WIKIPEDIA
The Free Encyclopedia
WIKIPEDIA

Clandestine HUMINT operational techniques

The **Clandestine HUMINT** page adheres to the functions within the discipline, including espionage and active counterintelligence.

The page deals with **Clandestine HUMINT operational techniques**, also known as "tradecraft". It applies to clandestine operations for espionage, and a clandestine phase before direct action (DA) or unconventional warfare (UW). Clandestine HUMINT sources at certain times act as local guides for special reconnaissance (SR).

Many of the techniques are important in counterintelligence. Defensive counterintelligence personnel needs to recognize espionage, sabotage, and so on, in process. Offensive counterintelligence specialists may use them against foreign intelligence services (FIS). While DA and UW can be conducted by national military or paramilitary organizations, al-Qaeda and similar non-state militant groups that appear to use considerably different clandestine cell system structure, for command, control and operations, from those used by national forces. Cell systems are evolving to more decentralized models, sometimes because they are enabled by new forms of electronic communications.

This page deals primarily with one's assets. See double agent for additional information adversary sources that a country has turned to its side.

Staff and skills in a clandestine HUMINT operations station

This description is based around the foreign intelligence service, of **country B**, operating in and against **country A**. It may also include operations against non-state organizations operating in **country B**, with or without **country B** support. It may also involve offensive counterintelligence against **country D** assets operating in **country B**.

The basic structure here can be pertinent to a domestic service operating against a non-national group within its borders. Depending on the legal structure of the country, there may be significant, or very few, restrictions on domestic HUMINT. The most basic question will be whether criminal prosecution, or stopping operations, is the goal. Typically, criminal prosecution will be the primary goal against drug and slavery groups, with breaking up their operations the secondary goal. These priorities, however, are apt to reverse in dealing with terrorist groups.

If there are separate organizations with diplomatic and nonofficial cover, there may be two chiefs. Sufficiently large stations may have several independent, compartmented groups.

Description	Soviet terminology	US terminology
Officers with diplomatic immunity	Diplomatic cover, emphasizing that GRU assumed that the host nation assumed all military attaches were intelligence officers but that some diplomats might actually be diplomats	Diplomatic cover
Public association with the service's country, but no diplomatic immunity	Civilian cover (e.g., Tass news agency, trade or scientific delegation)	Not often used. Personnel with Peace Corps and certain other backgrounds are barred from intelligence. Some, decreasing, cover as journalists now rarely used
No affiliation with host nation government	Illegal (usually with an assumed identity)	Nonofficial cover (NOC). May use real name or not, but often some invented background

Station under diplomatic cover

Nations vary as to how well hidden they choose to have all, part or none of their intelligence personnel under the guise of diplomatic immunity. Frequently, at least one individual is known to the host country, so there can be a deniable channel of communications. If the nations are allies, many of the intelligence personnel may be known and actively cooperating.

Certain diplomatic titles were often assumed to be cover jobs. With the United Kingdom, "passport control officer" was, much of the time, an intelligence position.[1] Today, it may be confusing that some passport control officers actually control passports. With other countries, "cultural attaché" was often a cover job, although, again, it might be legitimate. An intelligence officer covered as a cultural attaché might still do some cultural things.

- Chief of station or *rezident*. There may also be multiple chiefs if "country B" has both military and civilian human intelligence. Fairly recently, the US consolidated military and civilian into the National Clandestine Service. Russia still probably separates GRU military and SVR civilian, and the KGB, the USSR-era predecessor of the SVR, ran both illegal and legal residencies.
- Operations officer, also called case officer: interacts with local assets or leaders of local agent subnetwork. Israel's Mossad refers to these as katsas.
- Collection management officer (aka reports officer, intelligence officer): does preliminary report categorization and organization. May be the administrative chief.
    - Communications and encryption personnel
    - Drivers and guards
- Operational targeting officer: not always used. May be more focused on access agents and recruiting, handing off recruited agents to case officers. Might make the decision to use non-HUMINT collection, such as SIGINT based in the embassy.

- Technical collection specialists (e.g., the US Special Collection Service, a joint NSA-CIA operation)

Stations under official but nondiplomatic cover

An intermediate approach has the officers clearly working for their country but without diplomatic immunity and with a cover role that does not immediately suggest intelligence affiliation. For example, the Soviet GRU covered some intelligence officers under the TASS news agency, or as part of a trade or technical mission, or even as diplomats. The last might seem surprising but this was under a GRU assumption that military attaches would always be assumed to be intelligence officers, but that members of the civilian part of an embassy might actually be diplomats rather than intelligence officers.[2]

It was easier, of course, for the socialist USSR to assign people to state agencies. Western sensitivities tend to be much greater about using, for example, journalistic cover. The US has been emphatic in prohibiting any relationship between intelligence and the Peace Corps.

US military intelligence doctrine forbids a HUMINT specialist to pose as:

- A doctor, medic, or any other type of medical personnel.
- Any member of the International Committee of the Red Cross (ICRC) or its affiliates. Such a ruse is a violation of treaty obligations.
- A chaplain or clergyman.
- A journalist.
- A member of the civilian government, such as a Member of Parliament.[3]

An example of civilian cover for an American officer involved a German refugee, with the pseudonym "Stephan Haller", who had widely ranging interests and special skills in mathematics and physics, as well as native language skill. His overt role, in 1949, was directing a program that paid subsidies to German

scientists, part of a larger program of denying German talent to the Soviets. Initially, he was based in Pforzheim, (West) Germany.[4]

During two years in Pforzheim, with a well-established cover, he collected political and scientific intelligence from the scientists and also Germans that he knew in political circles before emigrating. In 1951, he moved to Berlin, directing overall "operations against scientific targets in the East Zone of Germany", while still managing the subsidy program. His new work included encouraging defection of key craftsmen working for the Soviets. He was considered a master craftsman,

> He did not grow careless or conceited with success. Here remained a meticulous craftsman. Before he debriefed a source, he mastered the subject to be discussed. His agents were made comfortable not only by his cigars and beer but also by the easy flow of communication. And he did not end until he had every last scrap of useful information. He never failed, moreover, to remain alert for operational leads--potential agents, counterintelligence indicators, propaganda possibilities. When Haller was finished, there were no more questions to be asked. And though he groaned over the chore of putting it on paper, his reporting became thorough-and more than thorough, illuminating-for he rarely failed to make interpretive comments. [quotation?] [citation?]

Stations under non-official cover

According to Victor Suvorov, the Soviet reaction to losing networks operated from diplomatic missions – after the countries in which those embassies were located were overrun in the Second World War – was to emphasize "illegal" (i.e., what the US calls non-official cover) stations (i.e., residencies) for HUMINT networks. The illegal residencies were preferred to be in safe locations, perhaps of allies such as the United States, Great Britain and Canada.

Soviet operations were tightly compartmentalized, with strict need-to-know an absolute rule. "Undercover residencies support illegals, but only on instructions from the Centre without having any idea for whom they are working. All operations in support of illegals are worked out in such a way that the officers of the GRU undercover residency do not have one crumb of information which is not necessary. Operations are planned in such a way that there is no possibility of the illegals becoming dependent on the actions of the undercover residency." A lesson learned from the loss of espionage networks was to keep them small, subdividing them, with independent reporting to Center, when more agents were recruited.[5]

Moving new agents into illegal residencies

Suvorov explained that new agents were separated from official Soviet institutions only after the agent has compromised himself by giving Soviet Intelligence a significant quantity of secret material; making it impossible for the agent to go to the police. The separated agent then occupies one of three guises: the separated acting agent, the agent group and the agent residency.

Separated acting agent

Greatest resources are devoted to these agents; which provide the most important material. Once the central headquarters assesses the materials as sufficiently valuable, the doctrine is to temporarily stop obtaining new material from the agent and improve their security as well as their knowledge of espionage tradecraft. This training is preferably done in a third country, from which the agent might or might not be moved to the Soviet Union. Typical cover for an agent absence would be taking a vacation or holiday.

> Thence he will go back to his own country, but as an independently acting agent. He will be run exclusively by the Centre, in concrete terms the head of a section, even, in special cases, the head of a directorate and in extreme cases the deputy head of

> the GRU or the head himself. The running of such an agent is thus carried out exactly as the running of illegals is.

Agent group

Less valuable than a separated acting agent but still of importance, was the agent group, which migrated from diplomatic or civilian contact, to the in-country illegal *rezidentura* (resident and infrastructure), to direct communications with the center. The leader of such a group is called, in Soviet terminology, a *gropovod*, and is conceptually the only member of the group that communicates with Moscow. In reality, clandestine communications personnel may be aware of the direct contact, but newer electronics allow the leader to manage his or her only communications.

Suvorov makes the important point that "A group automatically organises itself. The GRU obviously considers family groups containing the head of the family and his wife and children to be more secure and stable. The members of such a group may work in completely different fields of espionage." The pattern of having groups that are self-organizing and have preexisting ties, making them virtually impossible to infiltrate, has survived the GRU and is common in terrorist networks.

> Other agents recruited by residencies are gradually organised into agent groups of three to five men each. Usually, agents working in one particular field of espionage are put together in one group. Sometimes a group consists of agents who for various reasons are known to each other. Let us suppose that one agent recruits two others. ... Thus to a certain extent the members of agent groups are completely isolated from Soviet diplomatic representation. The agent group is in contact with the undercover residency for a period of time, then gradually the system of contact with the residency comes to an end and orders begin to be received directly from Moscow. By various channels the group sends it material directly to Moscow. Finally the contact with Moscow becomes

> permanent and stable and the agent group is entirely separated from the residency. With gradual changes in personnel at the residency, like the resident himself, the cipher officers and the operational officers with whom there was once direct contact, nobody outside the Centre will know of the existence of this particular group. Should it happen that operating conditions become difficult, or that the embassy is blockaded or closed down, the group will be able to continue its activities in the same way as before.[5]

Agent residency

When the GRU attaches one or more illegals (i.e., Soviet officer under an assumed identity), the residency changes from "an agent residency into an illegal residency. This process of increasing the numbers and the gradual self-generation of independent organisations continues endlessly." Suvorov uses a medical metaphor of quarantine designed to contain infection to describe separating agents for improved security.

The GRU kept certain officers immediately ready to go into illegal status, should the host nation intensify security.

> These officers are in possession of previously prepared documents and equipment, and gold, diamonds and other valuables which will be of use to them in their illegal activities will have been hidden in secret hiding-places beforehand. In case of war actually breaking out, these officers will unobtrusively disappear from their embassies. The Soviet government will register a protest and will for a short time refuse to exchange its diplomats for the diplomats of the aggressive country. Then it will capitulate, the exchange will take place and the newly fledged illegals will remain behind in safe houses and flats. Afterwards they will gradually, by using the system of secret rendezvous, begin to establish the system of contacts with agents and agent groups which have recently been subordinated to the

> undercover residency. Now they all form a new illegal residency. The new illegals never mix and never enter into contact with the old ones who have been working in the country for a long time. This plainly makes life more secure for both parties.[5]

Again, Suvorov emphasizes that the process of forming new illegal residencies was the Soviet doctrine for imposing compartmentation. Western countries, especially those in danger of invasion, have a related approach, the stay-behind network. The US military definition, used by most NATO countries, is

> Agent or agent organization established in a given country to be activated in the event of hostile overrun or other circumstances under which normal access would be denied.[6]

In such an approach, both clandestine intelligence and covert operations personnel live normal lives, perhaps carrying out regular military or government functions, but have prepared documentation of assumed identities, safehouses, secure communications, etc.

A representative illegal residency

Vilyam Genrikhovich Fisher, usually better known by his alias, Rudolf Abel, was a Soviet intelligence officer who came to the US under the false identity of a US citizen, Emil Robert Goldfus, who had died in infancy but was used by the USSR to create an elaborate *legend* for Fisher. On coming to the US, entering through Canada, Fisher/Abel took over the control of several existing Soviet HUMINT assets, and also recruited new assets. Key assets for whom he was the case officer included Lona Cohen and Morris Cohen, who were not direct intelligence collectors but *couriers* for a number of agents reporting on US nuclear information, including Julius Rosenberg, Ethel Rosenberg, David Greenglass, and Klaus Fuchs.

His role was that of the "illegal" resident in the US, under nonofficial cover. Soviet practice often was to have two *rezidents*, one illegal and one a diplomat under official cover. He was betrayed to the US by an alcoholic assistant who defected to the FBI.

That Fisher/Abel only had one assistant, with operational responsibilities, is not surprising. Unless a clandestine station has a strong cover identity, the larger the station, the larger the possibility it may be detected by counterintelligence organizations. Beyond the station chief, the most likely person to be associated with the station, not as a case officer, is a communicator, especially if highly specialized secure communication methods are used.

Support services

Some clandestine services may have additional capabilities for operations or support. Key operational agents of influence are apt to be run as singletons, although political considerations may require communication through cutouts. Useful idiots can be run by diplomatic case officers, since there is no particular secrecy about their existence or loyalty. Valuable volunteers, depending on the size of the volunteer group, may work either with case officers, or operations officers brought clandestinely into the area of operations.

Transportation, Infiltration, exfiltration, logistics

Proprietaries, which can be large businesses (e.g., the CIA proprietary airlines such as Air America, which, in the interest of cover, often had the latest aircraft and flew commercial as well as secret cargo), often are not controlled from the local area, but by headquarters. Especially when the proprietary is a multinational company, and has some commercial business of its own, central control makes the most sense.

In looking at internal as well as external assets, remember the fundamental rule of clandestine operations: the more secure, the less efficient. Because espionage operations need rigorous security, they are always inefficient — they take a lot of time, energy, and money. Proprietaries can be an exception, but, even

though they make money, they can require additional capital to be able to expand in the same way a comparable private business would do so.[7]

Volunteer and proprietary support

Another kind of resource could include foreign offices owned or operated by nationals of the country in question. A step farther is a *proprietary*, or business, not just individuals, under non-official cover. Both kinds of business can provide information from recruitment, unwitting agents, or support functions. Small and medium aviation-related businesses have been popular US proprietaries, including Air America and Southern Air Transport.

Once the service has a presence in aviation, it may become aware of persons, in private business, civil service, or the military, who fly to destinations of interest. They may mention it in innocent conversation, such as at the airport's restaurant or bar. They also may be assumed to be going there, based by analysis of flight departure times, aircraft type, duration of trip, and their passengers or cargo.

Having routine access to an airport can reveal: "Who's coming and going, on and off the record? What's in the hangars and warehouses? What are the finances? Political connections and loyalties? Access to planes on the ground? Flight plans?" It must be emphasized that a transportation-related proprietary—truck stops, boat maintenance, and other industry-specific businesses, have to operate as a real business. Occasionally, they may produce a profit, and that can be confusing for headquarters financial managers, provide a local but perhaps traceable source of funds, or both.

Public relations firms have long been useful proprietaries.[8] In a given country of operations, or perhaps adjacent countries that are concerned about the actions of their neighbor, news releases placed by experienced public relations professionals can help mold relevant opinion. Care must be taken that the news release does not "blow back" on the clandestinely sponsoring country.

Another viable industry for proprietaries is natural resources exploration. If, hypothetically, a mining company operated in a country where there are both resources deposits and non-national group sanctuaries, a proprietary company could get information on both, and also provide access and support services. If the proprietary began mining operations, it would naturally have access to explosives, which might be made available to sabotage groups in neighboring areas.

Use of nongovernmental organizations (NGO) is politically sensitive and may require approval at the highest level of an agency. Sometimes, there is a broader policy need not to have the possibility of drawing suspicion onto an NGO. For example, in World War II, it was occasionally necessary to send supplies to Allied POWs, but Red Cross parcels were never ever used for this purpose. The decision had been made that Red Cross parcels were important to the survival of the POWs and could never be jeopardized.

Safehouses

"Safehouse" is a term of intelligence tradecraft whose origins may be lost in antiquity. "The Bible is also replete with instances of espionage, including Yahweh's instruction to Moses to send spies into the land of Canaan. The account of the harlot Rahab sheltering Israelite spies and betraying the city of Jericho might be the first documented instance of a "safe house.' "[9]

The term is not strictly limited to houses, although many intelligence services use rural houses for extended functions such as debriefing defectors. In a city, a safehouse may be an apartment or house that is not known to be associated with an intelligence service.

Another usage refers to mailing addresses (postal and electronic) and telephone numbers, to which messages can be sent with a reasonable chance of not coming into the awareness of counter-intelligence.

Useful idiots

Useful idiot is a term attributed to Lenin, principally in Soviet use, for a person overtly supporting the interests of one country (e.g., the USSR) in another (e.g., a member of the overt Communist Party of the second country). Soviet intelligence practice was to avoid such people in the actual clandestine operations, regarding them at most useful as distractions to the counterintelligence services.

Agents of influence, who were witting of Communist plans and intended to influence their own country's actions to be consistent with Soviet goals, went to great lengths to conceal any affiliation. "Witting" is a term of intelligence art that indicates that one is not only aware of a fact or piece of information, but also aware of its connection to intelligence activities. the Venona project communications intelligence exposes that Alger Hiss and Harry Dexter White, accused of Communist sympathies, were indeed Soviet spies. They were Communist agents, and the Soviets certainly did not treat them as useful idiots. There were communications with them, and the dialogues were clandestine.

Gus Hall also had overt Communist affiliation, and it is extremely unlikely Soviet clandestine operatives would have had anything to do with him. Still, in situations such as emergency exfiltration, Party members in a Western country might be called upon as a last desperate resort.

The propaganda model of communication explains that people write news favorable to those who pay for their job or that people are hired with favorable viewpoints to the hirer.

Basic agent recruiting

This section deals with the recruiting of human resources who do not work for a foreign intelligence service (FIS). For techniques of recruiting FIS personnel, see Counterintelligence.

In principle and best practice, all country B officers in country A report to an executive function in their home country. In CIA terms, this might be a head of a country desk or a regional desk. Russian practice was to refer to "Center".

Actual recruiting involves a direct approach by a case officer who has some existing access to the potential recruit, an indirect approach through an access agent or proprietary, or has reason to risk a "cold" approach. Before the direct recruitment, there may be a delicate period of development. For details, see Clandestine HUMINT asset recruiting.

Basic agent operations

This section deals with the general structure of running espionage operations. A subsequent section deals with Specialized Clandestine Functions, and another with Support Services for both basic and specialized operations

The agent may join, or even create, a new network. In the latter case, the agent may be called a *lead agent* or a *principal agent*. The latter term is also refers to access agents, who only help in recruiting.

Well-managed agent relationships can run for years and even decades; there are cases where family members, children at the time their parents were recruited, became full members of the network. Not all agents, however, operate in networks. A Western term for agents controlled as individuals is *singleton*. This term usually is reserved for the first or most sensitive recruitments, although specialized support personnel, such as radio operatives acting alone, are called singletons.[10] In Soviet tradecraft, the equivalent of a singleton is a separated acting agent. Professional intelligence officers, such as Robert Hanssen, may insist on being singletons, and go even farther, as with Hanssen, refuse in-person meetings. Even as a singleton, the agent will use security measures such as secure communications.

Agents also may operate in networks, for which the classic security structure is the *cell system*.

The agent may join a proprietary, although that is more likely to be for access or support agents.

Training

Before the agent actually starts to carry out assignment, training in tradecraft may be necessary. For security reasons, this ideally will be done outside the agent's own country, but such may not always be possible. Increasingly less desirable alternatives might be to conduct the training away from the operational area, as in a safe house in a resort, and then a safe house inside the operational area.

Among the first things to be taught are communications tradecraft, beginning with recording the material of interest. Skills here can include the operation of cameras appropriate for espionage, methods of carrying out documents without detection, secret writing.

Once the information is captured, it must be transmitted. The transmission may be impersonal, as with dead drops or car tosses. It may involve carriers. It may be electronic. If there is a need for personal meetings, the agent must know how to request them, and also to alert the network leader or case officer that the agent may be under suspicion.

Teaching countersurveillance techniques to agents is a calculated risk.[11] While it may be perfectly valid for an agent to abort a drop or other relatively innocent action, even at the cost of destroying valuable collected material, it is much more dangerous to teach the agent to elude active surveillance. The ability to elude professional counterintelligence personnel following the agent, for example, may confirm the counterintelligence organization's suspicion that they are dealing with a real agent.

Still, the agent may need to have an emergency escape procedure if he confirms he is under surveillance, or even if he is interrogated but released.

Continued testing during operations

Case officers should constantly test their agents for changes in motivation or possible counterintelligence compromise. While "name traces cannot be run on every person mentioned by the agent, do not be stingy with them on persons who have familial, emotional, or business ties with him" to detect any linkages to

hostile counterintelligence.[11] Until an agent is well established as reliable, meetings must always be done with care to avoid detection. "The prime emphasis is put on vigilance and checking- has he been planted by the local counterintelligence, are his motives in agreeing to collaborate sincere? The need for personal meetings with such an agent is increased, for they give the opportunity to assess him more completely."[12]

An experienced US operations officer emphasized that field operations personnel should report status and progress often. Only with such reporting can a headquarters staff remain vigilant, looking globally for penetrations, and also aware of political implications. Reporting and headquarters advice is critical for joint operations (i.e., with the intelligence service of another country). Headquarters, aware of all joint operations with a given service, can give advice from a broader viewpoint without compromising the need for local initiative.[11]

Operating the agent

Even with the most sensitive agents, occasional personal meetings are important in maintaining psychological control. Nevertheless, some agents, especially trained intelligence officers like Robert Hanssen, will almost never meet, but provide material good enough to prove their bona fides. A Soviet officer commented, whatever an agent's role in the intelligence net, personal contact should be made with him only when it is impossible to manage without it. The number of meetings should be kept as low as possible, especially with sources of valuable information.

> Personal meetings may be held to give an agent his next assignment and instructions for carrying it out, to train him in tradecraft or the use of technical or communications equipment, to transmit documents, reports, technical equipment, money, or other items, or to fulfill several of these purposes. In actual practice several purposes are usually served by a meeting. In addition to its particular objectives more general needs can be filled. A meeting held for training purposes may be a means for clarifying

> biographic data on the agent or his views on various subjects. At every meeting with an agent one should study him and obtain new data on his potential and talents, thereby providing a better basis for judging his sincerity and deciding how much trust to place in him.[12]

Agents, to varying extents, need reinforcement. Salary is important and also gives a lever of compromise, although pressing it too hard can offend a truly ideologically motivated agent. Some agents benefit from recognition that they can never show, such as a uniform of your service, or decorations from it.

Agents will be more comfortable if they believe that they will have protection, preferably exfiltration, if compromised. Protecting their families may be even more important. When the agent operates in a country with a particularly brutal counterintelligence service, providing them with a "final friend", or means for suicide, can be comforting even if they never use it.[13]

Agent communications

This section deals with skills required of individuals, either agents or support personnel. Most skills are concerned with communications.

Meeting places for personal meetings

A Soviet officer commented, perhaps counterintuitively, that it is harder to have longer meetings with agents when the case officer is under diplomatic cover. The reason is that local counterintelligence is aware of the case officer, where the existence of an illegal (i.e., nonofficial cover in US terms) officer may not be known to them. For the legal officer, "here it is best either to have reliable safehouses or to deliver the agent discreetly to the official residency building. The latter is a serious

operational move. If neither is feasible, it is better to have Headquarters dispatch an officer to a third country, either legally or illegally, for the meeting."[12]

Clandestine transfer operated by humans

It is a case-by-case decision whether the material exchanged should have safeguards against accessing it in other than a precise manner. One straightforward protection method is to have the material on exposed photographic film, in a container that does not suggest that it contains film and might be, innocently, opened in a lighted room. Self-destruct devices also are possibilities, but they confirm that the transfer involved sensitive material.

Brush pass and other physical exchange with couriers

Under the general term "brush pass" is a wide range of techniques in which one clandestine operative passes a physical item to another operative.[14] "Brush" implies that the two people "brush" past one another, typically in a public place and preferably a crowd, where random people interfere with any visual surveillance. In a properly executed brush pass, the agents do not even stop walking; at most, they may appear to bump into one another.

During the brief contact, a common means of executing the exchange is for both to be carrying otherwise identical objects, such as a newspaper, briefcase, or magazine. The information being exchanged is in one of them. As the two people separate, they still appear to be holding the same object in the same hand.

More challenging versions are reminiscent of passing a baton in a relay race, and would be most commonly done with small objects such as a photographic film cartridge. In this more dangerous method, the transfer is from hand to hand, or from hand into a pocket. While this technique obviously takes better manual dexterity and is more prone to error, it has the countersurveillance advantage that the operatives are not carrying anything after the transfer, and can blend into a crowd even more easily.

A variation of the brush pass is the *live letter drop*, in which one agent follows a predefined route, on foot, with a prepared report hidden in a pocket. En route, a second agent unknown to the first agent picks his/her pocket and then passes the report on unread, either to a cut-out or to an intelligence officer. This technique presents opportunities both for plausible deniability and for penetration by hostile agents.

Dead drop

A dead drop is a container not easily found, such as a magnetized box attached to a metal rack in an out-of-sight alley. The box could be loosely buried. It should be possible to approach the container to fill or empty it, and not be easily observed from a street or window.

Typically, a clandestine collector will put espionage material, perhaps in encrypted form, into the box, and use some prearranged signal (i.e. signal site) to let a courier know that something needs to be taken out of the box and delivered to the next point on the route to the case officer. Such a route might have several dead drops. In some cases, the dead drop might be equipped with a device to destroy its contents unless it is opened properly.

Representative dead drop device

Signals to tell a courier, or a case officer if there is no intermediate courier, that the dead drop needs service can be as simple as a piece of colored tape on a lamp post or perhaps a set of window shades raised and lowered in a specific pattern. While "wrong number" calls with a predefined apology can be used, they are more vulnerable to surveillance if the phone in question is tapped.

Car tosses

A car toss can take many forms, one of which can be considered a moving dead drop. An agent or courier can put a magnetized box inside a bumper on a parked car.

In some cases, if a car can drive slowly down a street or driveway not easily observed, a courier can toss a message container into an open window, making the transfer method intermediate between a brush pass and a dead drop.

Cars with diplomatic immunity have advantages and disadvantages for tosses. They cannot be searched if the toss is observed, but they also are followed more easily. Diplomatic cars usually have distinctive markings or license plates, and may be equipped with electronic tracking devices. Counterintelligence could wait until the car is out of sight following a toss, then apprehend and interrogate the courier, or simply keep the courier under surveillance to discover another link in the message route.

Methods of protecting message content

A message left in a dead drop, or dropped during an improperly executed brush pass, is quite incriminating if counterintelligence personnel can immediately see suspicious information written on it. The ideal material for transfer looks quite innocuous.

At one time, invisible ink, a subset of steganography, was popular in espionage communications, because it was not visible to the naked eye without development by heat or chemicals. While computer-based steganographic techniques still are viable, modern counterintelligence laboratories have chemical and photographic techniques that detect the disturbance of paper fibers by the act of writing, so the invisible ink will not resist systematic forensic analysis. Still, if its existence is not suspected, the analysis may not be done.

Microphotography

Another technique, for hiding content that will resist casual examination, is to reduce the message to a photographic transparency or negative, perhaps the size of the dot over the letter "i" in this article. Such a technique needs both a laboratory

and considerable technical skill, and is prone to damage and to accidentally falling off the paper. Still, it does have a countersurveillance value.[15]

Encryption

Encryption, especially using a theoretically secure method, when properly executed, such as the one-time pad,[16] is highly secure, but a counterintelligence agent seeing nonsense characters will immediately become suspicious of the message that has been captured. The very knowledge that a dead drop exists can cause it to be trapped or put under surveillance, and the member of a brush pass that carries it will be hard-pressed to explain it.

One-time pad encryption has the absolute requirement that the cryptographic key is used only once. Failure to follow this rule caused a serious penetration into Soviet espionage communications, through the Venona project analysis.[17]

It is extremely difficult for a nonprofessional to develop a cryptosystem, especially without computer support, that is impervious to the attack by a professional cryptanalyst, working for an agency with government resources, such as the US NSA or Russian *Spetssvyaz*.[16] Still, when the message is very short, the key is random or nearly random, some methods, like the Nihilist Straddling checkerboard may offer some resistance. Improvised methods are most useful when they only have to protect the information for a very short time, such as changing the location or time of an agent meeting scheduled in the same day.

Plain language code

Less suspicious when examined, although very limited in its ability to transfer more than simple content, is plain language code. For example, the final attack order for the Battle of Pearl Harbor came in a radio broadcast of the Japanese phrase, "Climb Mount Niitaka". Subsequent espionage communications referred to ships as different types of dolls at a doll repair shop.

Plain language code is most effective when used to trigger a preplanned operation, rather than transfer any significant amount of information.

Steganography, covert channels, and spread spectrum

Steganography, in the broadest sense of the word, is a technique of hiding information "in plain sight" within a larger message or messaging context. It is hard to detect because the secret message is a very small component of the larger amount, such as a few words hidden in a Web graphic.

Even more sophisticated computer-dependent methods can protect information. The information may or may not be encrypted. In spread-spectrum communications, the information is sent, in parallel, at very low level through a set of frequencies. Only when the receiver knows the frequencies, the time relationship on when a given frequency or other communications channel will carry content, and how to extract the content, can information be recovered. Basic spread spectrum uses a fixed set of frequencies, but the signal strength in any one frequency is too low to detect without correlation to other frequencies.

Frequency-hopping spread spectrum is a related technique, which can use the parallel transmission of true spread spectrum, not using any one frequency long enough for plausible interception. The pattern of variation among channels may be generated and received using cryptographic methods.

Methods of protecting against electronic detection of the fact of messaging

Avoiding detection of radio signals means minimizing the clandestine transmitter's exposure to hostile direction-finding. Modern techniques generally combine several methods:

- Burst transmission or otherwise minimizing
- High-gain antenna and/or directional antenna
- Receiver or relay away from detectors, as, for example, satellites.

Exploring agent information often meant a good deal of interaction, in which the home service would clarify what the agent reported, give new orders, etc. One approach used in World War II was the Joan-Eleanor system, which put the case officer into an aircraft at high altitude. From that altitude, there could be fast interaction in voice, so that they get to the key issues faster than with many separately encrypted and transmitted messages.[18] The modern equivalent is a small, low probability of intercept radio transceiver, using a directional antenna aimed at an orbiting satellite communications relay. Avoiding detection of radio communications involves all the principles of transmission and reception security.

Termination

For any number of reasons, a human source operation may need to be suspended for an indefinite time, or definitively terminated. This need rarely eliminates the need for protecting the fact of espionage, the support services, and the tradecraft and tools provided.

One of the most difficult challenges is ending an emotional relationship between the case officer and agent, which can exist in both directions. Sometimes, an agent is unstable, and this is a major complication; perhaps even requiring the evacuation of the agent. More stable agents may be happy with termination bonuses, and perhaps a future emigration opportunity, that do not draw attention to their own side's counterintelligence. In some instances, an intelligence agency may issue a "burn notice", indicating to other such agencies that an individual is an unreliable source of information.

Especially in the case of non-national organizations, termination can be very literal, ranging from having a trusted operative kill the problematic agent, or, when culturally appropriate, sending the agent on a suicide mission.

When the clandestine phase is preparation for a DA mission such as the 9/11 attacks, or the assassination attacks, using suicide bombers, by the Liberation Tigers of Tamil Eelam, termination

of the operational cells is rather obvious. If there are support cells in the operational area, they may be vulnerable, but it would be good tradecraft to withdraw them shortly before the attack.

Special clandestine services

Agents of influence

An agent of influence, being witting or unwitting of the goals of a foreign power B, can influence the policy of Country A to be consistent with the goals of Country B.

In Soviet theory, influencing policy was one aspect of what they termed *active measures* (*aktivnyye meropriyatiya*). Active measures have a different connotation than the Western concept of direct action (DA), although Soviet active measures could include wet affairs (*mokrie dela*) conducted by Department V of the KGB, "wet" referring to the spilling of blood.

Strategic deception

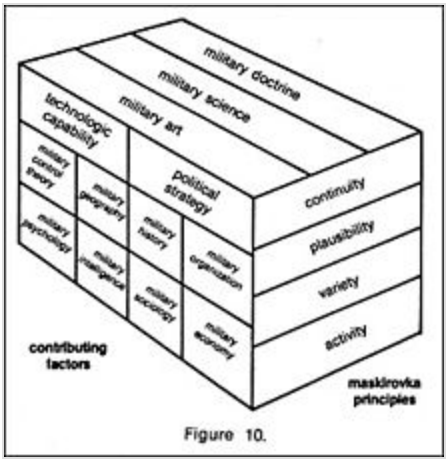
Intelligence organizations occasionally use live, or even dead, persons to deceive the enemy about their intentions. One of the best-known such operations was the British Operation Mincemeat, in which a dead body, bearing carefully misleading documents, was put in British uniform, and floated onto a Spanish beach. In World War II, Spanish security services, while officially neutral, often passed information to the Germans, which, in this case, is exactly what the British wanted done. This operation was under the control of the Twenty Committee, part of the British strategic deception organization, the London Controlling Section. A related British operation in World War I was run by a controversial military officer, Richard Meinertzhagen, who prepared a knapsack containing false military plans, which the Ottoman allies of the Germans were allowed to capture. The plans related to false British strategy for the Sinai and Palestine Campaign, setting up a successful surprise attack in the Battle of Beersheba and the Third Battle of Gaza.

Active measures, however, reflected a national effort to influence other countries to act in concert with Soviet goals. These measures could involve state organizations up to and including the Politburo, much as the World War II British organization for strategic deception, the London Controlling Section, and its US counterpart, Joint Security Control, could get direct support from the head of government. Much of the Soviet responsibilities for active measures was focused in the KGB. Its "First Main Directorate uses active measures such as agents of influence, propaganda, and disinformation to promote Soviet goals."

In the present political context of Western democracies, the sensitivity, and separation, of clandestine and open contacts do not lend themselves to the process of building agents of influence.

"Active measures is not exclusively an intelligence activity, and in this sense it differs from the similar American concept of covert action. There are many differences between active measures and covert action. One is the Soviet ability to mesh overt and covert influence activities through centralized coordination of party, government, and ostensibly private organizations dealing with foreigners. Despite interagency coordination mechanisms, the United States is too pluralistic to achieve full coordination between all the overt and covert means of exercising influence abroad. Other major differences are in scope, intensity, and importance attributed to active measures and covert action, and in immunity from legal and political constraints."

While deception and influence operations could involve the highest levels of Allied governments in World War II, it is worth noting that while the West generally speaks of military deception, strategic deception operates at a higher level. A Soviet, and presumably Russian, term of art, *maskirovka* or "denial and deception", is much broader than the current Western doctrine of deception being run by lower-level staff groups.



Russian concepts involve the full scope of grand strategy

In the military, responsibility for maskirovka easily can be at the level of a deputy chief of the General Staff, who can call upon all levels of government.

Returning to KGB doctrine, presumably still present in the SVR, "Influence operations integrate Soviet views into foreign leadership groups. Propaganda operations take the form of disinformation articles placed in the foreign press. Disinformation operations are false documents designed to incite enmity toward the United States."

The Second Main Directorate of the KGB, whose responsibilities are now primarily in the Russian FSB, is responsible for the recruitment of agents among foreigners stationed in the Soviet Union. The KGB influences these people unwittingly, as most regard themselves too sophisticated to be manipulated.

"The second deception program is counterintelligence, which aims to neutralize the efforts of foreign intelligence services. It achieves this through the use of non-Soviet double agents and Soviet double agents. Non-Soviet double agents are foreign nationals who have been 'turned'. A Soviet double agent is a Soviet with access to classified information. These officials may be used as false defectors".[19]

"Influence operations integrate Soviet views into leadership groups. The agent of influence may be a well- placed, 'trusted contact' who consciously serves Soviet interests on some matters

while retaining his integrity on others, or an unwitting contact who is manipulated to take actions that advance Soviet interests on specific issues of common concern."

Direct action services

There is no consensus on whether it is, or is not, advisable to intermingle espionage and direct action organizations, even at the headquarters level. See Clandestine HUMINT and Covert Action for more history and detail. A terminology point: current US terminology, ignoring an occasional euphemism, has now consolidated espionage into the National Clandestine Services. These are part of the CIA Directorate of Operations, which has some responsibility for direct action (DA) and unconventional warfare (UW), although the latter two, when of any appreciable size, are the responsibility of the military.

There is much more argument for doing so at headquarters, possibly not as one unit but with regular consultation. Certain services, such as name checks, communications, cover identities, and technical support may reasonably be combined, although the requirements of a particular field network should be held on a need-to-know basis.

Other countries might have the functions under the same organization, but run them in completely different networks. The only commonality they might have is emergency use of diplomatic facilities.

See also

- Tradecraft
- Undercover
- Honey trapping

References

1. Paterson, Tony (25 November 2004), "Berlin plaque pays tribute to 'Schindler of Stourbridge' " (https://web.archive.org/web/2008

0215220319/http://findarticles.com/p/articles/mi_qn4158/is_20041125/ai_n12813807), *The Independent*, archived from the original (http://findarticles.com/p/articles/mi_qn4158/is_20041125/ai_n12813807) on 15 February 2008, retrieved 14 February 2008

2. Rogov, (GRU officer) A.S., "Pitfalls of Civilian Cover" (https://web.archive.org/web/20080213105836/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v08i3a03p_0001.htm), *Studies in Intelligence*, Central Intelligence Agency, archived from the original (https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v08i3a03p_0001.htm) on February 13, 2008
3. US Department of the Army (September 2006), *FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations* (https://fas.org/irp/doddir/army/fm2-22-3.pdf) (PDF), retrieved 2007-10-31
4. Beller, Patrick R., "The Life and Work of Stephan Haller" (https://web.archive.org/web/20080109180709/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol3no3/html/v03i3a01p_0001.htm), *Studies in Intelligence*, Central Intelligence Agency, archived from the original (https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol3no3/html/v03i3a01p_0001.htm) on January 9, 2008
5. Suvorov, Victor (1984), "Chapter 6, The Practice of Agent Work" (http://militera.lib.ru/research/suvorov8/18.html), *Inside Soviet Military Intelligence*, MacMillan Publishing Company
6. US Department of Defense (12 July 2007), *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms* (https://web.archive.org/web/20081123014953/http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf) (PDF), archived from the original (http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf) (PDF) on 2008-11-23, retrieved 2007-10-01
7. Carroll, Thomas Patrick (5 September 2006), *Human Intelligence: From Sleepers to Walk-ins* (http://www.csus.edu/indiv/c/carrollt/Site/Welcome_files/Gov't%20139G%20class%20notes%20Fall%202006%20-%2024%20Oct.pdf) (PDF)
8. "R.F. Bennett" (https://web.archive.org/web/20071104084921/http://www.spartacus.schoolnet.co.uk/JFKbennettRF.htm). Archived from the original (http://www.spartacus.schoolnet.co.uk/JFKbennettRF.htm) on 2007-11-04.
9. U.S. Department of Justice,Commission for Review of FBI Security Programs (March 2002), *A Review of FBI Security Programs* (https://fas.org/irp/agency/doj/fbi/websterreport.html)

10. "Agent Radio Operation During World War II" (https://web.archive.org/web/20080109201318/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol3no1/html/v03i1a10p_0001.htm), *Studies in Intelligence*, archived from the original (https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol3no1/html/v03i1a10p_0001.htm) on January 9, 2008
11. Begoum, F.M. (18 September 1995), "Observations on the Double Agent" (https://web.archive.org/web/20080109184409/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no1/html/v06i1a05p_0001.htm), *Studies in Intelligence*, archived from the original (https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no1/html/v06i1a05p_0001.htm) on January 9, 2008, retrieved 3 November 2007
12. Bekrenev, (GRU officer) L. K., *Operational Contacts* (https://web.archive.org/web/20080109182659/https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v09i1a06p_0001.htm), Center for the Study of Intelligence, Central Intelligence Agency, archived from the original (https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v09i1a06p_0001.htm) on January 9, 2008
13. Hall, Roger (1957), *You're Stepping on my Cloak and Dagger*, W. W. Norton & Co.
14. Decision Support Systems, Inc. "An Analysis of Al-Qaida Tradecraft" (https://web.archive.org/web/20071116210341/http://www.metatempo.com/analysis-alqaida-tradecraft.html). Archived from the original (http://www.metatempo.com/analysis-alqaida-tradecraft.html) on 2007-11-16. Retrieved 2007-11-19.
15. John Barron (1974), *KGB: the secret work of Soviet secret agents*, Reader's Digest Press
16. David Kahn (1974), *The Codebreakers: The Story of Secret Writing*, Macmillan, ISBN 0025604600
17. National Security Agency. "VENONA" (https://web.archive.org/web/20071028100927/http://www.nsa.gov/venona/). Archived from the original (http://www.nsa.gov/venona/) on 2007-10-28. Retrieved 2007-11-18.
18. *The SSTR-6 and SSTC-502 - 'Joan-Eleanor'* (http://www.militaryradio.com/spyradio/joaneleanor.html), 2007, retrieved 2007-11-17
19. Edward J. Campbell. "Soviet Strategic Intelligence Deception Organizations" (http://www.globalsecurity.org/intell/library/reports/1991/CEJ.htm).