Only by understanding the threats and the basics of the tradecraft utilized to facilitate industrial espionage can an organization develop an effective counterespionage program. A review of espionage tradecraft will include the intelligence cycle, the categories of intelligence collection, and the methods of collection.

The Intelligence Cycle

There are five-steps in the intelligence process called the Intelligence Cycle. This process ensures the collection process is done correctly by use of a system of checks and balances.

Planning and Direction

Planning is the first phase of the process during which the decision is made concerning what intelligence is required, the sources of the intelligence needed, how it will be collected, and the value of such information. At this stage, the target company or individual will be identified. The type of information required from the target is then decided. The methods of collection will be decided upon and the techniques of using such collection methods must also be determined.

The budget must also be determined. This will include salary of agents; cost of collection equipment to be used, travel, possible hotel cost and other expenses. The funds, if any, used to pay for information retrieved through espionage must also be considered.
The collection phase is the gathering of intelligence information overtly (openly) and covertly (secretly). Examples of open-source information include reading foreign newspapers and magazine articles, listening to foreign radio, and watching overseas television. Other information sources may be covert (or secret), such as illegal information collected with listening devices and hidden cameras.

**Processing**

This phase of the intelligence cycle deals with taking all of the information collected and putting it into a usable intelligence report for the customer. The final product may be a report, photographs, video, charts, maps and graphs or a voice recording. Whatever the media chosen, it must be formatted in a form that can be used and based on what the customer requires.
Analysis and Production

During this phase, all the collected information is reviewed for quality and value and is formatted into the final product. This final written report or collection of photographs/video, charts, maps and graphs or voice recording, however the intelligence was processed, is put to use. In some situations, it may be determined at this phase that addition intelligence is required at which point the collection cycle begins again.

Dissemination

In this final phase of the cycle, the final written analysis is provided to the intelligence customer. The customer may come back with more questions. Then the whole process starts over again.

Categories of Intelligence Collection and Tradecraft

Within the intelligence community there are five categories of intelligence collection. The intelligence categories are identified by the type of intelligence and how it is collected.

- Human Intelligence (HUNINT)
- Imagery Intelligence (IMINT)
- Open Source Intelligence (OSINT)
- Signals Intelligence (SIGINT)
- Measure and Signatures (MASINT)

Human Intelligence (HUNINT)

Human intelligence is derived from or collected by human sources such as agents, informants, and human assets. Human intelligence is the most common method used for industrial espionage. The reason is that an individual or asset can be recruited from the target company. This will afford the asset both the access and long period of time required to collect the targeted protected information.

Methods of Recruitment

When a foreign nation, competitor, freelance espionage operative, or terrorist organization seeks to obtain protected...
information from an organization, there is, of course, the requirement of access to the information they are seeking. The goal is to obtain the information covertly, without the knowledge of the organization they are stealing it from, by photographing, photocopying, downloading the protected information from a computer system or transmitting it electronically while leaving the original source of the information intact. In this way, the target organization will not realize that information is being stolen thus allowing the perpetrator to continue the industrial espionage indefinitely and often for many years.

The country, organization, or individual seeking such information can attempt to infiltrate the target company. Not being an employee with approved access, it is not be easy to infiltrate the company in most cases. Human intelligence collection may also include the use of pretexts to gain information from individuals by phone, e-mail, or in person. A pretext may also be used to gain access into a targeted organization. The pretext may be appearing as a customer, a public utilities inspector, a delivery person, or a building inspector.

Covert entry is possible, but if successful, it only allows one time access to the protected information. Obtaining employment for the purpose of espionage will allow long term access. To obtain employment, there must be an opening and the organization agent who will carry out the espionage must meet the position’s requirement, pass security investigations, and be hired. This is not always achievable and if the person does obtain the position, it can take considerable time before he or she has access to the desired information. The agent must also study and work around the security program that is in place in order to obtain the required information through espionage.

The most effective method of information collection would be to recruit an employee, referred to as an asset or mole, who is already working at the target organization and who has access to the protected information the organization seeks to obtain. The asset will know the security procedures and physical security systems that have been established to prevent espionage. With this knowledge, the asset can easily circumvent the security systems. By recruiting a current employee, there is the expectation of long term access to protected information, which could last for decades. Using a current employee at the target location as an asset is not only of value to the agent or handler, this method also reduces the risk to the agent or handler.
the asset handler from identification and possible arrest for industrial espionage.

The recruitment of an asset can take time, but if successful, can result in the collection of an enormous amount of information over many years. The goal of the recruitment process is to find the right asset within the targeted company. When selecting an asset, there are several primary methods of recruitment to secure the asset’s cooperation.

Most cases of industrial espionage where human intelligence is utilized involve the asset’s desire for monetary gain. This need for money may just be to live a more enjoyable lifestyle. It may be to pay for expensive habits or addictions such as drugs, alcohol, gambling, sex, or just the need to buy things. It may also be due to health issues wherein the asset needs money to pay medical bills or routine bills and credit cards. If may also be due to divorce actions and the need to make payment to the former spouse and legal fees.

To recruit these employees as assets, the handler will gather intelligence on the various employees of a company to identify those in need of money due to debt, divorce actions, addictions or medical issues. This information may be obtained by searching public records of divorces or bankruptcy filings. Other methods might include frequenting restaurants where employees of the target company gather and to listen and to get to know individuals. A particular individual may be targeted based on his or her position in the target company.

Once a possible asset is identified, the handler will befriend the asset, get to know him or her and at some point will offer to help resolve the situation by offering extra money for information. Initially, the information requested may seem innocent such as an employee directory. The handler will gradually upgrade the information requested as he or she continues to pay for information.

Should the asset desire to discontinue stealing and providing the protected information requested, the handler will attempt to blackmail the asset. In most cases, the handler will document the transfer of protected document and payment with photographs or recordings. If the asset at some point in time wishes to discontinue the espionage, the handler will then expose this evidence and threaten to tell the asset’s employer or even law enforcement about the theft of the protected or classified company information. In some situations, an
individual will approach an intelligence agency, criminal or terrorists
group and offer to conduct espionage for them.

Blackmail can also be used as the initial method to recruit an asset.
The handler will arrange placing the prospective asset in a compro-
mising position and document it. Most often this is a sexual compro-
mise called a honey trap. If the target asset is married then there is
the threat to turn over documentation of the discretion to the spouse.
The sexual activity may also be homosexual or other activity such as
bondage. The evidence of the compromising situation, no matter what
it may be, will then be used as the leverage for blackmail in return for
conducting espionage.

In some cases an individual’s ideological or religious views may be
used to turn the individual into an asset for the cause. Such individuals
may even serve as an asset without the payment of funds because it is a
cause or religious view that they support. The cause may be socialism
over capitalism, or it could be an environmental issue. The religious
view is often used when espionage is conducted by Islamic nations or
Islamic terror groups. The religion, if Islam, often encompasses all
aspects of the believer’s life including political, religious, and personal
lifestyle. Regardless of how assets are recruited once they have stolen
protected information or divulged secret information they are trapped
and cannot walk away.

Once recruited, the assets receive training from their handlers on
the tradecraft of espionage and the various collection methods. The
asset is trained both on how to collect information and also what
information is to be targeted. The most secure methods of obtaining
the target information are also covered in the training.

In addition, the asset is trained on the way to contact the handler in
order to pass on the information. The first step is to inform the han-
dler that information or money needs to be picked up. The most com-
mon method is to have prearranged items identified such as a light
pole, mail box, or park bench. If there is to be a pick up or drop off,
place a chalk mark or tape on the item as notification of the exchange
of information or money.

To accomplish the transfer, several methods are commonly uti-
lized. One is the brush pass technique. This requires skill and coor-
dination, but it is an effective method. Two or more agents literally
brush past one another, passing the information or money from hand
to hand as they go by. This may be done any number of places, but is accomplished most effectively and securely in very busy areas where there are large crowds. Variations include standing together on a busy train or passing documents between restroom stalls in a busy public washroom.

A dead drop or dead letter box can also be used in an unpopulated area at a pre-planned location. The agent loads the dead drop by placing the item for later collection by another agent or the asset, be it information or money. This method alleviates the need for the two individuals to be in the same place at the same time. Examples include hiding information or money in a soda can, under a rock or other item, or in a hollow tree.

The use of a live drop or live letter box is also common. This is similar to the dead drop except that a person is used instead of an object. For example, the agent brings his suit to the drycleaners, where a person known to the agent works. Inside his jacket will be the letter that needs to be transferred. To any surveillance watching, the agent is just dropping off laundry. Later, another agent will come in to retrieve his suits and will be given the letter by the employee, probably inside one of the suits.

**Imagery Intelligence (IMINT)**

Various forms of technical surveillance are employed for industrial espionage. Use of imaging techniques to collect information through industrial espionage ranges from mobile phones, cameras, professional digital cameras, or videos operated by individuals on the ground, in motor vehicles, or in small aircraft. In many industrial espionage operations where the information is collected by an agent on the ground or an asset in a targeted facility, the images may be collected with a handheld, full-size or miniature digital camera or a disguised digital camera concealed in a pen or within some other common item that an individual would normally carry.

The images collected may be existing digital photographs that have been illegally downloaded from a computer. The illegal image may be an existing photograph that can be copied on a copy machine, scanned into a computer, and downloaded or re-photographed with a camera.
The most recent technology involves the use of very small unmanned aerial vehicles or UAVs. These small airborne platforms are used in the collection of information in remote areas or where there is no visibility from the ground view or surrounding terrain. Satellites that can record images from space may be utilized if the industrial espionage is being conducted by foreign nations that have the technology to use satellite imagery for espionage collection. Imaging techniques may also be used to obtain information on a targeted item. The video camera is most often used by organizations that are gathering intelligence on a possible target location for a terrorist attack.

These techniques may also be used to document individuals, the movement of individuals, or security force operation for a terrorist attack against an individual or a facility. Imagery of a target facility may also be acquired to facilitate a clandestine entry into the target property.

Open Source Intelligence (OSINT)

As discussed under human intelligence, open source intelligence is the collection of public domain information that is legally available to anyone. Public information is not always free information. There may be a fee to access the information. The primary difference between open source information and trade secrets is that there is a public right to access of the information in some form.

The gathering of intelligence from sources available to the public such as print material, Internet, video clips, and photographs is open source collection. This is legal. Much useful intelligence can be obtained using this method with no risk to the individual collecting the information whether the asset that was recruited or an intelligence agent or handler.

Open-source information can also come from governmental organizations, trade and professional organization publications, conferences, information from the target company’s own web page and publications, and trade shows. An example of a federal government source would be Securities and Exchange Commission filings which are a requirement of publicly-traded companies. Annual and quarterly reports can be obtained through this source. Information on stock holders and income statement can also be accessed.
All states require that companies doing business within their jurisdiction register, in most case with the secretary of state. Information on the target corporation, the officers and other vital information can be obtained. Plans of a target companies including their plans for expansion can be obtained from a local court house where deeds and transactions are filed.

Trade and professional organization publications such as Dun & Bradstreet and Lexis/Nexis databases can also be an open source of intelligence. Organizations provide intelligence on their company websites and social links such as Facebook, Twitter, and LinkedIn. A target organization’s booth at a trade show provides an excellent opportunity to collect information about that company both from handouts being distributed and by talking with a company representative.

Special methods of open source tradecraft include observing how many trucks a company is using to move goods and the time of movements. This can give an indication as to the amount of business the company has. Dumpster diving, or going through an organization’s trash can yield valuable information and is legal in most areas as long as the trash has been placed at the curb. It would be illegal to access a company’s property to explore and remove their trash in most areas.

Another method is to go to a local eatery where employees of a nearby company go for breakfast, lunch or to meet after work. By sitting near the group and listening, much open source information about the company can be learned from the conversations. It is also possible to become involved in conversations and gather even more information.

Posing as a customer of a company is still another excellent method of obtaining open source information. Company representative are willing to do what it takes to please customers and will provide the customer with much information.

Signals Intelligence (SIGINT)

Signals intelligence is information derived from the interception of signals from communications, electronics, and telemetry. It is the interception of communication. This includes the use of technology to intercept oral communication, telephone communication, and e-mail communication between individuals and organizations.
SIGINT consists of:

- Communications Intelligence (COMINT)—technical and intelligence information derived from intercept of foreign communications.
- Electronic Intelligence (ELINT)—information collected from systems such as radars and other weapons systems.
- Foreign Instrumentation Signals Intelligence (FISINT)—signals detected from weapons under testing and development.

Methods of monitoring oral communication between individuals can be accomplished with the use of a parabolic microphone, microwave interception, and hard-wired or wireless microphones and transmitters. The transmitters may be FM or a spread spectrum broadband radio signal. This type of monitoring can even be accomplished with a modified mobile phone left in a targeted room. If the mobile phone is discovered, one might assume it was just left in the location by accident and not for the purpose of industrial espionage.

Such listening and transmission devices can be concealed in most any object. This is especially true if device is battery operated. If the device is hard-wired, then it will be hidden where there is access to an electric source such as a light switch or wall outlets.

The monitoring of telephone communication is a common source of information. This can be accomplished using a series wiretap that monitors one side of the phone conversation or a parallel wiretap that monitors both sides of the phone conversation. Such surveillance equipment can be positioned at numerous places along the telephone line.

The surveillance of e-mail transmission can be accomplished by use of a key logger that allows access to the target computer or by the use of spyware that allows remote access to the target computer. These and other methods will be discussed further in the text under cyber security.

**Measure and Signatures (MASINT)**

Measure and signatures intelligence is derived from acoustic and radiation sources. Examples of this type intelligence include information related to nuclear and sound activity from which vital information can be gained.
There are several important distinctions between MASINT and the other categories of intelligence that have been discussed. MASINT is a relatively new technology and has very diverse options for use. Many MASINT-based systems are used in a variety of roles for intelligence collection just as varied as intruder detection systems or strategic missile launch warning systems are used. MASINT-based systems for the most part are used by government military or intelligence services for the collection of protected information, battle information, or for state security matters, and counterespionage activities. An organization being targeted with MASINT, in most cases, is facing a serious and qualified espionage threat as the adversary is most likely a foreign government intelligence service seeking highly protected and classified information.

The following are included in measures and signatures collection:

- Radar Intelligence (RADINT)
- Acoustic Intelligence (ACOUSTINT)
- Nuclear Intelligence (NUCINT)
- Radio Frequency/Electromagnetic Pulse Intelligence (RF/EMPINT)
- Electro-optical Intelligence (ELECTRO-OPTINT)
- Laser Intelligence (LASINT)
- Materials Intelligence
- Unintentional Radiation Intelligence (RINT)
- Chemical and Biological Intelligence (CBINT)
- Directed Energy Weapons Intelligence (DEWINT)
- Effluent/Debris Collection
- Spectroscopic Intelligence
- Infrared Intelligence (IRINT)

Deception and Pretext Tradecraft

In the world of industrial espionage, deception is used to obtain protected information. Most often the deception is in the form of a pretext. A pretext as it relates to industrial espionage involves assuming an identity or appearance other than one’s own in order to cloak the person’s real intentions which are the solicitations of protected information. Some forms of pretexts are legal as long as one is not using...
false identification, wearing uniforms or representing himself or herself as a law enforcement officer or a public utility employee. Even if the pretext is not illegal, depending on the how the pretext was used, civil action could result for the invasion of privacy or other damages that may have occurred.

There are many pretexts that can be used to solicit information. The primary premise of a pretext is to hide one’s real identity or motives. This is often accomplished by utilizing false credentials and dressing to the part that may include the wearing of uniforms based on the nature of the pretext. Some pretext attacks require no false credential or special dress or uniforms at all.

With the capability of computer publishing and copying, the creation of totally fictitious identifications or the fraudulent reproduction of real identifications is quite easy. Digital photography photos and logos can be inserted on the false identification. The fictitious identifications that are created could be those of a public office holder, a law enforcement officer, private investigator, utility worker, news reporter or delivery worker. The identification might be a fraudulent reproduction of a company’s real identification that the perpetrator wants to access.

Dressing for the part includes a fraudulent uniform of a police officer or a delivery worker from a nationally known company. Often it includes a jacket, sweatshirt or other garment with a fraudulent logo imprinted on the garment to provide the illusion that the person represents a legitimate company.

The ploys are limited only by the imagination when it comes to the use of deception and pretexts in facilitation of industrial espionage. Examples include seeking employment, writing a college paper, seeking a news story, delivery, or trying to locate a friend or business associate.

Before an individual uses a pretext for industrial espionage, he or she will conduct a background inquiry on the target or target location. If the target is a person, as much information as possible will be obtained in advance such as address, work location, vehicle driven, family members, travel routine, and routine stops during travel.

If the target is a location, the hours of operations will be identified, along with employee and visitor traffic patterns. The physical security such as security cameras, intrusion detections system and access control will be determined. The number and type security force will also
be identified as well as the movements, shifts, and schedules of the security force members.

In some situations, the actual pretext attack may commence with a telephone call to the target or target company to obtain information that can be used in person at the target location. The phone call may also be used to lay the ground work for the actual visit to the target location that would make that conclusion of the pretext successful.

An example of a case of industrial espionage in which there was the use of pretext involved three individuals associated with a private investigation firm in Florida. The three private investigators were found to have been using false identities to obtain the home records of board members, employees, and journalists. The employees of the private investigative firm were found guilty and have been sentenced in connection with a Hewlett-Packard spying scandal.

The private investigative firm was hired on behalf of Hewlett-Packard’s CEO to probe boardroom leaks to journalists in 2005. The three private investigators used pretexting. Using false identifications and by posing as account holders or employees of various phone companies, they were able to fraudulently obtain personal information on the target group which included board members, employees, and journalists. The information that the three private investigators obtained using a pretext included phone numbers, dates of birth, social security numbers, call logs, various billing records, and detailed subscriber information. The private investigators also obtained confidential information belonging to Hewlett-Packard board members, employees and their families. They also obtained confidential information on reports for Cnet, the Wall Street Journal, the New York Times, and the journalists’ families.

The investigative firm stated they used such pretext methods for years and grossed up to $30,000 just on that practice alone. Pretexting and the sale of phone records obtained using the technique led to a national controversy and congressional hearings on the subject. The Federal Communications Commission conducted its own investigation of the incident.

As stated previously, some forms of pretexting are legal; the pretext methods these investigators used were not. Their actions were also unethical and were not actions in which a professional private investigator or private investigative or security should participate.
Bibliography


