico City during 1981-1983, Ames reportedly failed to report his "close and continuing" intimate relationship with a foreign national, Rosario Casas Dupuy, who later became his wife. In 1984, he used poor judgment by bringing his then-mistress, Rosario, to CIA operational housing where CIA undercover officers were staying. In 1985, while assigned to the debriefing of Soviet KGB defector Vitaliy Yurchenko, Ames violated security by taking his mistress to the safe house where Yurchenko was staying. Also in 1985, he had a security violation for leaving his safe open.

In Rome from 1986 to 1989, he was known to prepare classified reports at home on his personal computer. He often left the safe open when leaving for the day, and he ignored security regulations that require reporting of all foreign travel.

An IT insider who exhibits such characteristics of utter disregard for security or company procedures should be a source of serious concern to his or her organization.

Moral Elasticity in the IT Culture

Morality has been stretched to frightening limits within the IT world. There have been concerns about looser moral boundaries within the so-called "IT culture." Recent studies of current computer technology professionals indicate the presence of a subgroup whose members do not see anything wrong with acts of wanton deciphering, cracking, espionage and sabotage against information technology systems. To these people it's sometimes simply a game.

Many IT professionals appear to maintain the position that if an electronic asset is not sufficiently secure, and then it is fair game to attack it. They blame it on the designers. According to Shaw et al. (1998, p.10), "the disturbing aspect of these findings is the association between decreased ethical constraints and youth, suggesting that this perspective may be shared increasingly among new and future employees."

Among several other outrageous ways of thinking, technology specialists have assumed the idea that breaking into; exploring and even copying files belonging to others inflicts no real damage since nothing physical was stolen. They have thus rationalized what would otherwise be considered incursion, infringement or theft.

Although the IT industry has established some ethical principles over the past few years, they have been implicated in the erosion of their own ethical standards. Some critics cite the hiring and promotion of former known hackers. This practice seems to have sanctioned hacking and even produced an incentive for this criminal behavior. A technology specialist who has the mind frame of seeing nothing wrong in invading other people's networks poses a real danger to the security of his organization, especially when combined with other traits.

Reduced Loyalty

Although the demand for technology specialists has considerably shrunk since the 1990s due to “oversupply”, those who have become versatile have continued to see a boom in their demand and pay. In fact, according to Diane Morello of Gartner Research, "businesses will increasingly look to employ IT versatilists - employees who not only specialize in IT but who demonstrate business smarts by handling multidisciplinary assignments.”[25]

The fact is that these versatile technology specialists are still in high demand – and they know it. Their high demand has also explained the continued high rates of turnover in the profession. The loyalty of these professionals to their companies has thus been greatly impeded since they know that there are other organizations ready to hire them sometimes for bigger pay. The resulting pressures to hire and retain versatile IT professionals have thus placed tremendous pressure on the information security process.

The resultant weak bond many of these specialists have with their employers has led to disagreements and tensions in the workplace. Uncertainties about the "ownership" of intellectual properties in the form of source codes and other programs have also lead to a large number of conflicts between employers and IT professionals. In fact, many of these IT specialists find greener pastures when they resign and become consultants.

Foreign interests of IT professionals can also lead to reduced loyalties. As in the PERSEREC study, offenders with foreign interests were significantly more likely than other offenders to have been motivated by ideology, which includes a set of beliefs based on common ethnic or national background. On the other hand, they can be less likely to be motivated by money (61% versus 78%).

[25] Morello, D., Gartner's Research. Retrieved February 21. 2006 from http://news.com.com/Gartner+sees+less+demand+for+IT+specialists/2100-1014_3-5974796.html).

It is not surprising that many espionage IT insider offenders have foreign interests. This does not indicate that Americans with foreign background or connections are less loyal than other Americans. In considering the security risk associated with foreign interests, it is important to distinguish between susceptibility to recruitment and vulnerability to being targeted for recruitment. Foreign interests do not make one more susceptible (less loyal), but they do make one more vulnerable. Americans with foreign interests have valuable language skills and area knowledge. Because of these skills, they are more likely than other Americans to be in positions where they have access to classified information. They are more likely to have contact with foreigners and more likely to feel comfortable dealing with foreigners. They are also more likely to be accessible for assessment and to be targeted for recruitment by unethical foreign competitors.

Sense of Entitlement

Indications of sense of entitlement can be seen in a majority of the cases that were the subjects of the PERSEREC study. Similarly, the IT cases discussed also have indications of the perpetrators feeling they were entitled to the confidential materials they stole or otherwise compromised.

Clinical investigations of vulnerable technology specialists, conducted by Shaw et al. (1998) consistently revealed two important traits as risk factors in technology specialists. In the assessments of technology specialist perpetrators of theft of business secrets, industrial espionage or sabotage, the researchers found that a sense of entitlement and anger at authority were consistent aspects of perpetrator motivation and personality.

The “sense of entitlement” syndrome has been used to describe the outrageous attitude of some narcissistic personality where people believe that the world "owes" them and they want to collect NOW or mete out punishment. Some technology specialists who have designed

critical programs or worked hard to derive formulas for ground-breaking technologies never feel that they have been paid or appreciated enough. They will always want more.

With this attitude, whatever their employers do is never good enough for them, and they also generally show no gratitude or express any thanks -- even when someone goes out of their way for them. They take offense when their companies are in the news and their names are not specifically mentioned as the real inventors. Like the most spoiled of royalty, they merely expect that they should be the center of the world at all times.

This sense of entitlement often combines with a pre-existing anger at authority to produce feelings in these individuals that they have been treated unjustly and are entitled to compensation, and that otherwise, revenge is due. Although they are generally introverts, their feelings of entitlement can be so strong as to overcome their introversion from time to time. They may hardly keep these strong feelings entirely to themselves. As such, a technology specialist who constantly complains that he is owed more is likely to exhibit this “sense of entitlement” attitude and is clearly vulnerable to acts of espionage, theft or sabotage.

Lack of Empathy

American technology companies have lost billions of dollars to the theft or compromise of their proprietary information. This parallels the experience of the US, where its own trusted citizens have utterly betrayed their country – making it lose billions of dollars and several years of research and defense and security advantages.

Take the case of former FBI agent Hanssen. Knowing fully well the grave repercussions of their activities, should their identities be revealed to the Russian authorities, Hanssen nonetheless, identified three Russian agents working for the United States in a bid to curry favor with the Russians. Two of these sources were tried in Russia and executed.

In her speech during the Department Of Defense Conference on Counterintelligence in San Diego, California on April 28, 2004, Michelle Van Cleave of ONCIX pointed to some reminders to the heartlessness of the perpetrators of espionage. She recalled the case of Alrich Ames (the former CIA officer) and his wife, Rosario Ames who in April of 1994 pleaded guilty. Mr. Ames had spied for the Soviet Union/Russia for nearly a decade, during which period some 30 operations against the Soviets (with their potential to save human lives) were compromised, and at least 10 Russians and East Europeans were executed as a result of his espionage. Ames' espionage activities were reportedly responsible for the loss of virtually all of CIA's intelligence assets targeted at the Soviet Union at the height of the Cold War. Ames obviously knew about the possibility of those wider repercussions of his activities on the nation, the world and other human beings.[26]

The case of William Holden Bell also revealed lack of empathy in the business of espionage. Bell's activities during the cold war, when millions of lives were at stake, for about $150,000 revealed secret technical information that neutralized some US military advantages and saved the Soviets approximately $185 million in technological research. The information also advanced Soviet technology by about 5 years by permitting them to implement proven design concepts.

Many companies like Ellery Systems, Inc. referenced before, have been forced into bankruptcy with thousands of employee layoffs. Some potential perpetrators may consider these grave impacts and drop their plots. However, some disregard the effects of their actions on their employers and fellow workers, and on the nation. They think and care only about themselves. This lack of empathy, when present in its extreme form has allowed these people to exploit their victims without remorse of any kind (Montana, 2003).

[26] For Michelle Van Cleave's speech, visit the Office of National Counterintelligence Executive web site at http://www.ncix.gov/publications/reports_speeches/index.html

A technology professional who has exhibited signs of lack of empathy on certain occasions ought to be considered vulnerable. This vulnerability is exacerbated by the fact that the impersonal layers of cyberspace has led many technology experts who have perpetrated these crimes not to relate their acts as having impact on real human beings. Many more perpetrators appear incapable of placing themselves in their victim's shoes and imagining how the experience felt. This lack of empathy is a hallmark of individuals with narcissistic and anti-social personalities, and is consistent with the traits of reduced loyalty and moral elasticity discussed before.

Revenge

Because of their enormous power to cause major disruptions at their choosing, an IT insider known to have a propensity for vengeance is a security risk.

Donald Burleson, who was a computer programmer for USPA & IRA Co - a Fort Worth, Texas securities trading firm was reprimanded for storing personal letters on his company-issued computer. For revenge, Burleson designed a virus to disrupt the system.

Also consider the Case of Smith, the civilian employee serving as an ordinary seaman on the USS Kilauea who stole confidential information. Investigation not only showed that Smith needed mental treatment and had a severe alcohol problem, but Smith reportedly told FBI agents that he wanted to get back at the crew for their mistreatment of him and that, in order to get revenge, he had tried to steal valuable classified materials because if he got something valuable, then he could turn his life around. To sell his cache, he thought he might go online and solicit buyers from terrorist groups.

CONCLUSIONS

The United States today has the dominant military force in the world without question. Although many people argue that the US military is currently overstretched, there is no doubt that the US can accommodate any real military contingencies that can currently be envisioned. The United States Department of Defense budget for fiscal year 2006 was $441.6 billion. For 2007, the budget was raised to a total of US$ 466 Billion. This did not include many military-related items that are outside of the Defense Department budget, such as nuclear weapons research, maintenance and production (which is in the Department of Energy budget), Veterans Affairs or the president's current wars in Iraq and Afghanistan (which are largely funded through extra-budgetary supplements). This partly accounts for the higher figures shown on Table 2.

US's military (DoD) budget accounts for almost one-half of the World's entire military spending (see Table 2). The US military spending alone, is larger than the military budgets of the next fourteen biggest spenders combined (China, Russia, Japan, UK, France, Germany, Italy, Saudi Arabia, India, South Korea, Israel, Australia, Brazil, Turkey and Canada), and nearly seven times larger than China's, which places second.[27] This huge military spending along with the concurrent massive intelligence requirements and equally massive security budget and investments has made the US the country to study, leading to constant spying by foreign military and security agencies.

[27] See the "Military Budget of the United States" at http://en.wikipedia.org/wiki/US_military_budget. Internet. Retrieved October 14, 2006

Military expenditure: in MER[1] dollar terms

Rank	Country	Spending level[2] ($ billions)	Per capita ($)	World share (%)
1.	United States	$478.2	$1,604	48%
2.	United Kingdom	48.3	809	5
3.	France	46.2	763	5
4.	Japan	42.1	329	4
5.	China[3]	41.0	31.2	4
6.	Germany	33.2	401	3
7.	Italy	27.2	468	3
8.	Saudi Arabia	25.2	1,025	3
9.	Russia[3]	21.0	147	2
10.	India	$20.4	$18.5	2%
11.	South Korea	16.4	344	2
12.	Canada	10.6	327	1
13.	Australia	10.5	522	1
14.	Spain	9.9	230	1
15.	Israel	9.6	1,430	1
	Subtotal, top 15	**$839.8**		**84%**
	World	**$1,001.0**	**155**	**100%**

1. MER = market exchange rate.
2. Spending figures are in U.S. dollars, at constant (2003) prices and exchange rates.
3. Estimated figure.

Table 2: Largest Military Expenditures, 2005

Source: SIPRI Yearbook 2006, Stockholm International Peace Research Institute

Unfortunately, many Americans entrusted with the secrets that are at the heart of US's security have betrayed their fatherland and sold or otherwise compromised secret information in favor of many nations or organizations that are clearly hostile to the US.

In response, US military and security agencies have conducted and have continued to conduct studies into the espionage cases with a view to better understanding the personalities and predisposing factors for the acts of espionage. Such studies have led to an improved understanding of the personalities of the perpetrators, and their modus operandi. The studies have also led to better monitoring and counterintelligence measures.

American technology companies have likewise led the world in innovation. For example, America's IBM in spite of the aggressive domestic and foreign competition over the decades, has remained the world's largest information technology company. Measured by revenue, IBM is the world's biggest provider of IT services ($46B), hardware ($31B) and financing ($2.6B), and second to Microsoft in software ($15B). With approximately 329,000 employees in 75 countries, serving clients in 174, and speaking more than 165 languages IBM's 2004 revenues were $96.2B.[28]

The US military and security agencies have traditionally worked in partnership with private high technology-based companies in preserving and enhancing the security of the nation. As a result, the high technology companies have become targets of prying eyes of not only worldwide commercial competitors, but foreign governments and security agencies. American hi-tech companies have been experiencing very concerted efforts to steal their secrets just as English firms experienced in the 18th century when they led the world in development. These hi-tech companies "are under considerable domestic and international competitive pressure – and information attack – from a variety of domestic and international actors, each with a different set of approaches and standards" (Nolan 1999, p.240). As a

[28] See IBM Background Information at http://www-03.ibm.com/press/us/en/background.wss. Internet. Retrieved October 15, 2006

consequence, they have been victims of theft of trade secrets, industrial espionage and have lost billions of dollars in compromised or stolen information.

The perpetrators have been companies that are sometimes sponsored directly or surreptitiously by state security apparatuses. They are not expected to slow down as top foreign government officials have openly encouraged their local companies in these acts against US companies. However, the assailants have usually gotten insider help. Indeed, every so often, company technology insiders have instigated these crimes and have become vendors of the information, selling them to any organization willing to pay.

While the technology companies have equally invested billions of dollars in security products and programs, there is a coherent cluster of antisocial tendencies and risk factors characteristic of a vulnerable subgroup of technology professionals who have access to the critical competitive information. These insiders are the designers, operators, programmers, networking engineers, and systems administrators. The negative personal and social experiences of some of them tend to make them more vulnerable to participating in espionage or sabotage activities than other employees. The failure to understand the personality and motivation of these at-risk hi-tech employees has been a major security management error.

The presence of certain antisocial tendencies, personality traits and attitudes within the IT culture increases the vulnerability of these technology specialists who work in American technology companies. These factors include substance abuse, excessive introversion, unbecoming activism, financial difficulties, social problems and personal frustrations, flirtation, grandiosity, moral elasticity, reduced loyalty, having a sense of entitlement, lack of empathy, having a history of previous dangerous acts, and revenge.

Although these antisocial tendencies or severe narcissism are associated with increased security risk, they do not necessarily lead to serious offenses. Gelles (2001) identifies three critical factors that will usually have to fall into alignment before a previously trustworthy and

loyal employee commits a serious crime. First, there must be a personality or character weakness, such as antisocial tendencies or narcissism that causes a predisposition to maladjusted, counterproductive behavior. Second, a personal, financial, or career crisis puts an individual with these weaknesses under great stress, triggering more obvious counterproductive behavior often observable by friends, coworkers, or supervisors. Third, the friends, coworkers, and supervisors fail to recognize the signs of a serious problem, decide they don't want to get involved, or assume that someone else will take care of it. As a result, no one intervenes to help resolve the problem, and the individual's behavior spirals out of control.

There’s no one that is perfect. Most people possess one or more character or personality weaknesses to some degree, but that does not mean everyone is a high security risk. All security judgments are based on the "whole person concept" which means looking at a person's strengths as well as their weaknesses. In a nut shell, while these tendencies, traits and cultures are not in themselves enough to conclude that a particular technology professional would commit these terrible acts, they are useful pointers to vulnerabilities and will be helpful for security professionals and managers in managing the technology staff better.

These facts, sad as they be, about these highly talented engineers, programmers, designers and system managers, who constantly crunch hard numbers and derive mathematical formulas to make life better for all, need to be taken seriously by security professionals. Threat to information in high-technology companies from those who are best familiar with the information seems to be highly entrenched in the industry. Whether a company is large, medium or small, and whether they have or do not have an Intelligence department or function, no one is going to change the nature of the business we live in today (Nolan, 1999, p.258).

REFERENCES

Allen. T.B. (1996), "Spy Book", Random House Reference

Allen, T.B. (1986) "Year of the Questions -- Spies, Software Moles, and Subversive Agents." Sea Power Publications

Allen, T.B. & Norman, P., (1988). “Merchants of Treason: America's Secrets for Sale” Delacorte Publishers

Ames, R. & Hall, D. (1987), “Thinking Through Confucius.” Albany, SUNY Press.

Associated Press, “Woman Charged with Conspiracy to Spy for Cuba”, 21 September 2001

Bamford, J., "My Friend, the Spy." *New York Times,* 18 Mar. 2001.

Baro Diaz, M., “The Story Faget”, *The Sun-Sentinel*., Saturday South Broward Edition. June 30, 2001

Bragg, R., “I.N.S. Official is Convicted on Charges of Espionage.” *The New York Times*, 31 May 2000

Brink, G., “Trofimoff Spy Trial Promises Intrigue.” *St. Petersburg Times*, 6 June 2001

Brinkley-Rogers, P., “INS Official Gets 5 Years in Spy Sting”. *The Miami Herald*, 30 Jun 2001

Byers, A. J. (2005), “The Imperfect Spy: The Inside Story of a Convicted Spy”, Vandamere Books

Chachere, V., "Top Military Man Alleged to Be Spy." *Associated Press*, 14 Jun. 2000.

CorpTech (2005). CorpTech Directory of Technology Companies File # 559, *OneSource Information Services, Inc., Concord, MA*

CSI/FBI (2005). “Tenth Annual CSI/FBI Computer Crime and Security Survey”, Computer Security Institute.

Dershowitz et al. (1999) "Justice and Jonathan Pollard." *The Washington Post*, Jan. 2, 1999, page A19.

Denning, D.E. (1999), “Information Warfare and Security”, Addison-Wesley Press.

Driscoll, A., & Tamayo, J. (2000). “Faget: ‘Spy’ Talk Was Only Business.” *The Miami Herald*, 12 March 2000

Eggen, D., "Webster Begins Probe of FBI Security Measures." *Washington Post*, 13 Mar. 2001.

Eggen, D. & Vise, D.A., "To Russia, With Longing." *Washington Post*, 24 Feb. 2001, p. A1.

Gelles, M. (2001). Exploring the Mind of the Spy. In *Employer's Guide to Security Responsibilities. Version 1.0.* Defense Personnel Security Research Center (PERSEREC)

Golden, T., "Ex-U.S. Aide Sentenced to 25 Years for Spying for Cuba" *New York Times*, 17 Oct 2002

Herbig, K., (2005). "Espionage by the Numbers: A Statistical Overview", TRW Systems.

Hoffman, L., "FBI Scandal Leaves CIA Gloating." *Chicago Sun-Times*, 11 Mar. 2001.

Johnson, T., "Cuban Spy Passed Polygraph at Least Once", *Miami Herald*, 28 Mar 2001,

Johnson, T., "She Led Two Lives—Dutiful Analyst, and Spy for Cuba" *Miami Herald*, 16 Jun 2002

Johnson, T., "U.S. Intelligence Analyst Charged with Spying for Cuba." *Miami Herald*, September 22 2001

Johnston, D., "F.B.I. Agent Charged as Spy Who Aided Russia for 15 Years." *New York Times*, 21 February 2001.

Johnston, D., "F.B.I. Never Gave Lie Test to Agent Charged as Spy." *New York Times,* 22 Feb. 2001.

Johnston, D. & Risen, J., "U.S. Had Evidence of Espionage, but F.B.I. Failed to Inspect Itself." *New York Times*, 23 Feb. 2001

Keating, S. (1994), "Global Intrigue on Info Highway, Local Case Alleges Chinese Piracy", *The Denver Post*, April 24, 1994, p. A-1.

Kotler, P. (2003), "Marketing Management" 11th Ed: Prentice Hall

LaFraniere, S., "Russia Says FBI Agent's Arrest Shouldn't Hurt Relations." *Washington Post*, 22 Feb. 2001, p. A6.

Lau, D. C. (1979), "Confucius: The Analects." Penguin

Lewis, N.A., "The Prosecution Case: Zigs and Zags of Spy Cases Put a Damper on Predicting." *New York Times*, 22 Feb. 2001

Livingood, J. (1995). "Revenge of the Introverts" in *Computer-Mediated Communication Magazine, Volume 2, Number 4 / April 1, 1995.*

Loeb, V., "Spies and Other Ego-Trippers: Psychiatrist Jerrold Post Weighs the Personality in Politics." *Washington Post,* 24 March 2001, p.C1.

Loeb, V. & Eggen, D., "Hanssen Carried Secrets Between FBI, State Dept." *Washington Post*, 1 Mar. 2001, p. A1.

Loeb, V. & Masters, B.A., "Spy Suspect Had Deep Data Access, Ex-Associates Say." *Washington Post*, 22 Feb. 2001, p. A1.

Loeb, V. & Pincus, W., "Bush to Speed Clinton Spy Changes." *Washington Post*, 24 Feb. 2001, p. A4.

Loeb, V. & Pincus, W., "Hanssen Case May Be Linked to Defector." *Washington Post*, 18 March 2001, p. A5.

Long, P., "Former Intelligence Officer Gets Life Sentence in Tampa." *Miami Herald*, 27 September 2001.

Long, P., "Spy Suspect Bragged of Deeds, Prosecutor Says." *Miami Herald*, 21 June 2000

Lynds, G. (2006), “The Last Spymaster”, St. Martin's Press

Lytle, T., “Brevard Retiree is Accused of Espionage.” *The Orlando Sentinel*, 15 June 2000

Macrakis, K. (2000), “The Case of Agent Gorbachev”, *American Scientists*, (November-December 2000.

Markon, J., "Coded Messages Add to Mystery of a Failed Spy." *Washington Post*, 28 Apr. 2003, p.A1.

Markon, J., "Convicted Spy Accepts Life Sentence: Sudden Sentencing Deal Will Prevent Prosecution of Ex-Air Force Analyst's Wife." *Washington Post*, 21 Mar. 2003, p.B1.

Markon, J., "Convicted Spy Led FBI to Papers Buried in Parks." *Washington Post*, 31 Jul. 2003, p.B1.

Markon, J., "Jury Opens Deliberations in Federal Espionage Case; Regan Could Face Death if Convicted of Spying Charges." *Washington Post*, 11 Feb. 2003, p.B2.

Marquis, C., "Ex-Army Employee Charged With Spying for Russia for at Least 25 Years." New York Times, 15 June 2000

Marquis, C., "Retired Army Employee, 74, Is Found Guilty of Spying." *New York Times*, 27 June 2001

Masters, B. A. "Retired Air Force Sgt. Charged With Espionage." *Washington Post*, 24 August 2001

Masters, B. A. "Spy Suspect Had Missile Site Coordinates." *Washington Post*, 24 Oct. 2001, p.A18.

Masters, B. A. & Eggen, D., "Indictment Says Suspect Tried to Sell Defense Secrets." *Washington Post*, 15 Feb. 2002, p.A19.

Masters, B. A. & Loeb, V., "Air Force Retiree Charged as Spy: Secret Documents Passed, U.S. Says." *Washington Post*, 25 Aug. 2001, p.A1

Masters, B.A. & Loeb, V., "CIA Officer Had Been Focus of Spy Probe." *Washington Post,* 23 Feb. 2001, p. A1.

Masters, B.A., & Pincus, W., "FBI Left Hanssen an Opening as His Debts Mounted." *Washington Post*, 28 Feb. 2001, p. A2.

Mendell, R. L. (2003) “The Quiet Threat: Fighting Industrial Espionage in America”, Charles C. Thomas Publishers.

Minieri, M.W. (2004), “Protecting Corporate Secrets”, *Kroll White Paper.*

Montana, S. (2003). “Understanding Empathy”, in *LUKENOTES, Vol. VII, No. 3*

Nasheri, H. & Blumstein, A. (Eds) (2005), “Economic Espionage and Industrial Spying”, Cambridge University Press

National Counter Intelligence Center – NACIC (2001). *Annual Report to Congress*

National Counter-Intelligence Executive, News and Developments, Vol. 1, March 2001

Nivison, D. (1996), “The Ways of Confucianism.” Open Court.

Nolan, J. (1999). Confidential: Business Secrets Getting Theirs-Keeping Yours. 1st Ed.: Harper Collins.

Petersen, N.H. (Comp. & Ed) (1992), "Counterintelligence and Internal Security - American Intelligence, 1775-1990: A Bibliographic Guide.” Regina Books

Pincus, W., "Ames Seeks to Renegotiate 1994 Guilty Plea Over Spying for KGB" *Washington Post*, 15 September 1999, p. A7.

Pincus, W., "Satellite Agency Has Tradition of Secrecy; Joint Defense-CIA Enterprise Uses Many Contract Employees Such as Alleged Spy." *Washington Post*, 25 Aug. 2001, p. A10.

Pino-Marina, C., "Virginia FBI Agent Arrested on Espionage Charges." *The Washington Post*. 20 February 2001.

Pocius, K.E. (1991). “Personality Factors in Human-Computer Interaction: A Review of the Literature.” *Computers in Human Behavior, Vol. 7: 103-135. Pergamon Press.*

PRNewswire (1997), “Federal Criminal Charges Brought for Theft of Gillette Shave Secrets.” Sept. 25, 1997 Issue

Risen, J., "Employee of U.S. Contractor Accused of Conspiracy to Spy." *New York Times*, 25 Aug. 2001

Risen, J., "F.B.I. Spy Case May Explain Arrest of a K.G.B. Agent." *New York Times*, 7 Mar. 2001.

Risen, J., "News Analysis: In Espionage Game, Get Caught, Lose Players." *New York Times*, 23 March 2001.

Risen, J., "Spy-Hunt Team Followed Trail to F.B.I. Agent." *New York Times*, 24 Feb. 2001.

Risen, J., "The Spymaster: Spy Handler Bedeviled U.S. in Earlier Case." *New York Times*, 22 Feb. 2001

Risen, J. & Bergman, L., "U.S. Thinks Agent Revealed Tunnel at Soviet Embassy." *New York Times*, 4 Mar. 2001.

Risen, J. & Perlez, J., "Russian Diplomats Ordered Expelled in a Countermove." *New York Times*, 22 March 2001.

Risen, J. & Shenon, P., "Accused Spy Suspected Loss of Access to Secrets, Prosecutors Say." *New York Times*, 28 Feb. 2001.

Schwartz, B. (1985), “The World of Thought in Ancient China.” Harvard University Press.

Schweizer, P. (1993), “Friendly Spies: How America’s Allies Are Using Economic Espionage to Steal Our Secrets.” Atlantic Monthly Press.

Shaw, E.D., Keven G. Ruby, K.G. & Post, J.M. (1998), “The Insider Threat to Information Systems”, Political Psychology Associates, Ltd.

Shenon, P., "From Dour 'Mortician' of F.B.I. to Suspected Russian Superspy." *New York Times*, 21 Feb. 2001

Smikle, P., “Seaman Admits Stealing Defense Secrets, FBI Says.” Seattle Post-Intelligencer. 14 April 2000

Tyler, P.E., "Russia Expels 4 Americans and Vows 'Other Measures.'" *New York Times*, 24 March 2001.

US Department of Defense (1998). Security Awareness Bulletin No. 2-98. Department of Defense Security Institute.

Vise, D. A., "FBI Sting at INS Found an Unlikely Cuban Spy Suspect." *Washington Post*. 19 Feb. 2000

Vise, D.A. & Eggen, D., "FBI Faulted For Rejecting Warnings." *Washington Post*, 22 Feb. 2001, p. A1

Weiss, P., "The Quiet Coup: U.S. v. Morison - a Victory for Secret Government," Harper’s, September 1989.

Wise, D. (1995), “Nightmover: How Aldrich Ames sold the CIA to the KGB for $4.6 Million.” HarperCollins

ZDNet Asia Staff, Gartner Sees Less Demand for IT Specialists, *ZDNet News, November 29, 2005 Edition*