

Jaime Bogardy

So you want to be a spy:

A look into the technology and training of yesterday's, today's, and tomorrow's spies

“In sending them to reconnoiter the land of Canaan, Moses said to them, ‘Go up here in the Negeb, up into the highlands, and see what kind of land it is. Are the people living there strong or weak, few or many? Is the country in which they live good or bad? Are the towns in which they dwell open or fortified? Is the soil fertile or barren, wooded or clear?’”

Numbers 13: 17-20

Surveillance has improved by leaps and bounds, far surpassing novel concepts introduced in 20<sup>th</sup> century literature and film, which were merely science fiction. Because of such unbelievable advancements, James Bond's charm has even begun to fizzle. From high resolution satellites to RFID chips, fictional spy technology is no longer a dream of the future. Intelligence relies not only on spyware, but extensive training and a constant sense of awareness. With the ethical questions of privacy invasion comes the growing concern of the importance of human intelligence versus technology. This “war” is unlike any other, and many feel that the billions of dollars that may be invested in a new satellite would be “much better spent on the kind of human intelligence needed to penetrate closed regimes and terrorist networks” (Jehl, 2004, p. 1.1). This paper considers past, present, and future spy technology as well as other procedures required in providing security to America by responding to the following questions:

1. What is intelligence?
2. How is spy technology protecting America?
3. What are some of the training procedures?
4. How has espionage changed?

Understanding the growing need for American security highlights the intricacy of the institution of surveillance. Furthermore, it draws attention to the need for appropriate tactics and technology in combating the nation's enemies.

### **What is intelligence?**

While “intelligence” generally refers to the capacity for acquiring knowledge, the word takes on a much more complex meaning when referring to national security. In his Age of Surveillance, Donner (1980) explains intelligence as “a sequential process, which embraces the selection of the subject...for surveillance, the techniques...used in monitoring the subject...,the processing and retention of the information collected...,and its evaluation in the light of a strategic purpose” (p. 3). In this respect, intelligence has three stages: acquiring, analyzing, and evaluating. During the gathering process, there are two general types of information attainment: tactical and strategic. Also known as operational gathering, the tactical method is used in most reconnaissance activities and involves current or short-term intelligence such as events on a battlefield (Yost, 1985, p. 9; Interagency OPSEC, 1996, p. 2-1). Strategic intelligence is the collection of information that has long-lasting importance, such as weapons testing (Yost, 1985, p. 9; Interagency OPSEC, 1996, p. 2-1). Upon being gathered, information is then analyzed and divided into five separate disciplines. Explanations of each discipline are summarized in Table 1.

Table 1

*Intelligence Disciplines*

<b>Abbreviation</b>	<b>Type</b>	<b>Purpose</b>
HUMINT	Human	Humans are an information source and collection instrument
SIGINT	Signals	Signals intercept COMINT (communications) ELINT (electric) FISINT (foreign instrumentation)
IMINT	Imagery	Information collected from photos, radar, etc.
MASINT	Measurement and Signature	Identifying features with the source ACOUTINT (acoustical) LASINT (laser) RADINT (radiation)
OSINT	Open Source	Available sources such as books and newspapers

*Note.* Information on intelligence disciplines has been compiled from OPSEC's Intelligence Threat Handbook (1996, pp. 1-2) and Shaffer (2006, p. 9).

From what leaks out of the various intelligence agencies in the nation, it may seem like progress is being made by the second and that the country is becoming undoubtedly safer. However, doubt looms over the heads of Americans when people like Soviet spy John Anthony Walker declare that "Kmart has better security than the Navy" (Barth, 2004, p. 79). A sense of fear may then be spawned from the thought of a mega store chain that *clothes* the country being better protected than the people and equipment that *protect* the country. Before writing off the American intelligence sector due to such statements, recent accusations, and the 9/11 terrorist attacks, it is important to compare the incredible successes of the government agencies to their unfortunate failures. Due to the inherent secrecy behind the various security agencies of the nation, it is extremely difficult to gather information about security measures being implemented to prevent terrorism. However, Robinson and Whitelaw (2006) confirmed that "several serious terrorist plots overseas" had been foiled and many critical Al Qaeda figures had been eliminated (p. 36). Surveillance of each intelligence agency also greatly contributes to the success of national security. The National Security Agency (NSA) is compartmentalized and often referred

to as the “puzzle palace” (S. Tatro, personal communication, May 7, 2006). According to a book written in 1985 by Yost, identity badges are magnetically coded so certain employees stay in designated areas based on their status or position in the agency: “...those who wander into a restricted area for which they do not have clearance will cause an alarm to sound, and they will have to explain their presence to an overhead camera” (p. 222). When asked about this specific type of security in the building itself, NSA mathematician Steven Tatro would not comment. He did confirm, however, that the badges were equipped with a magnetic strip and an RFID (radio-frequency identification) chip. In addition to this internal surveillance, visitors to the building must have their social security numbers checked against a database before entering (S. Tatro). Similarly, records are kept of all access into the White House. According to the 1975 Secret Service and IRS Surveillance and Records Policies, certain communications received at the White House are required to be sent to the Secret Service, including but not limited to anonymous communications, physical threats, and interest shown in any agency’s security procedures (p. 25). Such policies have likely helped to prevent terrorist attacks and provide the government with significant leads.

It is regrettable to acknowledge the failures of American intelligence, but each mistake is taken into account when developing new security measures. Recent disappointments include the 9/11 attacks, allegations of torturing detainees, unfound supposed weapons of mass destruction, and the resignations of personnel from various intelligence agencies. According to Tatro, since the former CIA director very recently resigned, his replacement is likely to be Michael Hayden, assistant director of national intelligence and former director of NSA (personal communication, May 7, 2006). While the change in administration is not necessarily a failure, personnel switches, as in any office, often cause confusion and reflect disorganization.

In 1946, Soviet school children gave the US Ambassador a carved wooden replica of the US seal; in 1952, a bugging device was discovered in the seal (International Spy Museum). These sorts of failures on the part of government intelligence are humiliating, but have security agencies learned from their mistakes? One may say no, considering that in the summer of 1998, a transmitter was found in a piece of wooden paneling in the US State Department building (Shannon, 1999, p. 75). Stanislav Gusev, a Russian spy, was seen daily outside the building fiddling with something in his pocket; it was later discovered that “an antenna was concealed in a dashboard box of Kleenex” (Shannon, 1999, p. 75). In 1966, “black bag” jobs (entries by force to steal documents) were deemed illegal in the United States, but microphone installations and burglaries were still permitted (Donner, 1980, p. 130). According to Donner, any means necessary should be enacted to gain intelligence, including violence (p. 207).

Skeptics use caution when deciding whether intelligence practices are protected. Said Farmer and Mann (2003), it is very easy to spread information over the internet since computers are “notoriously hard to secure” (p. 49). Perhaps this is why it is so easy for intelligence agencies to gain information about all citizens, leading to a decline in civil liberties. Says the Defense Department’s Total Information Awareness Program Manager John Poindexter in his letter of resignation, “It would be no good to solve the security problem and give up the privacy and civil liberties that make our country great” (Harris, 2006, p. 49). Americans have become more accepting of the breaches in privacy which have increased since 9/11, and Farmer and Mann (2003) fear that the country will become more accustomed to this lack of privacy and inevitably give up confidentiality to maintain a safe nation (p. 52). Moreover, the public availability of spyware has grown, creating an entirely new concern about surveillance.

As of 2003, 80 percent of major US companies were electronically monitoring their employees to prevent “cyberslacking,” and \$5 billion are spent per year on consumer spy gadgets (Farmer & Mann, 2003, p. 50; International Spy Museum). Businesses have technology such as fingerprint computer access and software to control office cameras. Main reasons for such surveillance are “measuring performance, preventing theft, and ensuring that workplace policies are adhered to” (Whitty, 2004, p. 39). While the company may think it is patrolling the work habits of its employees, it may just be making workers defensive, creating unnecessary pressure, inducing negative relationships, and creating ethical issues in the workplace (O’Malley, 1998, p. 251; Whitty, 2004, p. 41). Controversy has erupted over the privacy issues surrounding work surveillance because of the conflict in privacy expectations which differ based on location (i.e. home vs. office) and activity (i.e. shopping vs. showering) (Charlesworth, 2003, p. 217-8). Charlesworth has proposed that conditions of workplace surveillance be put in place to cease conflict: the employer must have a believable purpose, he must use a minimum amount of intrusive surveillance, observation must be fair, supervision cannot discriminate, and employees must be informed of surveillance measures. According to his article:

“The modern employee may be watched via CCTV...her telephone calls recorded, her office conversation monitored by listening devices, her key strokes logged, her computer screen monitored, her movements noted by sensors in her seat, her whereabouts in the building pinpointed by location badge” (p. 218).

Better lenses and sensors, faster computers, and larger databases are making surveillance inexpensive and habitual. According to Farmer and Mann, “we have met the enemy of our privacy, and it is us” (p. 47).

### **How is spy technology protecting America?**

A wide variety of spyware has been invented and re-invented throughout the years as foreign relations have changed the demand for surveillance. The International Spy Museum in Washington, D.C., is full of information on past spy gadgets, but who is to say that they are no longer in use? If most intelligence successes are kept secret, it is doubtful that their tools would be available as public knowledge.

Lock-picking has been of particular importance in spy work. Films such as *The Italian Job* show locks being meticulously opened, but the CIA officers never reveal their tricks. Spies concealed lock-picking kits in everyday items such as pens and dictionaries (International Spy Museum). They would train on lock cutaways to learn first and then go out into the field to practice their skills. Weapons are, of course, important parts of a spy's range of devices. The Office of Technical Service created the "cigarette pistol" as well as a combustible notebook and explosive flour (Richelson, 2001, p. 165). The Army's Special Operations Division also invented a special dart-gun that shot chemical-coated darts designed to debilitate enemy's dogs (Richelson, 2001, p. 11). Common in many intelligence agencies were "dead-drop" services that involved disguising documents or important objects inside quotidian items, then leaving them in specific places for a second party to retrieve (Richelson, 2001, p. 165). Another clandestine device was the microdot, which concealed a very small version of some document in a microscopic chip. The chip could then be inserted in between the layers of a post card or another common item and then only read with a special reader, often concealed in a cigarette or pen (International Spy Museum). The Museum houses many other items such as fluorescent ink, tear gas pens, and eyeglasses that concealed cyanide pills in case the spy was being interrogated and had to commit suicide rather than revealing any secrets. In 1950, the CIA's project BLUEBIRD

developed a drug that would induce a trance-like state in case of capture; two years later, the project was renamed ARTICHOKE and sought to design techniques that would induce amnesia in case of the same situation (Richelson, 2001, p. 10). Similar, but used against the opposition, spies could rub a fatal skin-penetrable drug onto the steering wheel of an enemy's car (Donner, 1980, p. 251). In 1961, the Technical Services Division developed toxic pills designed for clandestine placement in drinks, but when tested, the pill neither disintegrated nor dissolved (Richelson, 2001, p. 38).

From James Bond to Austin Powers, spyware has frequented many films and provided some insight into what tools may actually be used in reconnaissance. The creators of these films do not simply jump into spyware blindly; they research spy technology. Said Bruce Gellen, creator of *Mission: Impossible*, "Some [real devices] are so fantastic that if we put them on the show, nobody would believe us" (International Spy Museum). *The Recruit*, a 2003 film, provides a glimpse into the world of a CIA recruit. Details are not left out, especially when the main characters are able to pull up records instantaneously from some government databases. James Clayton, played by Colin Farrell, invents a program called Spartacus, which "turns any specified broadcast terminal into its slave," and he is able to broadcast his face onto every computer and television in the near vicinity (Donaldson). Such programs are likely already available to government agencies and are perhaps even more advanced. The film also features several other pieces of spyware, such as paper that dissolves in water, a concealed place for a flash drive in the bottom of a mug, and "paper ants," which are biological microphone transmitters that consume themselves within 48 hours.

Another film that puts a unique spin on the concept of surveillance is *Minority Report*, produced in 2002. The story takes place in the year 2054; pre-cognitives see crime before it



occurs and future criminals are caught before the crime is actually committed, resulting in “total surveillance in a society” (Kammerer, 2004, p. 468). Spyware such as biometric retina scan devices have the ability not only to provide security but to electronically greet customers in stores as they enter and ask how they enjoyed their previous purchases. There are “spider” retina scanners, which forcibly scan citizens to gain and wirelessly report their identities to the police. In addition, the film involves wiretapping and the automatic disengagement of a vehicle to capture criminals. While the film is an interesting piece of work involving surveillance, there are deep-rooted ethical questions hidden beneath the plot. People are arrested before they commit the crime, but they say they “[weren’t] gonna do anything” (Spielberg). The question of whether it is ethical to arrest someone before he has committed a crime is begged throughout the movie; however, if “you know your own future...you can change it if you want to” (Spielberg). Choice is removed before anything occurs because the “criminal” is arrested. When John Anderton (Tom Cruise) finds out that he is going to commit a murder, he does everything to prevent it but ends up in the predicted situation; he is thus “confronted with [the] technology and has to learn to find new ways of using it” (Kammerer, 2004, p. 468). Although the “pre-cogs” are designed to help and a majority of the population supports the new technology, the system must still be adapted to override its inevitable flaws. It seems that the American response today to the increasing invasion of privacy may be parallel to the existentialist theme of removing free will and the constant surveillance in *Minority Report*; most think it is a great system, but only to a certain point. In this way, both a fictional futuristic film and the reality of changing privacy boundaries inquire, When have we gone too far?

It is common to hear characters in films discuss the possibility of a wiretap or of phone lines being “bugged.” Two types of wiretapping allow a third party to listen in or record

conversations. Direct wiretapping involves placing actual intercepts into the phone line, while wireless relies on a radio transmitter (Yost, 1985, p. 166). Audio surveillance can be performed in other ways, such as hiding transmitters with microphones. A Trojan horse is something brought into a situation, usually as a gift, but concealing a microphone. These can be flowers, picture frames, books, or other common objects. Similarly, quick plants are items which would normally go unnoticed such as a lighter, phone, or electric switch (International Spy Museum). The Museum also has a wristwatch microphone used during the 1950s for reconnaissance.

Eavesdropping was defined hundreds of years ago by Sir William Blackstone as “listen[ing] under walls or window, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales” (qtd. in National Commission, 1976, p. 33). These days, this form of electronic surveillance is used to prove someone guilty of misconduct. While it may be improving law enforcement, its misuse is also increasing. In 1931, exceptions were given to wiretapping by the Attorney General: “...where the crimes are substantial and serious, and the necessity is great and [the bureau chief and the assistant attorney general] are satisfied that the persons whose wires are to be tapped are of the criminal type” (qtd. in National Commission, 1976, p. 35). In 1940, according to the same government report, wiretapping was entirely banned, and the ban was lifted two months later; since then, laws regarding eavesdropping have been changed and modified frequently (National Commission, 1976, p. 36). Between 1967 and 1974, only 1,555 illegal wiretaps were found through AT&T, but the National Commission assured that most of these were used among family members, followed in frequency by businesses (p. xviii). During the Watergate scandal, President Nixon made eavesdropping notorious. According to Miller (1999), he “used national security as a basis for at least seventeen... wiretaps” (p. 288).

Rumors have spread in the recent past about phones and computers being tapped. Some have said that if certain words are said over the phone, such as “White House,” “terrorism,” or “bomb,” there will be a click on the receiver indicating a wiretap in place to record any conversation which could be a threat. While such rumors have not been validated, it has been confirmed that ECHELON, the NSA wiretapping network, and CARNIVORE, the FBI e-mail searching program, do exist (International Spy Museum). A common misconception about the NSA’s recent wiretapping scandal is that the government is constantly listening to conversations. On the contrary, only records of called numbers from millions of Americans are being collected and a database is being maintained by the NSA to determine who people call and when (Wallace, 2006). Nevertheless, the privacy of Americans has been breached for the sake of national security. Supreme Court Justice Robert H. Jackson did say, however, that “Security is like liberty in that many crimes are committed in its name,” so Americans may have to start expecting more personal invasions (National Commission, 1976, p. 177).

Despite recent allegations within the NSA and previous scandals regarding illegal wiretapping, there have been successful wiretaps that provided much-needed information to the government. US intelligence was able to tap into Iraqi military without UNSCOM (an international team of arms controllers trying to eliminate Iraq’s weapons) finding out (Thompson, 1999, p. 29). Due to the secret nature of such projects, the effects of allegedly successful surveillance endeavors are unknown. Additionally, even though security agencies may not have eavesdropping warrants, a poll showed that the majority of Americans support wiretapping of terrorist institutions (Gorman, 2006, p. 6A).

As important, if not more important, than audio surveillance are spy cameras. Cameras are critical to all reconnaissance activity, considering they have been placed in practically every

major city in the nation as well as most stores and large public areas. Used during the Cold War and featured at the International Spy Museum, the Minox could take fifty photos without having to reload and was an extremely important tool for spies. Similarly, the Nicrom camera could roll over a document to record and be concealed easily while collecting data (International Spy Museum). The CIA used special discreet cameras during the 1970s, which, like microdots and other hidden devices, were difficult to recognize. Cameras were hidden in small devices such as fountain pens and key chains, although their quality may have waned due to the size (International Spy Museum). Digital cameras have become the spy cameras of today, as they are able to take hundreds of pictures and do not require film or developing. Closed Circuit Television (CCTV) is widespread and used in most areas where surveillance is heightened. According to a recent statistic posted in the International Spy Museum, 5,000 cameras are in place in New York City; 200 of them are in Times Square. Cameras are being used on the nation's borders as well, and surely in other ways unknown to the general public.

Cameras have not only been used on land, but they have played a very important role in the air. Early aerial reconnaissance during the Civil War involved using hot air balloons to draw sketches of the land and telegraph messages (International Spy Museum). When Sherman Fairchild invented aerial cameras, they became popular in high-speed planes instead of cumbersome balloons. The F-5 Lightning used five of these cameras in place of weaponry, but was followed by a back-up fighter (Smithsonian). It is obvious that while the creators knew the plane would need some sort of defense mechanism, they put reconnaissance first. Soon after, the RF-101 Voodoo carried six cameras and was unarmed; that was later followed by the SR-71 Blackbird, which was capable of high altitudes and used in the 1960s (Smithsonian). Called the

“Ultimate Spy Plane,” the SR-71 had the highest and fastest flight and was never shot down despite nearly 1000 attempts (Yost, 1985, p. 40).

Developed by Lockheed for the CIA in the 1950s, the \$350,000 U-2 spy plane was unknown to the public until one was shot down on May 1, 1960 (Smithsonian; Schorr, 2006, p. 9). In fact, the National Reconnaissance Office, which manages space-based intelligence assets, was not acknowledged until 1992, despite its existence since the 1960s (Benson, 2004, p. 55). Due to its absolute secrecy, the Utility-2 project was given the name Aquatone and was said to be doing “upper atmosphere research” (Yost, 1985, p. 19, 26). When the plane crashed, the government assumed that the pilot was dead, so they reported that an NSA weather plane had encountered trouble and was missing. However, Francis Powers, who had been flying the plane when it was shot down, lived to tell the enemy that he was with US intelligence (International Spy Museum). The plane was particularly helpful during the Cuban Missile Crisis in 1962, when it showed evidence of Soviet arms construction in Cuba, then later showed the dismantling of the weapon sites (Yost, 1985, p. 36). In addition, between 1965 and 1966, the U-2 performed missions in China, where it dropped a javelin into the ground; the spike was equipped with airwave and ground motion sensors (Richelson, 2001, p. 93). The plane was highly regarded because of its unique reconnaissance abilities. Able to photograph with a resolution of .75 meters from 65,000 feet, the U-2 used its 80-foot wingspan to reach up to 70,000 feet above the earth (Smithsonian). Even more spyware besides the camera was included on the plane. It carried a life raft, morphine and a poison pen in case of capture, water-purification tablets, a pistol, and a poster with a 14-language message in case of an unexpected landing (Yost, 1985, p. 28). In 1981, the modernized TR-1 was created and was 40 percent larger. The plane holds the record for

highest-flying single-engine aircraft, and it is still assumed to be doing reconnaissance missions (Smithsonian).

More important today than planes are satellites because of their precise reconnaissance abilities. Just like the U-2 spy plane and most other missions, the successes of spacecraft are largely unknown. Said President Lyndon B. Johnson in 1967:

“We’ve spent between thirty-five and forty billion dollars on space...but if nothing else had come from that program except the knowledge that we get from our satellite photography, it would be worth ten times to us what the whole program has cost. Because tonight I know how many missiles the enemy has...” (Smithsonian).

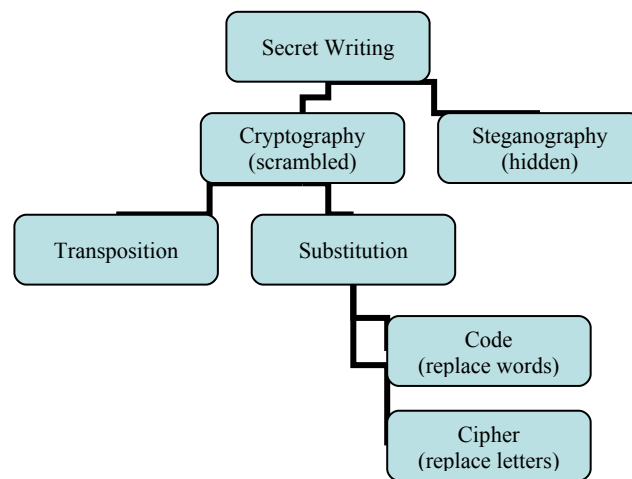
Managed by the CIA and Air Force between 1960 and 1962, GRAB (Galactic Radiation and Background) was disguised as SOLRAD to seem more like a scientific project. Similarly, CORONA, developed between 1960 and 1972, was disguised as Discoverer and took photos of the Soviet Union (Smithsonian). These satellites improved quickly, their resolution zooming in from 40 to 12 feet in only a year. By 1972, they were able to see a line of visitors waiting outside a monument (Smithsonian). While they lessened Cold War tensions, the satellites were later used to make sure the Soviet Union was following treaty terms (Smithsonian).

Once called “the world’s finest satellite,” the KH-11 could spot camouflage, see through clouds, and see in the dark (Yost, 1985, p. 3). Later, the SAMOS satellite (Satellite and Missile Observation System) was developed by the National Reconnaissance Office and was the only spy satellite to ever be identified as such (Yost, 1985, p. 73-4). The technology used to collect photos from space involved taking actual photos from the satellite, then dropping a capsule down with the film and having them developed. Today, the technology is more advanced to the point that satellites can show images instantaneously without the use of film or capsules. They are used

to report news, track migration, monitor changes in geography, and even to spy on neighbors (Smithsonian). A new \$9.5-billion satellite, which would have high-resolution reconnaissance only in daylight and in clear weather, has been proposed (Jehl, 2004, p. 1.1). However, many details about this proposal were reportedly undisclosed, such as the number of satellites that were to be created, and why this satellite was necessary if one that had excellent resolution and could work during better times already existed. Even though information about the project has been released, it is unlikely that many more details will be revealed to the general public since it will be a surveillance satellite.

Reconnaissance is not limited to the use of cutting-edge technology. In fact, spies rely heavily on their intangible resources, a concept which is reinforced during training. A particularly important element of espionage is having a cover, or a disguise to hide or create an identity. Covers are applied to more than just individuals, as can be seen from past British creation of false spy networks where the truth is protected with lies; “Operation Bodyguard” misled German intelligence into preparing for an attack (International Spy Museum). Spies also create a *lingua franca* which includes metaphors, aliases and nicknames when eavesdropping is suspected (Donner, 1980, p. 342-3). They may also soften certain words, according to Donner, where a word such as “break-in” becomes “surreptitious entry” (p. 464). Not only is code used in this type of general manner, but secret writing is an important part of surveillance and countersurveillance. The first code device was the cipher disk, used by the Confederates during the Civil War, and in 1943, the M-209 Cipher Machine was created by the US Army (International Spy Museum). A cipher is more commonly used is secret writing, the branches of which can be seen in Figure 1.

Figure 1  
*Secret Writing Branches*



*Note.* Information on secret writing branches has been assembled from *The Code Book* by Simon Singh (1999, p. 30).

Cryptography is used to hide the meaning of a message, as in codes, whereas steganography is used to hide the entire message, as in microdots (Singh, 1999, p. 7). Misleading the enemy is a practice used often to confuse and intimidate. Besides verbal and written communication, other surveillance devices may be used to delude an opponent. For example, “placebo” cameras are sometimes placed in large cities to deter thieves and vandals. The Panopticon, a prison scheme where “only a few guards—if any—are needed to watch a whole prison population,” places convicts in a position where they have no choice but to believe that they are being watched at all times (Kammerer, 2004, p. 464). If prisoners think they are being watched, then guards will most



likely have nothing of interest to keep track of and stop surveying, creating an easier job for security officials but still keeping inmates in check. Another important way to keep track of people is by maintaining files and lists. They are used to gain a maximum amount of information on a subject as well as to compile an “enemies list” for potential violent purposes (Donner, 1980, p. 416). Donner discusses in his book certain lists, such as the Rabble Rouser Index, which were created to identify dangerous subjects or “individuals prominent in stirring up civil disorders” (pp. 15, 166). Modern databases have improved these lists and have made it easier for intelligence groups to track suspicious persons.

In addition to misleading the opposition, there is a wide variety of other arts of intelligence. Practices such as propaganda, deception, infiltration, blackmail, and informers are just as important and dangerous as the use of spyware (Donner, 1980, p. 9). Donner has compiled a broad list of responsibilities which may be given to an informer:

“...stealing keys, furnishing diagrams and office layout drawings for use in break-ins; identifying photographs; interpreting cryptic communications overheard by tappers; alerting his control agent to a scheduled telephone conversation considered important enough to spot-tap...supplying information to be used as a basis for a ‘reliable informant’ affidavit to legitimate electronic eavesdropping or other forms of surveillance” (pp. 135-6).

Most films involving intelligence, such as *The Recruit*, feature some sort of informer who must retrieve an important piece of information. In past intelligence operations, informers have not been limited to humans. Pigeons, for example, carried messages during both World Wars and had a 95-percent success rate (International Spy Museum). The CIA tried to teach birds to carry cameras, but training proved to be too extensive; after an attempt with small mechanical birds

failed, the project was abandoned (Richelson, 2001, p. 148). Richelson also discusses the use of cats as audio surveillance devices, a project called “Acoustic Kitty” which was dropped due to its impracticality (p. 147). Despite the failure of these animal informers, most other intangible spy tactics have made great steps in the world of intelligence.

### **What are some of the training procedures?**

It may come as no surprise to learn that training for the CIA is rigorous and is only open to those who are recruited into the program. Moreover, recruiting is done clandestinely, as evident in the film *The Recruit* when Walter Burke (Al Pacino) circles the letters C, I, and A in a newspaper to indicate his objective. According to Robinson (2006), training to be an officer in the CIA takes five years and involves training at Camp Peary (also known as “the Farm”), language school, and an overseas tour (p. 39). While classroom training is important to new officers, only practice can effectively produce a good spy. During their time at “the Farm,” recruits are placed in real-life situations to simulate possible missions. There, they learn basic skills such as observation, debriefing, and memory improvement. Retaining memories is especially important for spies because they are often in situations where they cannot record information. More importantly, they cannot carry around personal documents and they must memorize their covers, terrain, and countless passwords (Barth, 2004, p. 26). Training is also a time to learn how to lie and deceive; many CIA officers have admitted that “training changes you” (Donaldson).

It is interesting to note that *The Recruit* is the first film to be set at a CIA training facility, and testimonies from actual officers have confirmed that much of what is seen in the film reflects actual training at “the Farm.” During the course of the film, recruits learn how to destroy

vehicles, use weaponry, defend themselves, read polygraphs, trick the opponent, and bug a house. At the real “Farm,” recruits learn how to use weaponry, defend themselves, run surveillance to determine whether they are being followed, handle explosives, use secret writing techniques, take photos, and sketch (Donaldson; Donner, 1980, p. 432). Walcott and Duffy (1994) add to this list training on how to write reports, gather information at parties, and take part in a “jail sequence” (p. 39). There is, in fact, a jail sequence in *The Recruit* in which James Clayton (Colin Farrell) is caught and placed in a fake prison until he gives the name of his supervisor to his interrogator. While there are large similarities between the film and what the CIA has chosen to disclose about its training facilities, some secrets must remain private.

The recruits being brought into training facilities are chosen for very specific reasons, usually for a special skill. Due to American relations with Arabic-speaking countries, it is likely that more Middle Easterners are being recruited. Said Waller in his 1992 article, intelligence agencies “still want a spy like the one you read about in a John le Carré novel...but now George Smiley will have to speak Japanese” (p. 27). The Mormon population is being heavily recruited because of their missionary work, which often results in mastery of a foreign language, not to mention their clean records (Waller, 1992, p. 27). People with other specialized skills are also being recruited, such as physicists, chemists, and businessmen. In addition, 40 percent of the recruits in 1993 were female, and the number was slowly rising (Waller, 1993, p. 32). Waller also mentioned the increase in number of husbands and wives being recruited together (1993, p. 32). The increase in female recruits can be surmised as a misleading tactic since spies tend to be male; neither the opposition nor the general public suspect women to be in positions of potential danger.

A specific type of officer, the non-official cover (NOC), plays an important but secret role in the CIA. The concept of a NOC is very important in *The Recruit*, ending with confusion on the part of a misguided administrator. In the film, two different people, each working alone, are assumed to be the NOC. Real NOCs perform “non-official cover” work at embassies or other security agencies under fictitious job titles (Robinson, 2006, p. 41). They have no ties to the government in order to protect intelligence organizations. One of the most important lessons that officers, and especially NOCs, are taught is to not get caught. Such lessons are taught in jail sequences during training, as well as in other procedures. There may be a great deal of pressure on any recruit who is chosen to be a NOC, since according to Burger (2005), the “US would deny any link to [them] and offer...no protection from prosecution or even execution if caught” (p. 25).

### **How has espionage changed?**

One of the most unique aspects of the Cold War was that it was fought differently than any other battle in history. Instead of a frontline with soldiers and weapons, most fighting was done behind the scenes via spies and other reconnaissance techniques. Secrets about nuclear warfare instilled a “threat of a total catastrophe that could be perpetuated by a few spies” (Miller, 1999, p. 36). Moreover, surveillance became the major weapon used in backstage battles. Says Virilio (1984), the “eye,” meaning any type of observation, functioned as a weapon (p. 3). Surveillance technology was never thought of as a means of artillery until the Cold War, at which time weapons were defined as “tools not just of destruction but also of perception” (Virilio, 1984, p. 6). The same form of battle continues today, evident from the 9/11 attacks. Since Al Qaeda’s attacks on the World Trade Centers, America’s intelligence agencies have made major

changes in the ways they train officers. Moreover, technological surveillance has improved and transformed to meet the needs of modern observation of potential terrorist activities. In 2001, Verton described the proposed security budget of the Bush administration for the following year:

**\$10 million** to fight cyber-crime and enforce intellectual property laws

**\$9.2 million** to the Department of Justice for computer equipment, forensic research tools, and a background-check system for the National White Collar Crime Center

**\$1.5 million** to the National Center for Rural Law Enforcement Technology for facial-recognition devices (p. 14).

In addition to these plans, the FBI seeks to locate sleeper cells (small groups of terrorists who lie dormant until ready to strike) in the United States (Verton, 2001, p. 14). Since these groups live in the country legally and they have the same rights as Americans, ordinary citizens feel threatened not only by the concept of living among terrorists, but also by the possibility of being observed with even more scrutiny. They have reason to be scared; by spying on Americans, intelligence agencies are not just gaining information on potential terrorists, but they are uncovering more information on these “innocent” citizens and taking care of domestic issues as well (Harris, 2006, p. 47).

Access to certain records and databases have unlocked important keys to terrorist groups and plans. Through such information, 9/11 hijackers have been identified, terrorist plots have been uncovered, and small details about the attacks have been analyzed to prevent further assaults. The National Security Agency was given access to telecommunications companies across America and then used their information to track down the frequency and means of calls made by terrorists (Harris, 2006, p. 48). The FBI reported, however, that despite such an important authorization, most of the webs the security agencies created from the people whom

the terrorists had called “led to dead ends or to innocent Americans,” again resulting in fear among those who are not guilty (Harris, 2006, p. 48). In addition to record searching, training through American intelligence groups has increased since the attacks of 2001. According to Robinson and Whitelaw (2006), CIA “clandestine case officers” have risen by 50 percent to 1,800 officers (p. 36). Despite the increase in recruits, the golden rule of quality over quantity becomes even more critical. Especially since administrative staff continues to shuffle, there are fewer people to train recruits and head recruiting missions, so many new officers could be highly inexperienced. Despite staff changes, it is obvious from films like *The Recruit*, albeit a fictional story, that the interest in joining a security agency or any military branch has skyrocketed.

With the increase in security agent recruits and trainees, one would think that humans are being specially trained with more attention to detail. The emphasis, however, is on technology used for such agencies, resulting in less specialized personnel who, unlike machines, require training and practice in their fields. Training, says Barth (2004), involves “developing mental and emotional strengths, not playing with a bunch of way-cool experimental gadgets and a tricked-up Aston Martin” (p. 16). While spyware is important in specific situations, the skills necessary to know when, where, and how to use them are crucial. It does not matter how many computers and satellites there are, says CIA Officer Chase Brandon; it all comes down to people (Donaldson). While intelligence agencies surely recognize the need for human intelligence, evident by their increase in language and other specialized training, it seems that more news is related to new technological developments and not recruits studying abroad to learn Farsi. The concept of humans versus technology is not new: “Before Iraq invaded Kuwait, the CIA had satellites to track Saddam Hussein’s forces but no agents in Baghdad to let Washington know what he intended to do with them” (Waller, 1992, p. 27). Now that another new satellite has been

proposed, many wonder if it will really benefit the security of the nation. “It’s not too late to stop this program,” says a former government official, “before billions of dollars are spent on something that...may add nothing to our security” (Jehl, 2001, p. 1.1). In the film *Minority Report*, the main message is that “Technology doesn’t fail. It is humans that fail” (Kammerer, 2004, p. 469). While this may be true in some ways, it has become more obvious that humans are not machines, and to produce positive results with them, they must be trained. Despite what James Bond and Inspector Gadget may demonstrate, technology is not the only part of espionage necessary to conduct superior surveillance.

Reconnaissance is not as “easy” as flying U-2 planes over specific regions and bugging central command centers anymore, chiefly because the opposition is not located in one place. Instead, espionage centers on “tapping into the amorphous, high-speed communications all around us, both in the wireless space and on the Internet” (David, 2005, p. 17). Since opponents are dissimilar and more dangerous, they are harder to identify, creating a sort of “asymmetrical” warfare (International Spy Museum). There have been major changes in the way war is conducted, especially since 9/11. Battles are no longer fought with weapons and tanks, but with ideas and fear. Although spyware is still used, the “spies” have become people sitting at desks filtering through records and terrorist communications. American soldiers are “fighting” in Iraq, but it is mathematicians who are “at the forefront of the battle to break...codes” (Singh, 1999, p. xv).

As the nation is threatened with new approaches to terrorism, particular elements of surveillance become more important than others. With the shift in reconnaissance tactics, ethical questions have risen regarding the nature of privacy. The current issue of illegal NSA wiretapping consumes news reports and has the country on edge about confidentiality. The

increasing use of spyware by consumers has also changed Americans' consciousness of being observed. Insight from some of the spyware used by intelligence agencies in the past has influenced the technology being invented today, and some cases of failure have resulted in large changes in recruiting and training of national security personnel. The war being fought today is different and more difficult than any other in history, and spy technology is being adapted to achieve effective surveillance. Now that America's battles no longer involve rifles and revolvers, the most significant war-related challenge facing the country is the machine and human-aided development of impenetrable espionage programs.



## References

- Barth, J. (2004). *International Spy Museum handbook of practical spying*. Washington, D.C.: National Geographic.
- Benson, L.R. (2004). Secret empire: Eisenhower, the CIA, and the hidden story of America's space espionage (book). *Air Power History*, 51(1), 55.
- Burger, T. (2005). Recharging the CIA. *Time*, 166(23), 25.
- Charlesworth, A.J. (2003). Opinion, privacy, personal information and employment [Electronic version]. *Surveillance & Society*, 1(2), 217-222.
- David, M. (2005). Spying has come a long way since deep throat's heyday. *Electronic Design*, 53(13), 17.
- Donaldson, R. (Director). (2003). *The Recruit* [Motion picture]. United States: Touchstone Pictures.
- Donner, F. (1980). *The age of surveillance*. New York: Knopf.
- Farmer, D. & Mann, C.C. (2003, May). Surveillance nation. *Technology Review*, 106 (4), 46-52.
- Gorman, S. (2006, May 8). Bush's expected CIA pick assaulted. *The Sun*, pp. 1A, 6A.
- Harris, S. (2006). How does the NSA spy? *National Journal*, 38 (3), 47-49.
- Interagency OPSEC Support Staff. (1996). *Intelligence Threat Handbook*. Greenbelt, MD: Interagency OPSEC Support Staff.
- International Spy Museum. Washington, D.C. Visited April 8, 2006.
- Jehl, D. (2004). New spy plan said to involve satellite system. *The New York Times*, p. 1.
- Kammerer, D. (2004). Video surveillance in Hollywood movies [Electronic version]. *Surveillance & Society*, 2(2), 464-473.

Miller, S.P. (1999). *The seventies now: culture as surveillance*. Durham, North Carolina: Duke University Press.

National commission for the review of federal and state laws relating to wiretapping and electronic surveillance. (1976). *Electronic surveillance*. Washington, D.C.: U.S. Government Printing Office.

O'Malley, C. (1998). Digital spy stuff. *PC Computing*, 11(10), 251-257.

Richelson, J.T. (2001). *The wizards of Langley*. Boulder, Colorado: Westview Press.

Robinson, L., & Whitelaw, K. (2006). Seeking spies. *U.S. News & World Report*, 140(5), 35-41.

Schorr, D. (2006, January 6). Secret surveillance is not new. *Christian Science Monitor*, p. 9.

Shaffer, J. (2006, February 10). Like it or not, secret surveillance is here to stay; the Cold War resulted in a permanent expansion of intelligence gathering. *Christian Science Monitor*, p. 9.

Shannon, E. (1999). It's still spy vs. spy. *Time*, 154 (25), 75.

Singh, S. (1999). *The code book*. New York: Anchor Books.

Smithsonian National Air and Space Museum. Washington, D.C. Visited April 8, 2006.

Spielberg, S. (Director). (2002). *Minority Report* [Motion picture]. United States: Twentieth Century Fox.

Thompson, M. (1999). Spies will be spies. *Time*, 153(10), 29.

U.S. Congress House. (1975). *Secret Service and Internal Revenue Service surveillance and records policies*. Washington, D.C.: U.S. Government Printing Office.

Verton, D. (2001). Feds boost online surveillance activity. *Computerworld*, 35(50), 14.

Virilio, P. (1984). *War and cinema: the logistics of perception*. New York: Verso.

Walcott, J., & Duffy, B. (1994). The CIA's Darkest Secrets. *U.S. News & World Report*, 117(1), pp. 34-44.

Wallace, C. (Host of FOX News Sunday). (2006, May 12). FOX 45 Morning News [Television broadcast]. Baltimore, MD: FOX 45 News.

Waller, D. (1992). The CIA's next generation. *Newsweek*, 119(7), 27.

Waller, D. (1993). The CIA's new spies. *Newsweek*, 121(15), 30-32.

Whitty, M.T. (2004). Should filtering software be utilized in the workplace? Australian employees' attitudes towards Internet usage and surveillance of the Internet in the workplace [Electronic version]. *Surveillance & Society*, 2(1), 39-54.

Yost, G. (1985). *Spy-Tech*. New York: Facts on File.