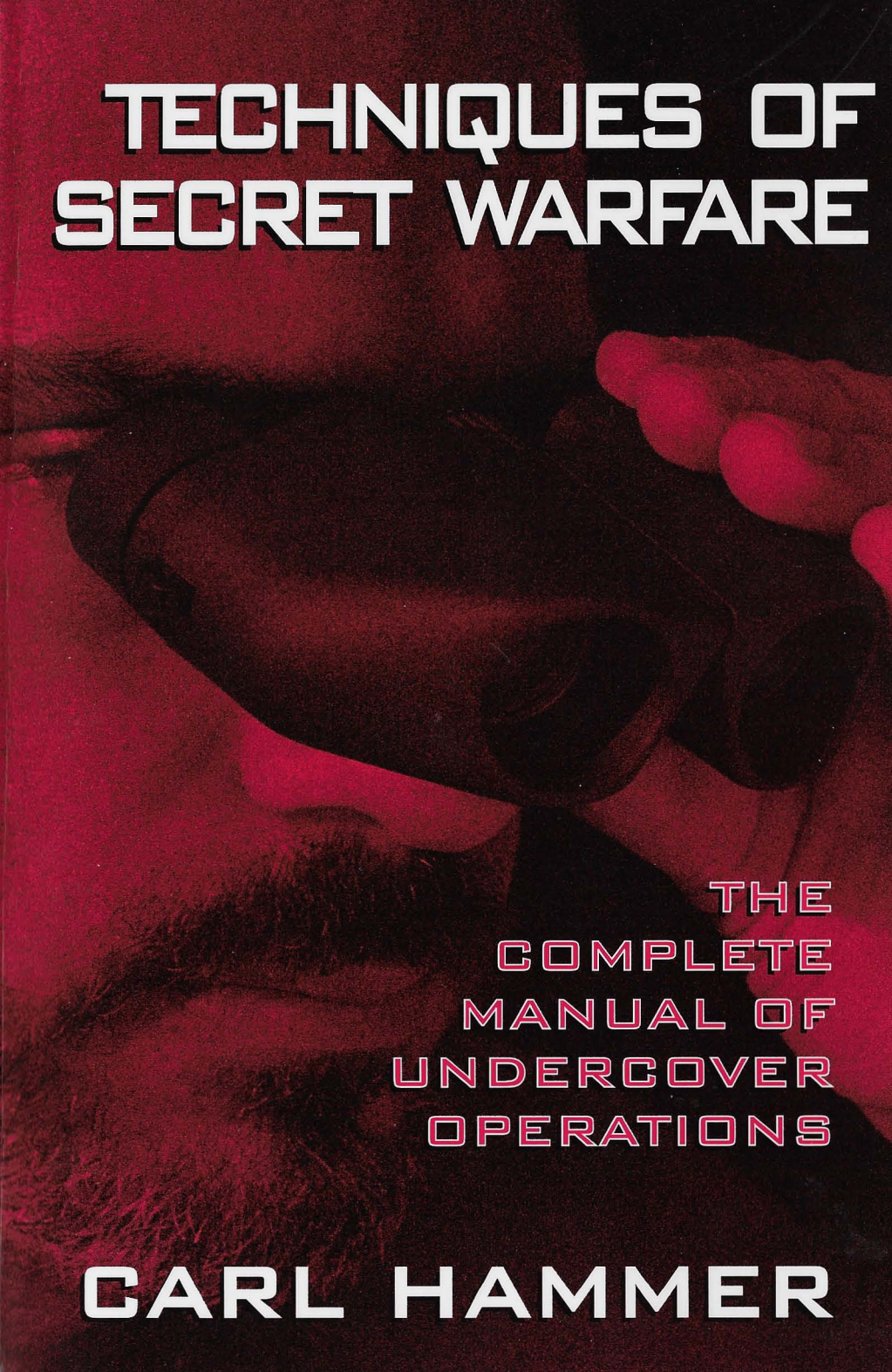
TECHNIQUES OF SECRET WARFARE



THE COMPLETE MANUAL OF UNDERCOVER OPERATIONS

CARL HAMMER

The most complete, up-to-date information on spying available anywhere!

Now you can study the techniques used by real professional spies and investigators. Learn how to gather any type of information you may want—or stop others from getting info on you!

Just take a look at the Table of Contents to get an idea of the many topics covered in this comprehensive book:

- The significance of Human Intelligence
- Infiltration and Maintaining cover
- Temporary missions: Methods for gaining entrance to enemy installations; how to open and reseal letters; surveillance techniques
- Protracted missions: recruitment techniques
- Security: travels; safe houses; hide-outs; clandestine meetings & counter-surveillance techniques; bug detectors
- Escapes: Trains and vehicles; ways of evading dogs; escaping from handcuffs
- Reporting systems & communications techniques: Letter drops; couriers; civilian postal and telegraph systems; telephone; radio;visual signals; audible signals; simple codes; scrambling systems; invisible ink
- Photography: Hand cameras; video cameras; night vision devices
- Enemy interrogation techniques & how to counter them

Examples from real operations and case histories are included to illustrate the techniques described. This is vital information for everyone interested in intelligence-gathering or privacy.

ISBN 0-918751-40-3

51695

9 780918 751409

TECHNIQUES OF SECRET WARFARE

CARL HAMMER

J. FLORES
PUBLICATIONS, INC
P.O. Box 830760
Miami FL 33283-0760

TECHNIQUES OF SECRET WARFARE by Carl Hammer

Published by:
J. Flores Publications, Inc.
P.O. Box 830760
Miami, FL 33283-0760

Direct inquires and/or order to the above address.

Neither the author nor the publisher assumes any responsibility for the use or misuse of the information contained in this book. The author and publisher specifically disclaim any personal liability, loss, or risk incurred as a consequence of the use and application, either directly or indirectly, of any advice or information presented herein.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the author or the publisher are not engaged in rendering legal or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Be advised that there may be certain items represented in this book as to which the sale, possession, construction or interstate transportation thereof may be restricted, prohibited or subject to special licensing requirements. Consult with your local ATF and law enforcement authorities in your area before obtaining or constructing such items.

Technical data presented herein, particularly technical data on dealing with dangerous chemicals, poisons, explosives, drugs, and safety procedures inevitably reflects the author's individual beliefs and experience with particular equipment and environments under specific circumstances which the reader cannot duplicate or experience exactly. The information in this book should therefore be used for guidance only and should be approached with great caution.

Since neither the author nor the publisher have control over the materials used, use of techniques or equipment, or the abilities of the reader, no responsibility, either implied or expressed, is assumed for the use or misuse of the data or procedures given in this book.

ISBN 0-918751-40-3

Library of Congress Catalog Card Number: 92-72147

Printed in the United States of America

Warning Notice

Neither the author nor the publisher assumes any responsibility for the use or misuse of the information contained in this book. The author and publisher specifically disclaim any personal liability, loss, or risk incurred as a consequence of the use and application, either directly or indirectly, of any advice or information presented herein.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the author or the publisher are not engaged in rendering legal or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Be advised that there may be certain items represented in this book as to which the sale, possession, construction or interstate transportation thereof may be restricted, prohibited or subject to special licensing requirements. Consult with your local law enforcement authorities in your area before obtaining or constructing such items.

Technical data presented herein, particularly technical data on dealing with dangerous chemicals,and safety procedures inevitably reflects the author's individual beliefs and experience with particular equipment and environments under specific circumstances which the reader cannot duplicate or experience exactly. The information in this book should therefore be used for guidance only and should be approached with great caution.

Since neither the author nor the publisher have control over the materials used, use of techniques or equipment, or the abilities of the reader, no responsibility, either implied or expressed, is assumed for the use or misuse of the data or procedures given in this book.

"An army without secret agents is exactly like a man without eyes or ears."

Chia Lin,
Tang dynasty
writer on military subjects

"Important state secrets and especially clues to the intentions and plans of potential enemies cannot be found in libraries or encyclopedias, but only where they are being kept under lock and key."

Alexander Orlov,
ex-General, NKVD

Table Of Contents

1

The Significance Of HUMINT (Human Intelligence)

Human Intelligence (HUMINT) is the technique of collecting intelligence through the use of secret agents.

The use of secret agents is fraught with danger. The failure and exposure of a HUMINT operation might well lead to death, torture, or imprisonment of the agents in question as well as a considerable loss of international prestige for the government employing them. Furthermore, secret agents are also the group of personnel most difficult to select and to train.

Despite these risks, secret agents continue to be one of the most important intelligence assets, maybe the most important one when it comes to strategic intelligence.

The reason for this is that HUMINT operations are still often the only way to collect really vital intelligence. Intelligence collecting by technical means can provide a lot of valuable information, but it can never inform of what is being planned in the enemy's most guarded installations and headquarters. HUMINT can, with a little luck and great skill, often provide such information.

Some intelligence services, notably the KGB, consider secret agents to be their absolutely most important intelligence source. Other agencies, such as the CIA, do use secret agents but to a considerably lesser extent. This lack of interest in HUMINT techniques has led to several intelligence failures in recent times, when technical means of intelligence collecting turned out to be impossible or unsuitable.

The following two examples serve to show what the effects of such a failure can be, if the government in question does not have the proper readiness to handle an agent operation.

The first case is the appallingly bad U.S. understanding of and planning for secret operations in Iran, shortly before Ayatollah Khomeini resumed control over the country. In 1979, when this happened, there were no Americans at all inside the country. The U.S. Administration was therefore totally unprepared for what was to happen.

After the U.S. embassy had been occupied by the Iranians, the CIA desperately tried to infiltrate the country. They soon found out that their only way of doing this was to recall an already retired agent, known as "Bob", as he was the only one capable of handling the situation in Iran.

This appalling preparedness was shown to the world even more clearly the 24th April 1980, when the much publicized rescue attempt ended in disaster. Several participating aircraft collided, eight men died, and the rescue had to be called off. One of the reasons for this failure was the preposterous belief that the operation would be possible to perform despite the lack of even the most elementary intelligence.

The second example is a case from the summer of 1985. A colonel of the KGB, Vitaly Yurchenko, had defected to the United States. After the defection he stayed for three months with the CIA, which interrogated him several times. However, no attempt to acclimatize him to his new country was done, apparently because nobody had the psychological preparedness to take care of a defector of this kind. A colonel of the KGB could not be handled in the same way as an ordinary ex-private Soviet Army soldier, which is the kind of defector more often entertained by the U.S. authorities (not by the CIA, however, as they usually do not entertain any defectors at all).

The result of this was that Yurchenko grew homesick. During a restaurant visit in Washington, he excused himself for a moment, left the premises, and returned to the Soviet embassy. Meanwhile, his American supervisors remained in the restaurant, not realizing what had happened. Naturally, the Soviet Union made a propaganda coup out of this, claiming that the CIA had kidnapped Yurchenko, drugged him and interrogated him, but that the colonel later had managed to escape.

Both these two cases made international news, thereby damaging the international prestige of the United States. The first failure also led to much suffering for the Americans taken as hostage, as well as to the death of certain soldiers during the air accident. In order to avoid this type of situation, it is imperative that an intelligence service maintains its ability to handle agent operations.

A field operative must be well trained and experienced, both in the techniques used in intelligence collecting as well as in many other areas of knowledge. He should be a resourceful individual possessing good judgement and complete self-confidence. It is an advantage if he is physically strong and it is a definite requirement that he possess courage to meet unforeseen situations. An ability to make quick and sound decisions is also required. He must also be psychologically strong and healthy.

The field operative must also have the ability to act in a particular assumed role, his cover. He must have a memory capable of recalling incidents without the use of notes, as he will encounter many situations where notes cannot be taken or will compromise him.

If the cover assumes a certain occupation, he must be skilled in that occupation. His physical appearance and capabilities must also be consistent with his qualifications. His hobbies, interest in sports and other subjects, musical ability, and so on must also be consistent with the role he is required to act in.

Last but not least, a linguistic ability is a definite requirement. There have been instances when extremely talented field operatives managed to successfully conclude important operations without any linguistic ability at all, but there are many more cases in which the operative was caught, killed, or otherwise failed only because of his lack of knowledge in a certain language required by his cover.

The training of an agent must be geared toward a deep knowledge of the conditions in the country in which he will be expected to operate. This must include as much information as possible on the culture, history, and daily life in the country in question. It is also imperative that the agent learns as much as possible about the way of life of the different social classes in the country, and the average views of many subjects among different groups of people. Naturally it is also vital that the national language as well as the local dialects be properly learned.

The agent should also learn as much as possible about practical psychology. Finally he must learn which intelligence is most searched for, and what is already known. In this way the agent is able to plan his own intelligence collecting in a proper way, as well as understanding when an earlier known piece of information is no longer valid and needs updating.

Naturally, no field operative is expected to know all possible intelligence techniques and all fields of general knowledge, languages, etc. The

intended mission must always decide what is necessary to include in the training program.

Secret agents are actually trained in several different ways, depending on their assigned missions. The possible types of missions include the following:

- Protracted infiltration and recruitment of native agents.
- Temporary infiltration for determining one or a few specific pieces of vital information.
- Infiltration for "action" missions, such as sabotage or assassination.

The last mission type has usually nothing to do with intelligence collecting and will not be detailed in this volume. But naturally most of the techniques described here are still of relevance to an agent on this kind of mission. But if this is the case, specialized training in for example weapons or explosives must be given to the prospective agent. Furthermore, this kind of mission requires a psychological stability of the highest degree.

Most government agencies, and some commercial agents, involved in HUMINT operations have a lot of sophisticated electronic equipment for use in the field. However, sometimes the equipment fails and at other times, due to some reason, the specialized equipment is not available when it is needed. It is of the greatest importance that the agent not depend too much on advanced technical equipment. The existence of suitable technical equipment in full working condition must not be a requirement for concluding the mission. The operative should rather see this as an unexpected advantage.

This volume therefore assumes that no special equipment is available. Other volumes will fully describe the special equipment available.

In many cases, the nature of secret agents is not properly understood as people tend to base their ideas of secret agents on what they see on television or read in fiction. Therefore, a few definitions might be in order:

Agents can be all kinds of people, trained or untrained, but in this volume it will from now on only refer to native individuals recruited by a foreign intelligence service, usually in order to betray their country by providing information or by other means facilitating the operations of the foreign intelligence officers.

Field operatives are the officers of the intelligence service working under cover in the foreign country. They often have to reside in the country illegally, as they otherwise would expose themselves to the enemy security services. Field operatives are usually highly trained.

Spies, finally, consist of both native agents and field operatives but this word is highly emotional and its meaning is also quite uncertain. It will not be further used in this volume, as a field operative or an agent is generally called a spy only when he is exposed or convicted in court.

Here follows a general piece of advice to the prospective field operatives studying this volume:

This book contains many rules on how to behave in real operations. These rules are sound guidelines. But the best guidelines will always be your own common sense and good judgment.

2

Infiltration

When infiltrating enemy territory, many different methods can be used. The most common methods are to travel by:

- Legal entry, with a forged passport.
- Land, illegally crossing the border.
- Sea, landing at an unguarded point.
- Air, by the use of helicopter or parachute.

If a forged passport is being used, the entry and exit stamps, visas, etc., must show the travel route from the "issuing country" to the target country. If for example the field operative travels from Britain to France on a French passport, the entry stamp to Britain must be in the passport. In many cases the supposed travel route is much more complicated than this, and then it is of the utmost importance that all stamps in the passport coincide with the assumed cover.

Also, it must be decided whether the forged passport is to be utilized as a permanent identification document or whether it is only to be used for entry (and possibly exit, when the mission is completed). If the last option is chosen, the field operative must not keep the forged passport among his belongings, when in the target country, as this could compromise him.

If a forged passport is used to obtain a visa, or the field operative is deficient in the language he is supposed to know, it is usually safer to ask a travel agency to procure the visa. This method works well as long as the passport is not lost by the travel agency. This can mean no end of troubles, as the operative cannot merely go to "his" embassy and ask for a new passport. Even if a new passport can be procured from the embassy, the unavoidable police investigation might reveal the forged nature of the lost passport. A reliable travel agent is therefore a necessity, if a travel agent must be used to obtain a visa.

An Israeli national, Nathanael Malhi (fictitious name), in the spring of 1960 offered his services as an agent for the Egyptian intelligence service. The Egyptians, however, only showed a passing interest in him, so the negotiations dragged on for a long time. At that time, Malhi was residing in Ethiopia. Unfortunately his Israeli passport was due to expire.

Malhi therefore at first contacted the Israeli consulate to renew his passport. Soon, however, he changed his mind and decided to "extend" the validity of the passport himself. By doing this he forgot (or was not aware of) the simple rule, that a field operative should not attract unnecessary attention by participating in unnecessary illegal activities.

Malhi, who did not speak any foreign languages, did not know that an Israeli passport had text both in Hebrew and French. As his passport expired on the 8th June 1960, he could have "extended" the date by two years by writing the French word deux (2) after the word soixante (60). The other, necessary changes were easy to make. But Malhi did not understand that the language was French, so he wrote two in English instead. He was arrested when he returned to Israel.

At least in Europe, passport checks are minimal when travelling by night train. It is common that the train ticket collector also collects all the passports when the journey begins. Every passport will be stamped at the border without awakening the sleeping passengers and without checking whether the passport's description of the passenger coincides with his real appearance. Custom checks are also done very infrequently, which facilitates entry with illegal equipment such as weapons and bugging equipment.

Entry by illegally crossing the land border is generally easy if a guide is available. Such a guide is usually easy to find in those countries where smuggling is common, such as in many parts of Asia and Africa. In Europe a guide is seldom needed, as high quality maps are available. As long as maps are available, a field operative can cross almost any border, with proper preparation, even if alone. Naturally, all enemy outposts, patrols, and installations must be avoided at all costs.

The map must not be marked in any way. It the operative is captured by the enemy, such marks can be used as evidence against him, and also against any other operatives involved in the infiltration attempt. The operative must also take care not to mark the map accidentally, for instance by handling it roughly with soiled fingers. Such marks can also be used as evidence for an illegal border crossing.

More problems will be encountered, however, if it is impossible to cross straight into the target country from an allied country, because then it is first necessary to cross the neutral borders before one reaches the enemy border. This means that at least two additional borders must be crossed, that is entry to and exit from the neutral country.

Electrified fences present a special problem when illegally crossing a land border. The operative should watch out for indications of fences of this kind, such as dead animals, insulators on wires, and tell-tale flashes from the wires during rain and storms and from short circuits.

One way to determine whether a wire is electrified or not is to slowly and carefully approach the wire with a stem of grass or a damp (not wet!) stick. If the wire is electrified, the operative will receive a mild shock, but suffers no injuries.

In times of war, areas contaminated by chemical weapons might be another difficulty. The operative must look out for liquid droplets on vegetation, unexplained dead animals, and the presence of liquid in the bottom of shell craters or a mysterious "film" on the surface of pools of water. If the vegetation suffers from discoloration, not appropriate to the season, there is a strong possibility that chemicals have been used in the area. The operative must naturally try to bypass all contaminated areas, even if he is equipped with protective clothing.

Infiltration by sea is generally carried out in one of three different ways. It is possible to use a small boat, or in some cases even a submarine, to land a field operative on hostile territory. A different way is to enter by way of a port as a sailor from a merchant ship. This can be done openly or covertly, depending on the situation. Yet another method is to infiltrate by a sea plane, landing on a large lake, river, or coastal water.

Infiltration by air is generally carried out by helicopter, in some cases small aircraft, or by parachute. If the latter method is used, it must be decided whether to use low-altitude drops, or so called HALO techniques (high altitude low opening). The latter technique is generally safer for evading discovery but requires special training and equipment.

In all infiltration situations, it is preferable to have at least one man who can meet the operative and make certain that the area is safe before the operative arrives.

Exfiltration of field operatives or agents is usually performed in a manner similar to infiltration. There are, however, two further complications. If the field operative some day needs to return to the target country,

then perhaps it is necessary to hide his real destination. In any case, when he returns, this requires that the entry and exit stamps as well as the visas in his passport correspond to the assumed cover.

The cover must also explain why he leaves the country and why he returns. It must also explain where he has been, and why he has been there. It is also important to remember that airlines and travel agents may keep records on his real travels, if the field operative has not taken the precaution to use an assumed identity.

One case, clearly demonstrating the importance of entry and exit stamps, occurred in January 1973. At that time three members of the PLO were arrested in Vienna. They had been supplied with Israeli passports by one of the departments of RASD, the Palestinian intelligence and security service. The forged passports had, however not been satisfactorily doctored, as the forgers had not cared to check how the Jewish religious festivals affected the issuing of passports. One of the passports was for example "issued" on Yom Kippur, a holiday. Another one had been stamped with an exit stamp dated on a holiday when no civilian aircraft departed from Lod, the airport in Tel Aviv, so that one was also clearly falsified.

Furthermore, if it is necessary to permanently exfiltrate a field operative or an agent who is not yet exposed to the enemy, the utmost care must be used to prepare his cover, so that, if he at any time must return to duty, his cover will satisfactorily explain his absence.

One case, demonstrating this, is the already mentioned "Bob", recalled by the CIA for duty in Iran after the return of Ayatollah Khomeini.

Even if the agent is truly permanently leaving the target country, this must be done so as not to allow the enemy to realize that he was an agent. If the enemy understands this, even if too late, he will try to set the situation right by changing the supposedly exposed procedures and facts, as well as reorganizing exposed organizations. Thus, if the enemy never gets the chance to suspect the agent, the information he delivered will be of use for a much longer period of time. Otherwise his work will be undone in a short period of time.

An important Soviet operative, usually based in Paris, was at one time during the 1930s secretly travelling to Moscow in order to report the results of an important operation. In order not to get his Canadian passport stamped during the train ride east, he decided to instead use his old, Soviet passport.

Everything went well until he reached Berlin. Among the new passengers in the train, he noticed a young diplomat from Poland, at that time an independent country. The Russian operative realized to his horror that he not so long ago had met and made friends with the Pole, but at that time he had used his Canadian cover.

The Pole, upon recognizing his "Canadian" friend, was overjoyed. He asked the "Canadian" if he also was going to Warsaw. The Russian hurriedly declined, answering that he was on his way to Moscow in order to change to the Trans-Siberian Railway, as he was going to Tokyo. The Polish diplomat then tried to persuade his friend to first stay for a week in Warsaw, as his guest. They could hunt wild boars on his father's estate, see all the interesting things in Warsaw, meet beautiful Polish girls, and generally have quite a good time.

While the Pole in great detail told his friend about all the joys of Poland, the Russian was deep in thoughts. He knew that the train would reach the border within a few hours. Then the border guards, first the Germans, and then the Poles, would ask to see his passport. And when he produced his Soviet passport, the Polish diplomat would certainly realize that he was not a Canadian but a Soviet intelligence officer. And this would mean that he never again could return to his cover in France.

Shortly before the train reached the border, the Soviet operative excused himself, and departed toward the toilet in the end of the railway carriage. Over there, he changed to another carriage, and finally sat down in one of the third class carriages. There he awaited the border guards.

Meanwhile the Polish diplomat waited for his friend to return, so that they could visit the restaurant carriage together. The train finally arrived at the border. Immigration and custom officials checked the passengers, and when everything was concluded, the train began moving again. Now the Pole was definitely worried, as he believed that his "Canadian" friend might have left the train at the border station and accidentally been too late to catch it again.

The Pole was relieved when his friend returned from the third class carriage. The Russian was also relieved, as he now could continue to pretend being Canadian.

3

Maintaining Cover

The cover is the most important security measure adopted by a field operative. It is a partly falsified life story which conceals the real identity and experiences of the field operative. The cover must include the following details:

- A family background, including addresses of parents, relatives and friends.
- School and education records.
- A legitimate occupation, including records of past employment and employers.
- Explanations of past and future travels, especially travels abroad.

Whenever possible, the cover must be supported by official records, both among the operative's belongings and in the proper administrative departments.

It is also necessary to devise a system in which "old friends" of the operative can testify that he really is the person he claims to be. Such "old friends" are sometimes native agents, recruited mainly for the purpose of supporting field operatives working under cover.

Likewise, it is important that "new friends", such as recruited agents and other field operatives, be provided with sound explanations of how they got to know the operative and each other.

Field operatives and agents who know each other must not show this in public, unless they previously had the opportunity to meet "for the first time" under conditions which are both natural and believable. Such meetings can be prepared in many different ways. One of the best methods is for the two men to, independently of each other, secure an invitation to a social event of some kind, such as a party or dinner. During this occasion, an innocent person can be manipulated to introduce the two to each other.

The innocent person must of course not realize that the two already

know each other. Therefore, if questioned, he will affirm that the two men did not know each other before he introduced them to each other. This may be very helpful, if the local security service begins to suspect one of the two operatives.

Other methods include legitimate business transactions. If an agent puts an advertisement in a newspaper, wishing to sell something, for example a car or a stamp or coin collection, the operative can reply, and later buy the object. This will introduce the two men to each other in a legitimate way, especially so if the object is a coin collection and the two men are both avid coin collectors.

It is certainly of the utmost importance that all details in the cover story are correctly prepared and described. If some preparations are left to chance, the chance of failure will increase greatly.

Kaburak Yakobian was an Armenian living in Egypt. The Egyptian intelligence service decided to train him as an agent and then send him to Israel. They recruited him in December 1959, when Yakobian was twenty-one years old. During one year, he was trained in everything he was supposed to know in order to claim being a Jew. He was even circumcised. Yakobian also studied Judaism, and read Israeli newspapers. His cover was carefully prepared. He was told to claim being the son of a Jewish refugee from Turkey. According to his forged identity, he was born in 1935 (by the way three years earlier than his real birth date) in "Salonica, Turkey".

Unfortunately the counterfeiter did not know that Salonica (now Thessaloníki) had been occupied by the Greeks during the war in 1912, and remained a part of Greece since then. Furthermore, the training and the preparations had also in many other ways been inadequate. Especially Yakobian's knowledge of Judaism was insufficient. This soon caused suspicions, and Yakobian was arrested in Israel shortly before his planned wedding to an Israeli girl. He was sentenced to eighteen years in prison. Luckily for him, he was exchanged a few years later and returned to Egypt.

The cover of a field operative must be as close as possible to his own experiences and the true story of his life. This is to ensure that he does not give himself away because of a lack of knowledge of something the cover demands that he knows.

It is also dangerous if the operative displays knowledge of something which the cover cannot explain. It has happened that operatives, suddenly confronted by car accidents, a house on fire, and similar accidents, have

displayed unexpected abilities in medicine, scaling walls, or something else which his cover definitely cannot explain.

In the same way, the field operative must be able to describe for example those cities, buildings, etc., where he is supposed to have formerly lived or worked. His specific interests and hobbies must also fit into the cover. If the cover reflects the real experiences of the field operative, it will also be easier to learn and to remember. A skilled operative can in this way sometimes even fool a lie detector test, as the experiences he mentions are true and correct, even if the basic assumptions are not.

One of the most important parts of the cover is the occupation. This must be carefully chosen in order to allow the operative maximum advantage. First of all, it must be an ordinary job, which will not entice people to ask too many questions about. Secondly, if it is a full-time job, it will leave little time for the operative's intelligence activities. But despite this, the job must properly explain the economic situation of the operative and also, if possible, justify his travels.

The best solution is therefore in most cases to open a private business, usually in a small scale, such as antiques or rare books. Another possibility is to become an agent or representative for a foreign business concern. Yet another frequently used cover is that of a journalist or a free-lance writer.

A business cover of this kind must include all necessary details such as correspondence, etc., but the operative must never forget that his real business is intelligence, not making money. It has many times happened that operatives on extended missions gradually forget this, and get bogged down in the details of making a good life for themselves. In some cases this can be avoided if the operative is provided with enough money, so that he does not need to worry about a lost contract or other wasted business opportunity.

As the cover must include letters, souvenirs, and other paraphernalia of the fictitious life of the field operative, it is equally important that all compromising material, such as specialized equipment, weapons, letters and souvenirs from his real family, must never be kept among the operative's belongings. At any time, his home might be subjected to an open or a covert search by the enemy, whether they are enemy operatives or police officers.

One example of this was the Soviet agent Hambleton, arrested in Canada in the 1970s. He had Soviet cryptographical equipment hidden in

his house. This proved beyond the shadow of a doubt that he was a Soviet agent.

The objects used to support the cover story may be of any kind. Old letters and post cards, old tickets, medicine or anything only obtainable at his former (fictitious) residence are frequently used in this role.

All personal possessions must be appropriate to the assumed cover in quality, price, and age. The fit, and degree of cleanliness is also important when it comes to clothes. In certain countries, it is common that clothes have laundry marks. If so, they must also be consistent with the assumed cover.

It must always be remembered that what is common dress and appearance in certain countries is considered strange in other countries. A free-lance writer, especially one who is not famous (and an operative with this cover would hardly be famous) cannot afford an expensive car and flashy clothes. A minor business man can often travel around in an expensive car, but at least in Europe he will not sport tailor-made clothes, unless his company can show a considerable legitimate profit. In Asia, however, tailor-made clothes are common among business men, even the not so successful ones. This kind of consideration must be done for every cover.

Other minor items which may give the operative away are books, personal calendars, watches, rings, and other tokens of marriage or graduation from certain universities, matches, especially those from restaurants and hotels, letters, larger sums of money, bank accounts and pass books, and many other personal items, especially so if they are marked with the operative's initials.

During the Vietnam war, many CIA operatives and other CIA employees stationed in Southeast Asia chose to wear the expensive gold Rolex watch. At that time, it was often quite easy to recognize them by their use of this expensive watch. The practice of wearing this watch seems, remarkably enough, still to be followed despite the fact that it has became well known in the area as a piece of the CIA "uniform".

Especially letters and mementoes of the operative's real family are dangerous to keep. Unfortunately there have been many cases in which field operatives out of loneliness and home-sickness kept such mementoes, and also were exposed to the enemy by them. All those cases led to personal tragedies, as the very souvenirs of the beloved family caused the operative to get arrested and never again to return.

An interesting phenomenon in Buddhist countries is the fact that people with dangerous occupations usually carry several Buddhist amulets in order to protect themselves against the risks of the occupation. Among the dangerous occupations are naturally also the police and of course the intelligence service. This means that plain-clothes police officers and military intelligence field operatives, all of them certainly dressed in civilian clothes, usually carry a manifold of lucky amulets. Thai military intelligence field operatives are easy to identify in this way.

Especially in the past, but even today in certain countries, the police usually wear black shoes, even if they dress in civilian clothes. The reason for this is that men do not change comfortable shoes as often as women. Even if the police officer changed into civilian clothes, he would retain his black, service-style shoes.

It is also important that documents or identity cards show the appropriate amount of wear. These are easily prepared in a natural way if the operative or somebody else carries them on his person for a long time before the mission begins. It is, of course, then vital that these items are not lost or observed prior to the mission. Furthermore, the origin of the documents and also of all other possessions must be easily explained by the operative. He must also be able to tell naturally and logically how each item came into his possession. When it comes to official documents, such as passports, the operative must also be able to explain his procedure for applying for them.

It is usually too dangerous to pretend infirmities, as they are difficult to maintain for any length of time and may give the operative away in time of stress. Only when absolutely necessary should any infirmity be adopted in the cover.

It is however always a good idea if the operator can have a female counterpart, preferably his real wife, as a couple or family is less likely than a single man to raise any suspicions. During extended missions, lasting for several years, this may also be the only way to avoid the operative suffering from psychological problems, of the type always coming to light during such long-term missions.

Furthermore, women and even children can perform many types of missions, compromising to a male operative. One example of this is to leave reports and other pieces of communication in ladies' rest rooms. More information on communication techniques follows in chapter 8.

If children are used for missions of this type, it is also imperative that

they too are included in the cover. One case, demonstrating this, took place in Vienna in 1950. The British intelligence service MI6 was involved in monitoring a number of Soviet telephone wires. They used a young school girl as a courier. She delivered the recorded tapes to a British operative, whom she met in the Schönborn Park. At one time, however, an Austrian police officer noted the meeting and grew suspicious. He promptly arrested the British operative, suspecting him for molesting children.

In certain situations, names, addresses and telephone numbers may be disguised in the form of telephone numbers or similar harmless writings, such as the names and addresses of ordinary friends and acquaintances. But if this is the case, then it is absolutely vital that these numbers will not be detected and checked out by an enemy security service.

The residence of a field operative must also be chosen with the utmost care. The worst place to stay is in a boarding house, because in such a place the operative is bound to meet many people over whose behavior and questions he has no control. The other occupants might for example be involved in criminal activities, or they may be the victims of accidents, or merely dying. If this is the case, the subsequent police investigation may reveal the operative.

Another disadvantage is that the operative might be forced into conversation with strangers, asking questions which he may find difficult to answer in a satisfactorily way. It is also bad for security reasons, as it is easy for the enemy to plant a surveillant in the same house.

The best arrangement is usually to have an apartment in a quiet neighborhood where the inhabitants seldom know each other. It is however important to remember that especially the aged and retired often have nothing better to do than to spy upon, and gossip about, their neighbors. Even this might expose a careless operative.

Children also often find strangers interesting, especially if the stranger behaves in a "mysterious" way. The field operative must always behave in a way as natural and inconspicuous as possible.

It is also necessary to stay away from places, such as restaurants, where the field operative might accidentally meet people who know him under another identity.

One such case took place in Germany in the 1930s. A Soviet operative, Ivanov, who previously had been employed as second secretary at the Soviet embassy in Vienna, was now working under cover in Germany. He claimed to be Canadian, a common cover for Soviet operatives at that time.

On one occasion he had invited a German couple, a doctor and his wife, for dinner in a hotel restaurant. In the same restaurant, a group of Germans also happened to have a party at the same time.

Suddenly one of the Germans from the other group rose from his seat, strolled over to Ivanov, and heartily greeted him in Russian. Then, addressing the operative as "Herr Ivanov", he asked if he stayed in the hotel, and proposed a meeting to discuss the old times. Ivanov recognized the German as his old teacher in the German language from the time in Vienna. But his present friends knew him as a Canadian. He had to do something, quickly, to save the situation.

He answered that he stayed with some friends, instead of in the hotel, but he would call the German as soon as possible to arrange a meeting with him. At the same time, he rose from his seat and led the German back to his friends.

When Ivanov returned to his own table, he explained the situation to the German couple. The German, he said, had evidently been drunk and mistaken him for somebody else. He had decided to agree with the stranger in order to keep him from sitting down at their table in order to try to sort out if they had met or not. As he wanted to avoid the company of the drunk stranger, he had also led him back to his own friends. Luckily for him, the German couple believed his story. They even began to tell him other stories about people who had mistaken them or others for somebody else. Just in case, however, Ivanov checked out from the hotel, as the German teacher might return there looking for him.

It is also necessary to acquire as many legitimate friends as possible, preferably in influential positions. If the field operative falls under suspicion, these friends will usually vouch for his legitimacy, if questioned by the police or security service. Such questioning of friends and acquaintances is common procedure, especially if the operative's cover is that of a foreigner residing in the country. As long as the operative has stuck to his cover at all times, the legitimate friends will vouch for the validity of his identity.

One such case took place in a European country. A Soviet operative noted one day that somebody probably had entered and searched his home. He was not certain, however, as the search had been expertly done. As he did not want to abandon his mission simply because he feared something that might never have happened, he decided to remain in the country.

Shortly afterwards, however, he met a couple of his legitimate friends,

a very conservative couple. They told him that a detective from the secret police had asked questions about the operative. The couple had naturally answered that their friend was above all suspicions. The man even excused himself for the occurrence, joking about the police always spying on foreigners.

The operative realized that he would soon be exposed. He concluded the current operation and left the country in time to avoid arrest.

Another important point, which deserves to be mentioned in this context, is that the field operative must at all cost avoid taking part in unnecessary illegal activities. Such activities, even if not sufficiently proved to warrant an arrest, may cause the police to get their eyes on the operative. He will end up in their files, which may cause his exposure at a later time.

During the Second World War, the British intelligence service was heavily involved in Yugoslavia. One of their Yugoslav agents, Dr Ivo Popov, was actually a double agent, as he officially worked for the German intelligence service Abwehr. But Popov did not only work secretly for the British. He also worked secretly for the Yugoslav partisans, partly financed by his smuggling gold from France to Yugoslavia. In his own country, he sold the gold on the black market, with a three hundred percent profit. The smuggling was easy, as he had been supplied by the Germans with a permit to pass the borders without any customs control.

Popov, known among the British by the code name DREADNOUGHT, decided despite the risks to once again, in 1944, return to Yugoslavia. This time, however, he was arrested by the Gestapo because of his illegal currency transactions. But they never discovered his covert work with the British and the partisans. As a mere black marketeer, he was put in prison.

This was lucky for Popov, as he managed to escape after a few weeks. He joined his friends among the partisans. Everything considered, the war was profitable for Popov. After the war, he became a British citizen and moved to the Bahamas.

4

Temporary Missions

Temporary missions are usually executed in order to collect specific pieces of intelligence not possible to get in any other way. The most common temporary mission is to "find out what or who is in a specific place". This commonly includes covertly gaining entrance to an enemy installation or surveillance of certain individuals.

Techniques for gaining entrance to enemy installations

There are many possibilities to successfully gain entrance to enemy installations. The techniques employed naturally differ depending on whether the target is a military base, a government building or an office, or a private home. Also, the techniques possible to use differ depending on whether it is war or peace.

In times of peace, there are usually several methods to enter enemy installations as long as the security level of the installation is not too high. Generally, people who are dressed and act like service staff, such as telephone engineers, maintenance men, cleaners and window cleaners, delivery men and chauffeurs, can enter without too many questions asked.

This provides excellent opportunity to inspect documents, maps, etc., which might be temporarily displayed in an office. It also provides opportunities to determine availability of certain equipment, vehicles, or identity of units, in a military formation. Signs, equipment, and uniforms usually tell this at a glance.

In times of war, more risky methods can be put to good use, as the conditions in war zones tend to be slightly chaotic. One such method to enter guarded installations is to ambush an ordinary supply vehicle, put on the driver's (and guards') uniforms, determine the correct password by interrogating the captives, and finally boldly drive to the installation in the captured vehicle. This simple method tends to work as soldiers are more prone to check the uniforms and password instead of the documents,

which might be difficult to read due to dirt and oil, or even "accidentally" lost due to some reason.

One interesting example of this took place during the Spanish Civil War. A Spaniard, commanding a small guerrilla force fighting against the Nationalists, had been ordered to blow up an arms depot, guarded by more than twenty men. In addition to these guards, the enemy had also positioned a roadblock about half a kilometer before the entrance to the depot on the only access road. There the guards demanded to know the correct password, before they let anybody near the depot.

The guerrilla commander realized that the guards at the depot would be alerted if he and his men tried to fight their way through the roadblock. And in that case it would be very difficult to attack the depot without suffering heavy casualties. He decided to use a ruse instead of a direct assault.

For this purpose the guerrilla commander erected his own roadblock about a kilometer in front of the Nationalist road block. Then he and his men awaited the arrival of one of the Nationalist supply trucks. The guerrillas were lucky. Soon one of the trucks, belonging to a workshop located next to the depot, appeared on the road. The guerrilla commander halted the vehicle, and demanded to know the password. The driver promptly answered him, without any hesitation.

After the guerrillas had overpowered the driver, they began marching toward the depot. The commander had on an earlier occasion been able to secure a Nationalist lieutenant's uniform, and the remaining guerrillas looked more or less the same as the Nationalist soldiers. The war had been going on for some time, and new uniforms were not always available. Besides, they were all whistling one of the Nationalist marching tunes.

When they reached the real roadblock, the enemy guards demanded the password. The guerrilla leader answered, nonchalantly, with the same password as the driver had used. This was of course the correct one, and the guerrillas were allowed inside, as they claimed they were going to the workshop.

As soon as they were safely inside, they attacked the depot. As the guards were totally surprised, not having received the expected advance warning, they were quickly defeated. The guerrillas blew up the depot and made good their escape before any other enemy units had time to react to their presence.

False roadblocks of this type have been used in many recent wars. A

fairly safe method is to dress in enemy uniform and raise a roadblock across an important but only lightly trafficked road deep inside enemy territory. Then all military vehicles can be halted and the drivers' I.D. and orders inspected. If the questioning is executed in a subtle way, the drivers can often be persuaded to tell which unit they belong to, and where it is located for the moment, or where it will deploy next time. This information alone will usually result in reliable intelligence about the enemy movements.

In addition to this routine intelligence collecting, there is always the chance that an important staff officer might be found in the halted vehicle. If so, he and his driver can be overpowered and then interrogated in the ordinary way. Very often, maps and other documents found in the staff officer's luggage can provide additional intelligence.

Another example of a similar case took place during the Second World War in the part of Finland occupied by the Soviet Union. A Finnish patrol, led by Major Kuismanen, got into a gunfight with a unit of the Red Army. One of the Finns got wounded, and Kuismanen realized that he had to get a vehicle of some kind for returning home. He ordered one of his men to wait at the side of the road, in order to try to hitchhike with one of the many Red Army trucks regularly trafficking the road.

Finally one truck stopped, without expecting any trouble. The two Russians in the truck were quickly overpowered. The Finns hid beneath a tarpaulin on the platform, while Kuismanen and a Russian-speaking soldier sat down in the driver's cab. Then they drove towards the front line.

The first bridge they reached was guarded by a detachment of the Red Army, but Kuismanen simply drove on, without halting, while the interpreter shouted something about being in a hurry. In the next roadblock they had to stop, however. One of the Russians demanded to see the identification documents. But the Finn answered that they had to leave in a hurry, as they had received a report on Finnish saboteurs in the area. They had forgotten to bring the documents, he explained, as their departure had been so hurried. The Russians said that they understood, and Kuismanen's group was allowed to continue back to their own lines.

Yet another example of this also occurred during the Spanish Civil War. Many Soviet officers took an active part in the fighting. One of them was Captain Nikolayevsky. He, together with many other Soviet intelligence officers, led guerrilla raids against Nationalist bases and installations. In

the summer of 1937, he and his men received orders to attack an enemy air base.

Nikolayevsky was tall and blond. Furthermore, he could hardly speak any Spanish. For these reasons he had tied a swastika ribbon around his arm, pretending to be a German captain from the Condor Legion, the German intervention force.

Late one night, Nikolayevsky and his men drove straight to the air base in two recently captured enemy vehicles. They passed the road block at the entrance to the base without stopping, as it was open. The guerrillas simply shouted the Nationalist slogan "Arriba España", and the surprised guards let them in without any questions.

Having reached the inner buildings of the base, the Spanish interpreter of Nikolayevsky introduced him to the startled Nationalist officers as a German captain from a certain Nationalist unit, who presently was on a special mission and needed accommodation for the rest of the night. Nikolayevsky briefly flashed his forged identification papers. The Nationalist officers accepted him as real and advised the group of guerrillas to sleep in one of the barracks of the base.

During the night it was easy for Nikolayevsky and his men to pinpoint the most important targets of the base. Shortly before dawn, they attacked. The air base was destroyed, and the guerrillas' casualties were only two lightly wounded men.

Sometimes, it is necessary to break into an enemy building. This may well be difficult and is not recommended except in certain cases and then only in areas of a low security level. Many military installations do not really require a break-in. Often it is sufficient to merely observe the area from a distance, with binoculars and camera, in order to determine the vehicles or units deployed and their strength.

If the objective of the break-in is to steal secret documents from the enemy, it must be decided whether it is worth the risk to try to replace the documents after they have been copied. If possible, this should be done as the enemy then will not know that his documents have been exposed.

But if the intention is to return the documents several precautions must be taken. For example, the documents must never be folded when brought out from the enemy building, as this would be conclusive evidence that the document has been hidden and removed illegitimately from its proper file.

Another risk, if the enemy suspects that somebody will try to illegiti-

mately remove some documents, is that they may coat the documents with some colorless dye that will blacken the fingers, or the interior of a briefcase, of anyone touching them. Such dyes are reputed to be able to penetrate through leather gloves.

Techniques for opening and resealing letters

The traditional way of opening letters is still quite useful to know, especially if a break-in has been executed in a post office or in a mail box. If the letter is resealed in the proper way, the field operative can send it once again to its address, and the receiver will not know that the contents of it has been exposed.

There are several ways to open a letter. The operative must decide which method to use depending on the characteristics of the envelope.

First of all, it is important to wear for example rubber gloves so as not to leave any fingerprints on the letter. It is also important to avoid soiling the letter or the envelope with dirty or oily tools and equipment. Cleanliness is therefore a necessity.

If the envelope seems to be made of fairly hard paper, so that the glue has had difficulties in penetrating into the fibers, or the envelope lacks a sufficient amount of glue on the flap, it might be possible to use the dry opening method. This means that the glue will be separated into layers, one remaining on the flap and one on the body of the envelope.

A dry opening is unfortunately quite difficult to perform. Before the opening procedure is commenced, the operative must determine which flap is the most easy to open. A sharp tool is then inserted under the flap at the opening at the end of the envelope. The edge of the tool should be sharp, in order to be inserted properly, but the main part of the tool should have curved shoulders, so that the paper surfaces will be simply pushed away from each other, without any unnecessary cutting. The tool should be moved in a sawing motion, and the pressure must remain light during the entire process. If strong pressure is applied, the envelope may be damaged.

It is very easy to accidentally damage the envelope if using this method. Therefore, the utmost care must be used in the process.

The dry opening is not always possible to execute, or alternatively there might be a certain spot on the envelope which is resisting the dry opening attempt. The wet opening method can then be used in conjunction with

the dry opening method, if the glue used on the envelope is soluble or can be softened in water. When this method is used, a small and carefully controlled amount of water is applied to the outside of the envelope over the glue line. A wet piece of cotton, which is pressed down over the difficult spot, is used for this purpose. At the same time, continue to use the opening tool in the same manner as before. When the glue softens, it should be possible to open the envelope.

It is generally preferable to use hot water, instead of cold. The water used should be absolutely clean, so as not to soil the envelope. It is always safest to use distilled water.

The operative must also be careful not to wet the ink on the envelope or the letter. If there is writing or a stamp on the flap, the wet opening method is probably impossible to use. Check whether the ink will dissolve or not by lightly pressing a damp piece of cotton on it.

The most common method of opening a letter is the steam opening method. There are actually two different ways of opening a letter with the help of hot steam. The first method is similar to the previously described methods, in that a flap of the envelope is opened in order to remove the letter. The other method will be described below.

The amount of steam used is very important, as neither too little nor too much should be used. Too much steam may alter the characteristics of the envelope, and should therefore be avoided. This is especially important when opening envelopes made of thin paper. It is also preferable to use an opening tool made of wood, as the temperature difference between the tool and the hot steam otherwise will produce droplets of water, when the steam is condensing on the surface of the tool. In any case, the tool should be heated, and wiped dry, several times during the process.

To produce the steam, and to facilitate directing it to the proper spot on the envelope, an ordinary coffee-pot with a beak may be used. Some types can be directly connected to a wall outlet, thus dispensing with the need of a stove. They are easy to acquire and do not appear conspicuous, if found by the enemy.

Envelopes of manila paper or any other types of heavy paper should be opened by steaming open a small part of the flap at a time, lifting it with the opening tool, which should be kept under the flap but away from the glued portion. The glue might otherwise get stuck on the tool. Envelopes made of thin paper should however be treated in a slightly different

way, as the flap otherwise might get wrinkled. Here the opening tool should be held in a fixed position near the jet of steam. The envelope should then be moved across the tool at a speed determined by the rate at which the glue loosens. This requires a lot of practice, but the result is usually very satisfactorily.

In either case, it is important that the envelope is not allowed to reseal itself during the opening process. It is also necessary that no glue from the opening tool is allowed to leave marks on the inside of the envelope. This would be definite evidence that the letter has been covertly opened.

It is, however, not always necessary to open the entire envelope by steaming it. Instead another, older method of opening a letter can be used. This requires a powerful lamp and a split bamboo stick. The bamboo stick is inserted into one of the corners of the envelope. Only the corner will, if necessary, be steamed open. By checking the contents in front of the lamp, the bamboo stick will be used to grip the letter. By turning the bamboo stick, and thereby rolling the letter around the stick, it is then possible to withdraw the stick and by this procedure pull out the letter.

The letter can then be inserted again by the same method but in reverse.

A common method to prevent steam opening is to put carbon paper into the envelope, wrapped around the letter. The carbon paper will be damaged, if steam is used to open the letter. Other, similar ruses are also in common use. They will be described below.

Sometimes the envelope or the letter will be damaged in the process of opening it. This might result in torn fibers in the paper, or glue which has soaked through the paper. Torn fibers might be accidentally removed from one surface, and then attached to the opposite surface, for instance on a flap. If this is the case, the operative must attempt to repair the damage by rubbing the torn fibers off with a piece of damp cloth.

Excessive glue should be removed, if possible, so that it will not create any serious trouble later. This can be done by wetting it and then pressing a piece of dry cloth against the troublesome part. If the glue soaks through the paper, especially in isolated spots in the flap of a heavy paper envelope, then the chance of detection is fairly high.

If the damage seems to become severe, because of the glue soaking through the envelope, then it might become necessary to remove all glue, and then reapply a very thin layer of new glue in the same position. This is most easily performed by positioning the flap in between two damp

sheets of blotting paper, and then pressing a hot iron down on the sheets in order to steam off the glue. This process should be repeated several times. Afterwards the envelope must be carefully ironed dry. The iron must not be allowed to touch the envelope directly, however, as the paper then might be damaged. Always use a clean sheet of paper in between the envelope and the hot iron.

If the damage is less serious, and the glue has not created problems, it may be enough to simply tamp the torn fibers down in place. Some damage on the outside of the envelope can be explained by careless handling in the post office, but damage on the inside must be repaired in some way, or the recipient will become suspicious.

The operative must devote as much time and care to resealing the envelope as to opening it. If at all possible, the same glue as was used originally should be used once again to seal the letter. If another glue is used, then the two glues should look the same both under visible and ultraviolet light. In either case, the glue (or the water) should be applied with a brush, or with a piece of cloth.

If sufficient time is available, the envelope should be pressed for several hours under, for instance, some heavy books, before it is returned to the mail box. If time is not available, the same effect can be had by ironing the letter. Remember, however, never to touch the envelope with the hot iron without covering the former with a sheet of clean paper.

If an old-fashioned wax seal is used, it is sometimes possible to cut it, and later repair it, with a very thin and sharp, heated knife or razor blade. This will unfortunately not be sufficient if the enemy has a photograph of the original wax seal, and compares it to the seal on the letter, when it finally arrives. Then he will be certain to notice that somebody has tampered with the seal.

One way to avoid this is to make a mold of the original metal stamp used to create the seal. The original stamp is not necessary, as the seal in itself is a good impression of the stamp, and therefore can be used as a pattern to the mold. Making a mold, and then restamping the wax seal, is a time-consuming and difficult process.

First of all, choose the clearest, most complete, and thickest seal on the envelope, as this generally is the best one for reproducing the stamp, as well as for tampering with. Then brush a very thin layer of mineral oil over the face of the seal. The oil must be kept away from the paper. Only

the seal may be touched. Then mix some plaster of Paris with water, first pouring some water in a cup, and then slowly adding plaster in sufficient quantities to produce a mixture which is neither too thick nor too thin. Apply the plaster to the seal, while taking care not to allow it to flow off the edge of the seal and onto the paper.

Continue to build up the mold until it is sufficiently thick. This may require waiting for several minutes, while the original plaster is drying. The original layer of plaster must be sufficient to cover the entire seal, however, as the stamp will otherwise appear broken.

When dry, the slab of plaster will be used as a stamp. It should therefore be made sufficiently strong for this purpose, and its sides should be shaped as vertical as possible.

Before the piece of plaster is removed from the seal, remember to make some pencil marks on both the mold and the envelope, so that the new seal can be oriented on the envelope in exactly the same way as the original stamp. Sometimes there is no need for any pencil marks on the envelope, as the edges of the flaps can be used for this purpose. This should of course be considered before the operation.

When the mold has been removed, and checked for completeness, the operative should clean off any remaining oil or dirt from the original seal. Then place the mold face down in mineral oil, thus preparing it for use in the final process, without it becoming stuck in the wax at that time.

The original seal should then be heated, for instance with an infrared lamp. Be careful not to damage the envelope or the other seals. If heat cannot be applied exclusively on the seal, then the remaining parts of the envelope might be protected by wrapping with aluminium foil. As the wax softens up, it should be pushed from the edges inwards, and formed into a lump. This lump should be removed, and reused when the seal is finally being remade. When the wax has been removed, the envelope can be opened by any one of the opening methods described above.

When the envelope is to be resealed, the procedure is much simpler. First of all remove the mold from the oil, and wipe off any excess oil with a soft piece of cloth. Then position the lump of wax in its original position on the envelope, and apply heat to it. As the wax softens, make certain that it fills out the correct outline of the original pattern. Then apply some more heat, and finally push down the mold, after having aligned it properly with the pencil marks. This must be done with the utmost care, however, as too

much pressure will force the wax out from under the mold, and in this way ruin the appearance of the new seal.

Allow the wax to cool, and then carefully remove the mold. Any particles of plaster or oil must be removed, although a very light film of oil is sometimes applied to the new seal in order to make it look more shiny. The new seal should be compared to the other, original seals before this is undertaken, however, so that they look the same. Finally, do not forget to remove the pencil marks on the envelope, if any were used in the process.

It is, however, quite possible that the enemy has used waxes of different colors to make up one seal. If this is the case, then the wax cannot be melted and reused, as this will change the blend of colors of the wax seal. This process can never be duplicated exactly, but if the original types of wax are available to the operative, then it might be worth a try. It should however never be attempted if there is a serious risk that the enemy will compare the seal to a photograph of the original one.

Unfortunately, nowadays important letters are usually protected by security tape or metal, pre-fabricated seals. This makes it almost impossible to reseal the letters in a convincing way without access to unused security tape or seals of the correct type.

If ordinary cellophane adhesive tape, or an inferior type of security tape, is used to protect the envelope, the tape can be removed, however, by the application of carbon tetrachloride. Carbon tetrachloride is highly toxic, and must not under any circumstances be allowed to get in contact with the operative's skin. The chemical should be applied to the envelope with a brush, and then be allowed to flow under the tape, thus softening it up. The brush should not be used for introducing the chemical directly under the tape, as this can leave marks. By adding small amounts of carbon tetrachloride, and using a pair of pincers, the tape can then be carefully removed. Only touch the tape with the pincers, however, and only in one corner, so as to avoid leaving any marks or fingerprints on the tape.

Do not expose the removed tape to hot steam, if a steam opening is to be used. This will change the appearance of the tape. For this reason, the entire tape is usually removed, and stored on a clean and dry glass sheet, until it is returned to the envelope. If the operative will try to return the original tape, he must keep it free from dust and dirt, as this will very

quickly attach itself to the tape, and is indicative of the fact that the tape has been removed and repositioned.

When a tape has been removed from an envelope, some adhesive will always remain on the paper. This must be protected, for instance by clean aluminium foil, or else completely cleaned off, as the adhesive otherwise will attract dirt during the handling of the envelope in the continuing opening process.

When returned, the tape must naturally be positioned in exactly the same position as before the letter was opened. Some people will use the tape as a kind of trap for the person opening and resealing the envelope. This can be done by positioning the tape in a certain, overlapping way, or by including certain particles of dust or sand behind it. The operative must look out for this. It is always a good idea to snap a clear photograph of the original appearance of the envelope, and use it for comparison when resealing the letter.

There might also be stamps or writing under or on the cellophane tape. This must also be checked carefully. When repositioning the original tape, it is also vital to check whether the tape is completely dry or not. If a small wet spot of carbon tetrachloride remains under the tape, it might never dry because of a lack of air. Furthermore, the tape must not be repositioned with too much tension applied to it, as the envelope then will curl in a noticeable manner.

The enemy may also use some ruse hidden in the letter to determine whether it has been opened or not. The carbon paper hidden in the envelope has already been mentioned, but there are several other ruses known to be in use, too. In some cases the operative opening the letter will notice that he has been exposed to a ruse, but in other cases he will not.

Ruses can be of any kind. For instance, wax paper can be used in the same way as the previously mentioned carbon paper. The same is true of thermal printing paper. Parts of the letter might also be glued to the envelope. Spots of powdered dye may be hidden under the flap, so that they will color the envelope if it is opened by a wet opening. Pencil marks may be hidden under the glue line on the flap. Sometimes invisible ink has been used to mark or write down something across the flap. Extra glue may be used in certain spots, so as to cause damage to the envelope if it is opened carelessly.

Yet another method is to leave some broken part of the envelope under

the flap, so that the operator opening it will believe that he did the damage. He will then try to repair the broken part before he reseals the letter. A similar ruse is to leave a small part of the flap unglued, hoping that the operator will not notice it and subsequently glue it together. Other ruses are also possible.

Because of these reasons, the operator must carefully inspect the letter from all angles, before he attempts to open it. Ultraviolet light should also be used in this process, if possible. As was previously mentioned, it is advisable to retain detailed photographs of the original appearance of the letter during the entire opening and resealing process. If no camera is available, the operative must make detailed sketches of the letter, one from each side. The manner in which the letter is folded and positioned in the envelope should also be noted.

In order to check the position and outline of the contents of the letter, the envelope should be viewed in front of a strong light. Also remember to shake the letter, to determine whether it is glued to the envelope or not. If at all possible, the contents of the envelope should be determined before it is opened. When handling the letter, gloves should always be used, so as to avoid leaving any fingerprints.

If the entire flap is opened, the operator should make two small pencil marks across each side of the flap, so that he can properly align the flap during the resealing process. This will ensure that no marks in invisible ink will reveal the opening of the letter. The opening will be revealed, if the flap is not resealed in exactly the same position as it was originally sealed.

As a final note, the method known as the French opening should be mentioned. This method, although fast, is not recommended. In the French opening, the end of the envelope is simply cut off with a pair of scissors. The letter is then resealed by glueing the ends together with a narrow layer of glue. This method is easy to detect, and should therefore be avoided.

Surveillance techniques

To put surveillance on a certain individual usually requires that a number of operatives are available for following him or alternatively observing his residence. Surveillance may also mean that the operatives conduct observation on a specific building or installation. In this case, everybody who is in contact with the object is of interest, while surveil-

lance on an individual usually is restricted to only that specific individual and those individuals he is in contact with. In both cases, surveillance generally involves both physical and electronic methods of following and observing a target.

There are two general types of surveillance: mobile and fixed. A mobile surveillance is sometimes referred to as "tailing" or "shadowing", and the fixed, as a "stakeout" or "plant". A mobile surveillance may be made on foot or by vehicle, and is conducted when the persons under observation move from point to point and are followed by the surveillants.

A fixed surveillance is conducted when a person or activity remains in place, although surveillants may move from one vantage point to another in the immediate area.

Surveillance missions are fairly easy to execute in cities, but difficult to carry out in the countryside. The reason is naturally that there are more opportunities to hide on a crowded city street than in a deserted country area. Basically, though, surveillance is carried out in the same way in both types of terrain.

The surveillance team ideally consists of several people of both sexes, some on foot, at least one in a car, and one preferably riding a motorcycle. The team members need to be equipped with walkie-talkies or similar wireless communicators. A team of several members is necessary, as the target is highly likely to recognize one person, or one specific vehicle, which is following him all the time.

The surveillance team also requires a team leader who can direct the team members by wireless communication to different locations in the area. This is important, as the target may be alerted if he discovers that the same people follow him all the time. The team leader is responsible for directing that the operatives come and go in a seemingly innocent and natural way. The leader is ideally located in a command car, usually a van, located some distance from the area of operation. The command car should be equipped with maps and communication equipment.

In addition to this, a support car with driver is needed to pick up and let off team members on foot. In some cases it may be necessary to pick up everybody and leave the area, if for example the target leaves by taxi, or enemy personnel (police, military, or security service operatives) suddenly turn up in the area.

The latter incident can often be avoided by putting surveillance also on the police and military installations in the area. This can be performed

either through physical observation or by monitoring their radio communications.

The objective of following an individual in this way is to determine one or several of the following pieces of information.

- Location and movements of the target at particular times.
- The target's physical protection, such as bodyguards, security systems, etc.
- Defensive systems in house, office, vehicle, and other places where the target often appears.
- Contacts with other people, and identification of those people.
- Weaknesses in the target's personality, which might be used for exploiting him.
- The target's access to secret and vital information.

The first three points refer to details necessary for assassinations and other types of special actions, such as break-ins, kidnappings, and assaults. The last three points are necessary for determining the suitability and possibilities for recruitment of the target as a native agent.

Observation of a certain building or installation is much simpler. If the security level of the area is low, it is often possible to observe the installation from a shop or apartment across the street or, by the use of binoculars, from a distance. In other cases it is possible to observe the area by simply walking or driving past the installation regularly.

The objective of this type of surveillance is usually to determine the security precautions, number of guards, type and number of alarm systems, and similar pieces of information, necessary in order to plan a break-in, an assault, or a similar kind of special action.

All surveillance missions demand clothes and equipment which are not easily recognizable or remembered. This means that all surveillants must be dressed in order to melt into the crowds. Conspicuous dress must be avoided at all costs.

Another common mistake is to use a car with an easily remembered license plate number. The registration numbers of the group's vehicles must not be possible to read as a recognizable word, as this can cause the target to remember them. Furthermore, if the national registration number system also indicates state or city, all vehicles must be fitted with local license plates. Plates from other, distant areas may draw unnecessary

attention. It is also important to avoid all kinds of unusual colors, and this applies both to vehicles and to clothes.

If the target is unknown to the surveillant, the best method of identification is to have the subject pointed out to him in order to allow the surveillant to make his own observation. The surveillant should also be provided with a photograph and a detailed and accurate description of the target. A photograph and a detailed description of the target's car, if there is one, should also be obtained at the initiation of the surveillance.

An alternative method is to show the surveillants a video recording of the target, prepared during the preliminary surveillance before the regular surveillance begins.

The surveillants' dress and behavior should be in harmony with the area, neighborhood or group in which the surveillance is to take place. The dress must be inconspicuous and blend with the environment so that if the target sees the surveillant once or twice, or even more often, he will not have any lasting impression. The dress must therefore not be excessive in any way, which is sometimes the case when plain-clothes police officers try to "dress down" in order to look like criminals. In many countries the police tend to look more like something created by the film industry than like real criminals.

Especially the KGB agent-provocateurs in Moscow are known for their tendency to dress like caricatures of black marketeers. They frequently wear worn, foreign coats, American baseball caps, and jogging shoes. No decent black marketeer would dress like that.

Appearance should not stop at just the manner of dress. Rings or other pieces of jewelry indicating professional status or graduation from certain universities must be discarded. This also includes religious amulets customarily used in some countries by high risk professions such as soldiers and field operatives, as well as the rings many free-masons wear. If a ring is normally worn it should be replaced by an innocuous one, since the mark left on the finger would be visible and could arouse suspicion, leading to questions difficult to answer satisfactorily.

Weapons should only be carried if they do not detract from the chosen cover and appearance of the surveillant, as they otherwise could give their owner away. In addition to this, the surveillant should not have any physical characteristics which might attract attention to him. If at all possible, he should not appear alone but with his family in order to appear

completely innocent. In most areas (but not all!), a family will always be less suspected than a lone man.

When two or more surveillants are to work together, the team leader must ascertain that every surveillant completely understands the surveillance techniques to be used, and in which situation they should be used. Discreet signals should be arranged so that each surveillant will understand exactly what a given situation is, and proceed with plans previously formulated to cover the possible developments of events.

While planning is absolutely important and essential, it must nonetheless take second place to the adaptability and resourcefulness of the surveillants. Surveillants should be chosen for their ability and resourcefulness. They must have confidence, patience, and endurance.

Prior to initiating the surveillance, the surveillant should prepare and document a cover which will stand up if confronted by the enemy, or the police. This cover should explain why he is in the neighborhood and why he is participating in the activity he is undertaking.

As part of the preparation and planning it is advisable to also consider the use of electronic surveillance techniques. For foot surveillance, transmitters and receivers can easily be hidden on the person without arousing suspicion. For vehicular surveillance, electronic homing devices can be planted in or on the target's car. The use of night vision equipment for night-time surveillance should also be considered. For more information on this, see chapter 9.

The surveillant should never appear "furtive" by hiding in doorways or sporting theatrical disguises such as false beards. Such disguises have a tendency to fall off, for example if hit by a sudden puff of wind.

The surveillant should also be careful never to look directly into the eyes of the target. If a surveillant must look at the target while facing him, he should look slightly behind him or at his feet. The reason is that most people do not stare at each other, as they find it impolite. If somebody is staring at a person, this easily draws attention, as the person stared at may believe the other man to plan a robbery or an assault. The least reaction is, that the person stared at feels something odd, and may for the first time notice the surveillant. If the surveillant watches the target too closely, there is always a risk that their eyes instinctively will meet. This must be avoided at all cost.

A typical example of how easy it is for the target to detect such "furtive" behavior took place in Leningrad (now named once again St. Petersburg)

a few years ago. The KGB had initiated surveillance on a suspected foreign operative. At first, the target was not aware of the fact that he was being shadowed, but finally he noticed that a Russian stared at him in a remarkably intrusive way. When the two suddenly looked straight into each other's eyes, the Russian hurriedly withdrew his eyes and tried to hide his behavior by getting absorbed in the nearest shop window. Unfortunately for him, this window turned out to be empty, as the shop was temporarily closed for renovation.

In certain countries there are areas, known for being dangerous because of crime or other reasons. When in such openly dangerous areas, the surveillant should not appear too innocent. Instead he must even here try to adopt the manner common in the neighborhood. He should for example walk on the curb side of the sidewalk to preclude the possibility of being attacked from doorways or alleys, and to obtain the best observation vantage point. This means that it might be a good idea to walk on this side of the sidewalk also in safer areas.

For a really successful surveillance, the surveillant must be experienced. Only by experience is it possible to learn if the target really has "made" (identified) the surveillant just because he glances at him several times. This might not be the case, even though an inexperienced surveillant may believe so. On the other hand, however, it is not likely that an experienced field operative would show if he has noticed any enemy surveillance attempts.

It is also vital to study the topography of the area in which the surveillance is to take place so that areas or objects that will deny or clearly mark the observers to the target can be avoided. The surveillant must also be aware of the location of dead end streets or alleys so that he can avoid being trapped or discovered in those places.

Remember that in such situations minor changes in outer clothing, hand-carried items, etc., may alter the overall impression of the surveillant sufficiently to prevent recognition by the target.

It is a good precaution to always carry something, for example an attache case or a plastic bag. The reason for this is that plain-clothes police officers usually can be recognized by the simple fact that they never carry anything, which marks them from ordinary people, who usually carry at least a plastic bag.

The target will sometimes reverse his course, enter a dead-end street, board and suddenly depart from a bus, subway, or other public transpor-

tation system, or engage in any other ruses in order to provoke unconventional behavior by possible surveillants. The surveillants must try to counter this by carefully planned tactics and reconnaissance of the area.

Larger hotels, cinemas and theaters, restaurants, elevators, and most types of public transportation systems pose special problems to the surveillant. Generally, it is necessary to move closer to the target when he enters such areas in order to preclude his leaving through the usually many and various exits.

In restaurants, the surveillant should enter the restaurant quite soon behind the target and pick a seat where he can both ensure observation of the target and of the premises. The surveillant should order a meal which can be quickly prepared, preferably today's special, if such a course is on the menu. Should the target depart before the surveillant is served or he has been able to finish his meal, the surveillant should pay for his meal and leave. He must naturally always keep enough cash in the correct denominations to pay quickly.

When the target uses an elevator, the surveillant should use the same elevator. The surveillant should not announce a floor, as he does not know where the target will get off. If he must select a floor, he should select the top floor. If at all possible the surveillant should exit behind the target.

The use of public transportation systems is facilitated if the surveillant supplies himself with adequate small change or tickets in advance.

Surveillance can be either loose, close, or combined loose and close. During loose surveillance, the target need not be kept under constant observation. The surveillance should be discontinued if the subject becomes suspicious.

In close surveillance, however, the target is kept under observation continuously and surveillance is maintained at all times, even if the target appears to be suspicious and openly accuse the surveillants of following him. Close surveillance is only used in exceptional situations.

Combined loose and close surveillance is used if certain circumstances, usually depending on the target's actions, necessitate a change from a loose surveillance to a close surveillance. In these cases, preplanning is vital.

Even though it is almost always necessary to use an entire surveillance team for a really successful surveillance, it often happens that only one field operative is in position to conduct a surveillance. In this case, he must act alone. Special surveillance techniques have been developed to work

even if a proper surveillance team is unavailable. when on foot, the following techniques may be used.

A one-man surveillance is best employed in situations calling for a fixed surveillance. It should be avoided in a moving surveillance because it does not provide for flexibility. If a moving one-man surveillance must be resorted to, the surveillant should operate to the rear of the target when on the same side of the street and keep as close as possible to him in order to observe his actions properly. Crowd and street conditions will dictate the appropriate distance to be maintained between the target and surveillant.

When the target turns a corner in an uncrowded area (Fig. 1), the surveillant should continue across the intersecting street. By glancing up the street in the direction in which the target disappeared, he can once again note the target's position and actions, and act accordingly. The surveillant can operate from across the street from the target and later recross the street when the right opportunity allows him to fall in behind the target.

In a crowded area the surveillant should decrease the distance between himself and the target, and observe the target from the corner. Unless the target is standing just around the corner, the surveillance can be continued from the same side of the street. Do not turn a corner immediately behind the target, as the target may wait there in order to scrutinize everybody passing the corner behind him, memorizing their behavior, hoping to detect a surveillant. Another reason for not doing so, is that the target, if he already has detected the surveillant, may wait there to attack him.

When operating across the street from the target, circumstances will dictate whether to operate forward, to the rear, or abreast of the target. The surveillant should be abreast of the target when he turns a corner to enable the observation of any contact the target makes or to see if he enters any building.

If the target enters a railway or bus station ticket line, the surveillant should make an effort to get right behind him in order to learn his destination or overhear his conversation with the clerk.

If the target enters a telephone booth, the surveillant should enter an adjacent one to overhear any conversation, if possible. Otherwise he may wait beside the telephone booth, as if he was waiting to make a call. This might however expose him to the target, unless there are several people standing, waiting for their turn. In any case, the surveillant should try to

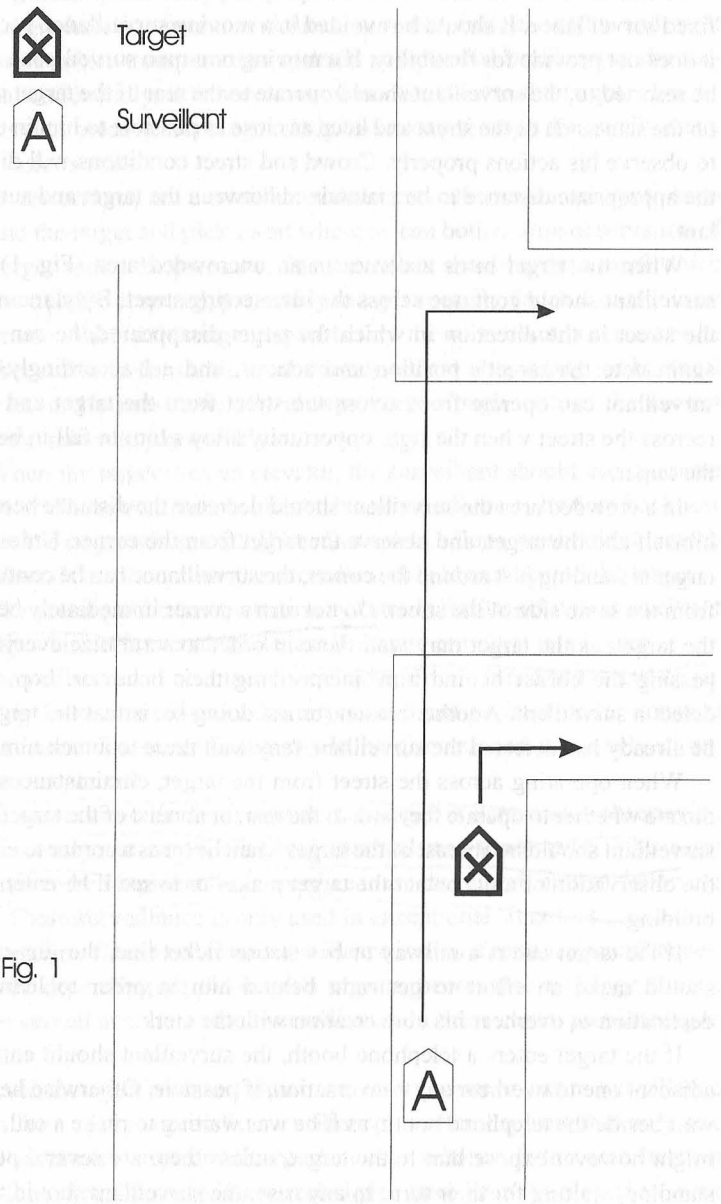


Fig. 1

overhear the target's conversation. It is unfortunately quite possible that the target is only simulating a call to check whether anybody is following him.

If the target leaves anything behind, an effort should be made to recover those items discarded by him. Likewise it is worthwhile trying to recover second sheets from pads which the target has used. These sheets can sometimes be read, by raking the sheet with a narrow beam of light. This is most easily done by shining a small flashlight on the sheet at the steepest possible angle. The lens of the flashlight should be positioned right at the edge of the paper. The fibers of the sheet will have been altered by the pressure from writing on the top sheet, and these irregularities on the surface of the paper will sometimes be revealed by the raking light.

However, the surveillant should avoid picking up an item discarded by the target when this might lead to his recognition of the surveillant.

Two-man surveillance (or "AB" surveillance) is characterized by the use of one surveillant, known as "A", directly behind the target. A follows the target, while the other surveillant, known as "B", follows A either on the same side of the street or from across the street.

When both surveillants operate on the same side of the street as the target, and the target turns a corner, A continues in the original direction and crosses the intersecting street, and from a vantage point there signals the correct moves to B. B should not turn the corner or come into sight of the target until he has received the signal to do so.

When B is operating across the street and the target turns a corner to the right, away from B, B will cross the street behind the target and take up the A position, while A crosses the intersecting street and takes up the B position (Fig. 2). This move should be prearranged, and no signals should be necessary.

All visual signals employed should be discreet and consistent with the environment. The signals could be anything such as scratching one's head or moving a plastic bag from one hand to the other.

Should the target instead turn to the left and cross the street toward B (Fig. 3), B should drop back to avoid meeting the target. B could go into a store, or continue straight ahead. B should keep A in sight to observe his signals indicating what the next move should be. A should continue in the original direction and cross the intersecting street, and if the situation demands it, take up the B position by crossing the street after the target.

Three-man surveillance (or "ABC" surveillance) is intended to keep

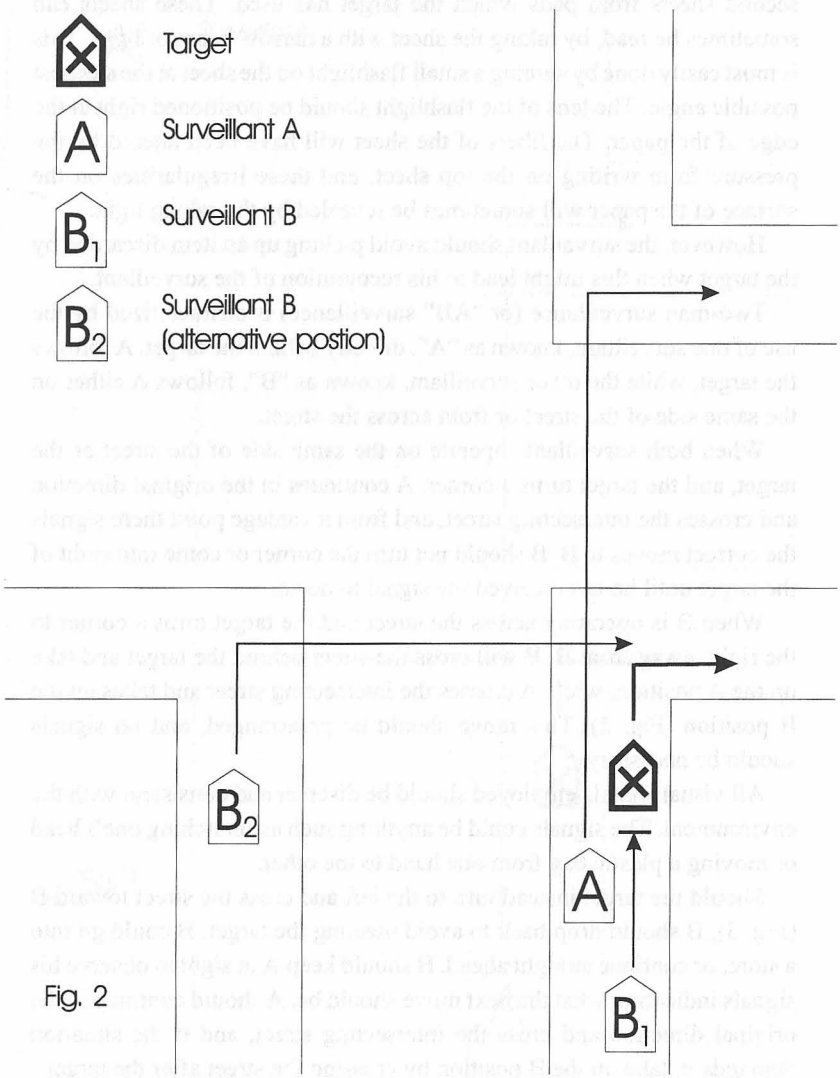

Target
A
Surveillant A
B1
Surveillant B
B2
Surveillant B
(alternative postion)
B2
A
B1

Fig. 2

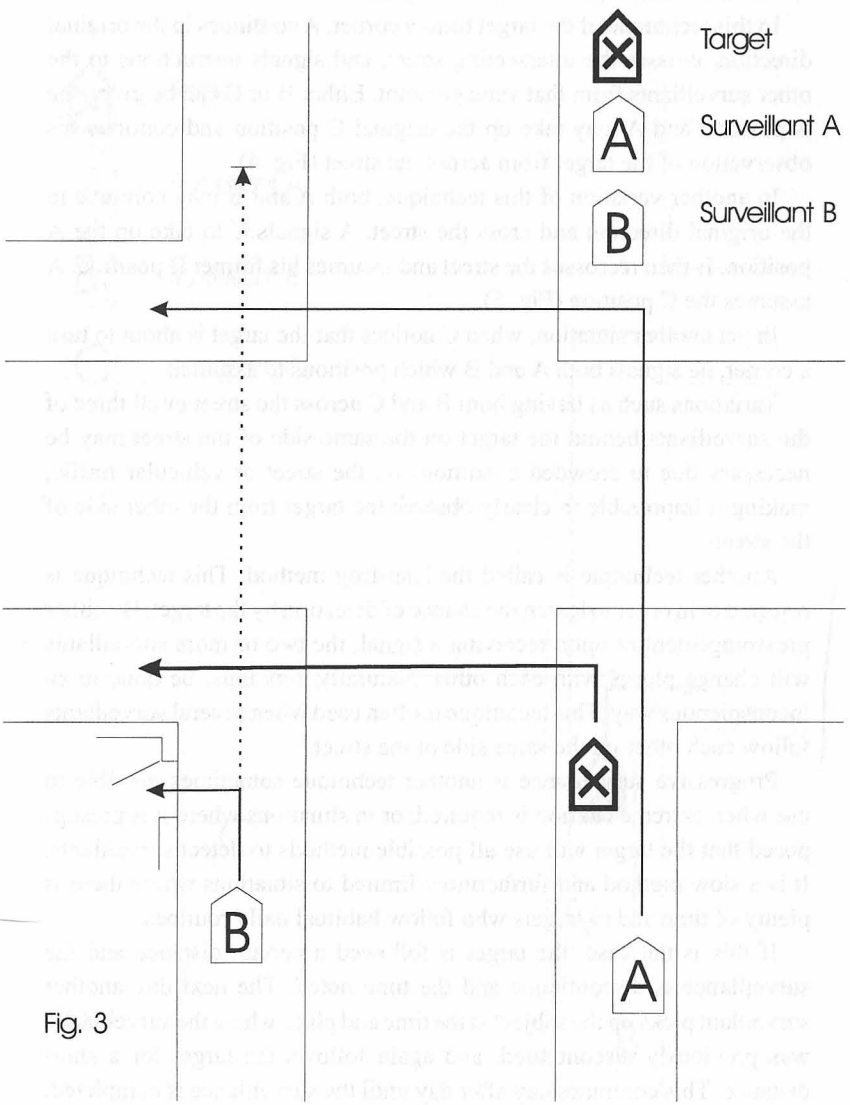


Fig. 3

two sides of the target covered. A follows the subject. B follows A and concentrates on keeping A in sight rather than the target. The normal position for B is behind A. The third surveillant, known as "C", normally operates across the street from the target and slightly to his rear, enabling C to observe the target without turning his head.

In this technique, if the target turns a corner, A continues in the original direction, crosses the intersecting street, and signals instructions to the other surveillants from that vantage point. Either B or C can be given the A position and A may take up the original C position and continue his observation of the target from across the street (Fig. 4).

In another variation of this technique, both A and B may continue in the original direction and cross the street. A signals C to take up the A position. B then recrosses the street and assumes his former B position. A assumes the C position (Fig. 5).

In yet another situation, when C notices that the target is about to turn a corner, he signals both A and B which positions to assume.

Variations such as having both B and C across the street or all three of the surveillants behind the target on the same side of the street may be necessary due to crowded conditions on the street or vehicular traffic, making it impossible to clearly observe the target from the other side of the street.

Another technique is called the leap-frog method. This technique is resorted to in order to lessen the chance of detection by the target. By either prearrangement or upon receiving a signal, the two or more surveillants will change places with each other. Naturally, this must be done in an inconspicuous way. This technique is often used when several surveillants follow each other on the same side of the street.

Progressive surveillance is another technique sometimes possible to use when extreme caution is required, or in situations where it is presupposed that the target will use all possible methods to detect surveillants. It is a slow method and furthermore limited to situations where there is plenty of time and to targets who follow habitual daily routines.

If this is the case, the target is followed a certain distance and the surveillance is discontinued and the time noted. The next day another surveillant picks up the subject at the time and place where the surveillance was previously discontinued, and again follows the target for a short distance. This continues day after day until the surveillance is completed.

Very often, the target is not only walking on foot but also moving

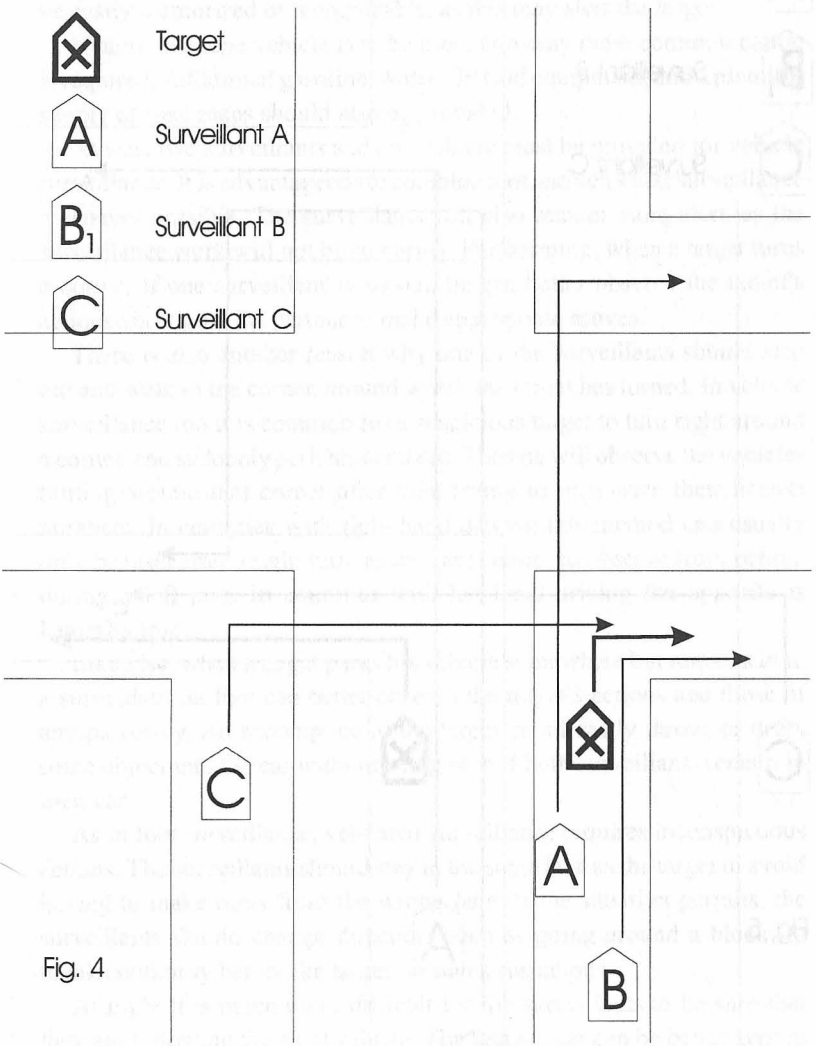


Fig. 4

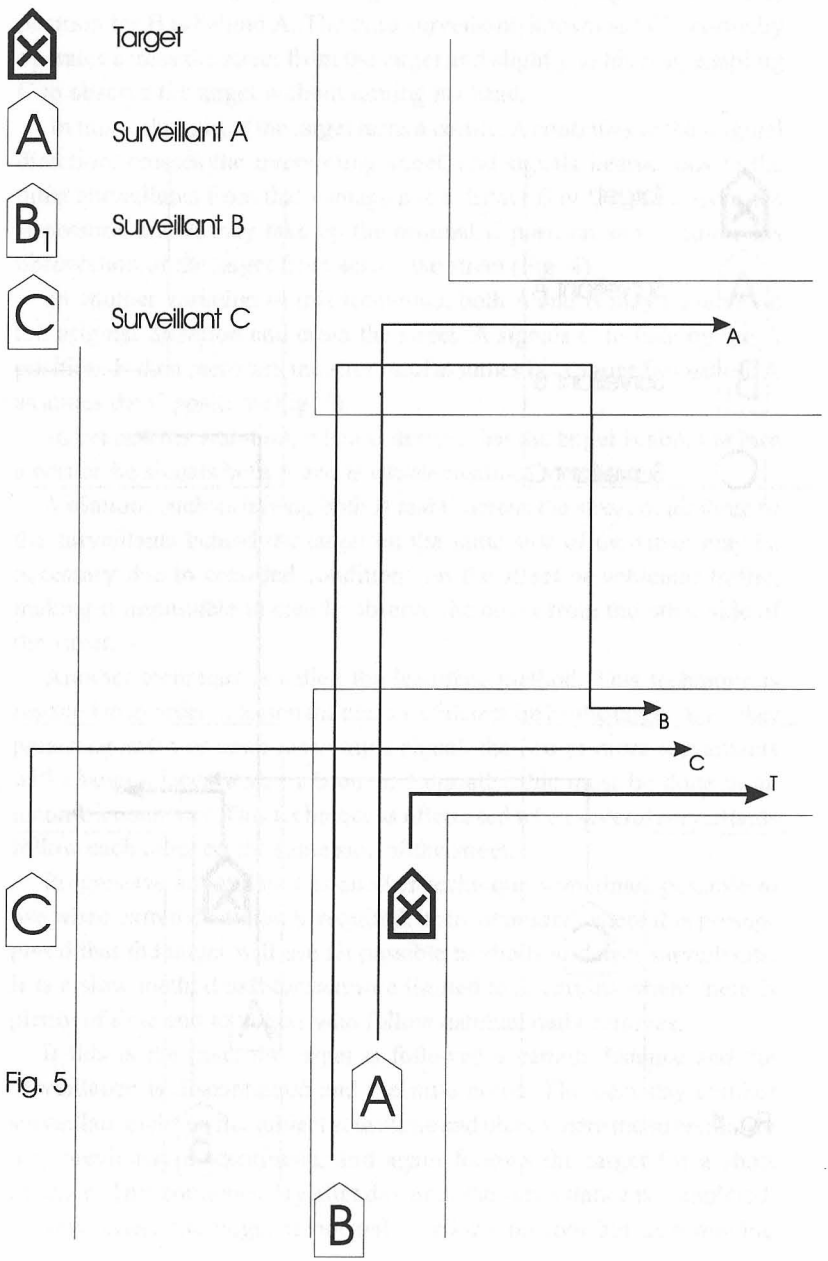

Target
A
Surveillant A
B1
Surveillant B
C
Surveillant C
A
B
C
T
C
A
B

Fig. 5

around in a vehicle. When this is the case, the surveillants must resort to partly other techniques. First of all, at least one dependable vehicle must be provided similar to types commonly used in the area in which the surveillance is to take place. The license plates must not be identifiable as belonging to the operative. They should be of the country and, if applicable, state or city in which the surveillance will take place. They should not be easily memorized or recognizable, as this may alert the target.

If more than one vehicle is to be used, two-way radio communication is required. Additional gasoline, water, first aid equipment, and a plentiful supply of road maps should also be provided.

At least two surveillants and one vehicle must be provided for vehicle surveillance. It is advantageous to combine foot and vehicular surveillance whenever possible. The surveillants will also remain more alert, as the surveillance work will not be so boring. Furthermore, when a target turns a corner, if one surveillant steps out, he can better observe the target's actions and signal his partner to make appropriate moves.

There is also another reason why one of the surveillants should step out and walk to the corner, around which the target has turned. In vehicle surveillance too it is common for a suspicious target to turn right around a corner, and suddenly park his car there. Then he will observe the vehicles turning around that corner after him, trying to memorize their license numbers. In countries with right-hand driving this method can usually only be used after a right turn, as the car is easier to observe from behind during a left turn. In countries with left-hand driving the opposite is naturally true.

Likewise, when a target parks his vehicle somewhere but remains in it, a surveillant on foot can better observe the target's actions and those of any passer-by. An accomplice of the target could easily throw, or drop, some object into the car without being seen if both surveillants remain in their car.

As in foot surveillance, vehicular surveillance requires inconspicuous actions. The surveillants should stay in the same lane as the target to avoid having to make turns from the wrong lane. If the situation permits, the surveillants should change direction, such as going around a block, to break continuity before the target becomes suspicious.

At night it is much more difficult for the surveillants to be sure that they are following the right vehicle. The target's car can be better kept in sight if the car is distinctive. If the opportunity presents itself, a piece of

reflectorized tape may be attached to the rear of the car or a red tail-light glass can be broken. A white rear light is easily followed.

The surveillants' car should also receive some attention. The dome light should be disconnected so that the light will not show when a door is opened, such as when one surveillant steps out. One or both of the headlights and the license plate lights, if any, can be wired to permit them to be turned on or off independently of each other. With this simple method the night-time appearance of the vehicle can be changed quickly and efficiently.

It is however necessary to remember that the target's vehicle may also be improved in this way.

One-vehicle surveillance is not recommended. The surveillants' vehicle must remain close enough behind the target to permit the surveillants to observe his actions, but far enough behind to escape detection. When the target's car stops, one surveillant should follow his actions on foot. The target will hopefully not expect to be tailed by a person on foot while he is using his vehicle.

When the target turns a corner, the surveillants may make one of two possible moves (Fig. 6). They may continue in the original direction, cross the intersecting street and make a U-turn, as the target will take less interest in a car turning into the street behind him coming from a direction that is opposite to that which he was travelling before turning the corner.

An alternate move would be to continue in the original direction, crossing the intersecting street and continuing around the block. The surveillants will then resume contact with the target somewhere on the street along which he is driving, turning after him. The target will probably not expect to be tailed by a car approaching him from a direction to his front. Naturally, it is essential to know the area well before trying one of these moves, as especially an unexpected one-way street may cause the plan to fail completely.

The two-vehicle surveillance technique is similar to the two-man technique of foot surveillance. Two vehicles follow the target at different distances on the same street. This technique can be varied by having one vehicle going in the same direction as the target on a parallel street while receiving radio-transmitted directions from the surveillants directly behind the target.

This technique is naturally more flexible than one-vehicle surveillance in that two vehicles can exchange places from time to time (Fig. 7).

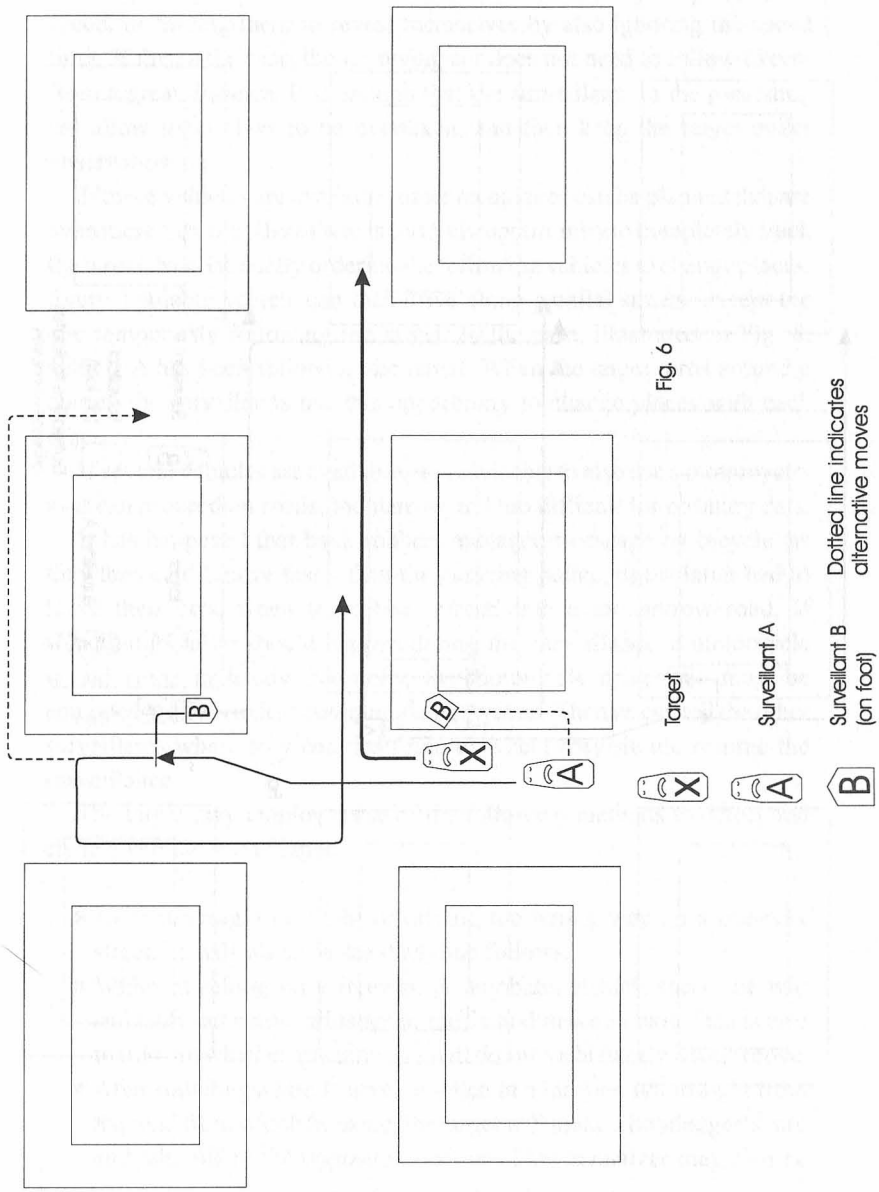

B
X
A
B
B
X
A
Target
Surveillant A
Surveillant B (on foot)
Dotted line indicates alternative moves

Fig. 6

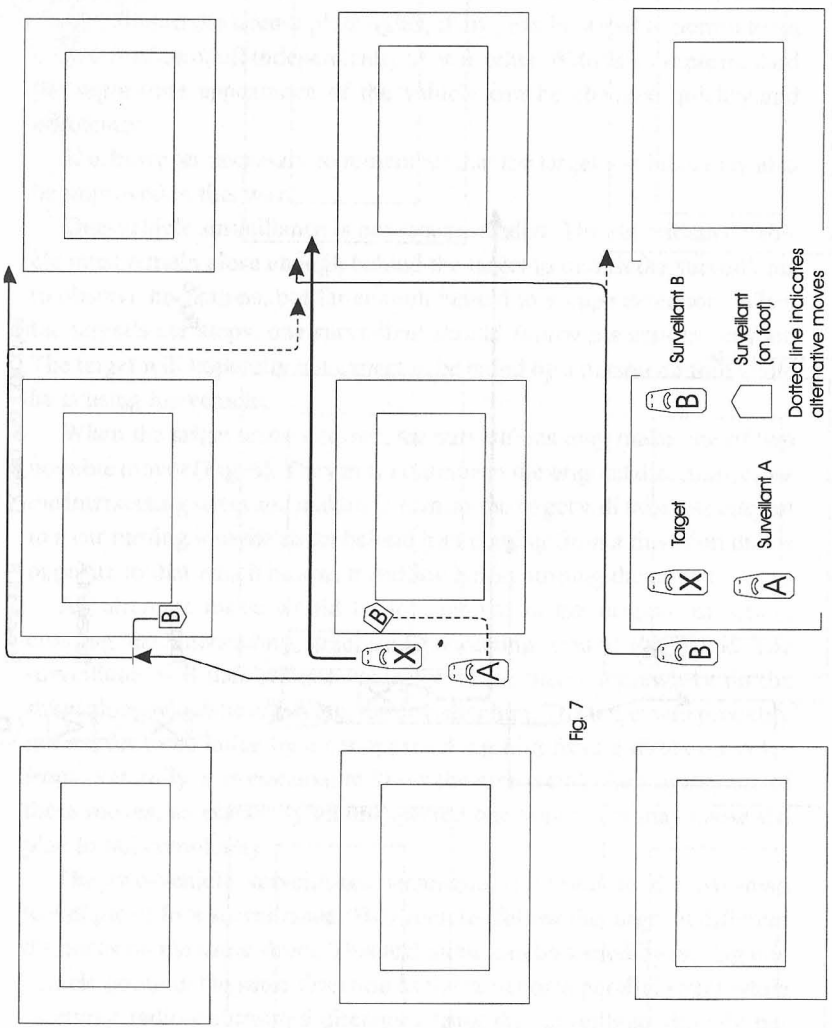

B
B
X
A
B
Surveillant B
Surveillant (on foot)
Dotted line indicates alternative moves
Target
Surveillant A
X
A
B

Fig. 7

One of the vehicles can also precede the target. This may safeguard against discovery if the target tries to detect any surveillants by seriously breaking the speed limit, either trying to lose any surveillants by the higher speed, or forcing them to reveal themselves by also ignoring the speed limit. If this is the case, the following car does not need to follow except from a great distance. It is enough that the surveillants in the preceding car allow themselves to be overtaken, and then keep the target under observation.

If more vehicles are available, other techniques can be planned that are even more flexible. Here there is certainly opportunity to completely track the target, by continually ordering the following vehicles to change places. Every available vehicle can then drive along parallel streets, except the one temporarily following the target. In the case, illustrated in Fig. 8, vehicle A has been following the target. When the target turns around a corner, the surveillants use this opportunity to change places with each other.

If several vehicles are available, it is advisable to also use a motorcycle, as it can proceed on roads, too narrow and too difficult for ordinary cars.

It has happened that bank robbers managed to escape by bicycle, as they then could move faster than the pursuing police, as the latter had to leave their cars, when the robber turned into a too narrow road. If something similar should happen during the surveillance, a motorcycle would come in handy. Naturally, the motorcycle driver too must be equipped with a wireless communication system. Then he can tell the other surveillants where they can meet him or where they should resume the surveillance.

The target may employ some of the following methods to detect and elude a vehicle surveillance.

- After running a red light or driving the wrong way on a one-way street, he will watch to see if anyone follows.
- While travelling on a freeway or autobahn at high speed, he will suddenly cut across all lanes of traffic and make an exit. This is also to find out whether any other car will do such a blatantly wrong move.
- After rounding a blind curve, or when in a location not in sight from the road from which he came, the target will make a bootlegger's turn and take off in the opposite direction. This maneuver may also be

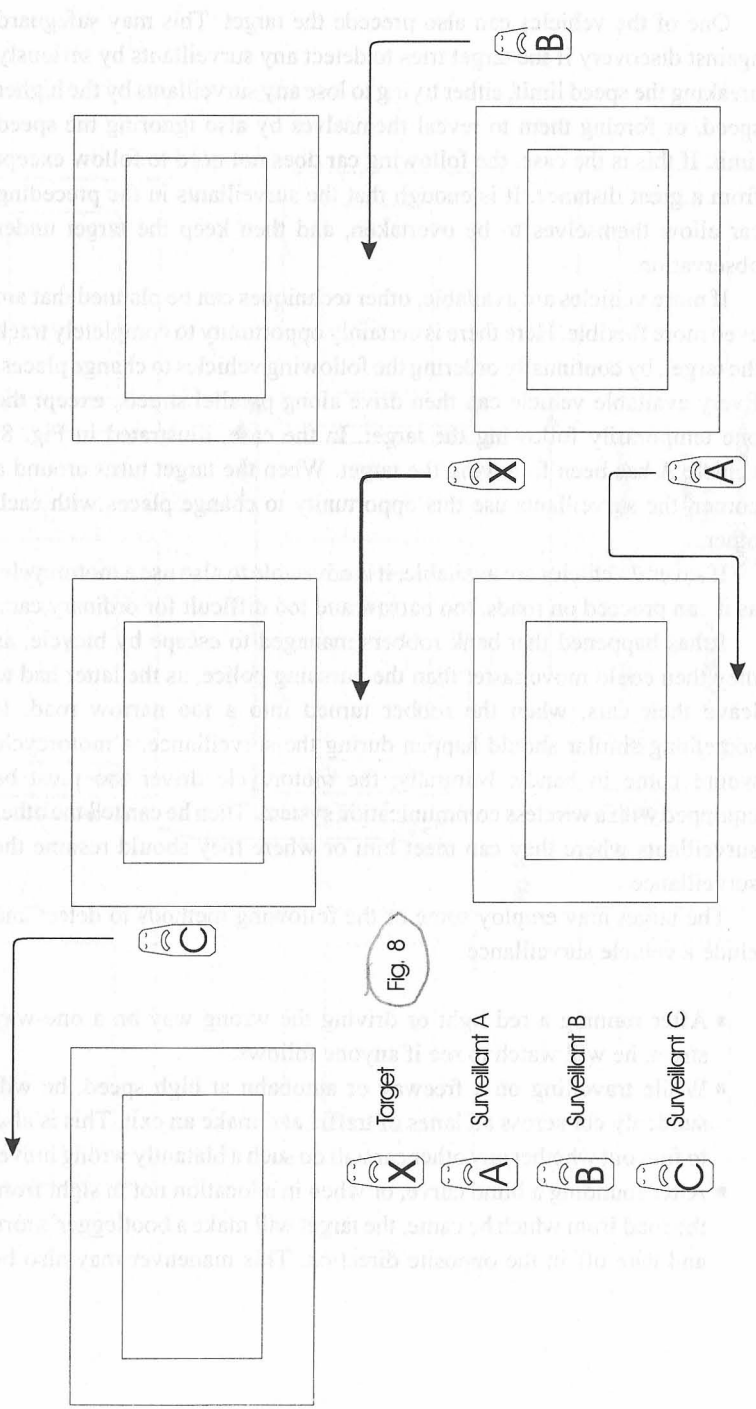

B
X
A
C
Target
Surveillant A
Surveillant B
Surveillant C
X
A
B
C

Fig. 8

executed on a long bridge, as long as the bridge is not divided between the two lanes of opposing traffic, or the traffic is too heavy.

- After turning a corner, the target may pull over and park. He will then try to memorize all vehicles turning after him.
- The target may pass through alleys, bad roads, or even cut across people's lawns.
- The target may have a friend following him in order to detect any surveillance.

The first and the second methods are interesting because they are not conclusive evidence that the driver expects to be under surveillance. He may merely be a bad driver. They should however if possible be avoided, as they nevertheless will draw the attention of the surveillants.

The other methods, with the exception of the last one, should always be avoided, unless the situation clearly is an emergency. The surveillants will understand that they are following the right individual, even if they were not certain before.

The last method is inconspicuous and highly effective, and should always be used by a cautious target. The surveillants must be prepared for this possibility and not reveal themselves by using mystical signals and gestures even if the target is out of sight. This applies whether on foot or in a vehicle.

Moving vehicles can also be located by the use of automatic direction finding systems. Such a system can also be used for monitoring the progress of important vehicles or vehicles carrying valuable cargo. The system consists of two parts, the transmitter (frequently called a "bumper beeper") and the receiver (Fig. 9).

The miniature transmitter is easily mounted onto car bumpers, gas tanks, or other metal objects of the vehicle to be followed. It has a magnetic base which secures the transmitter into place, so no wire connection is required.

If the system is used for monitoring the progress of important vehicles, the transmitter is permanently installed. It is then powered from the car's battery and the car's own radio antenna is used for transmitting.

The receiver, usually fitted on the dashboard of a vehicle, informs a pursuing vehicle, or aircraft, of direction changes, relative course, and distance. A helicopter can also be used for this purpose. The signal strength indicator surveys relative distance (this gives an idea of the tracked car's

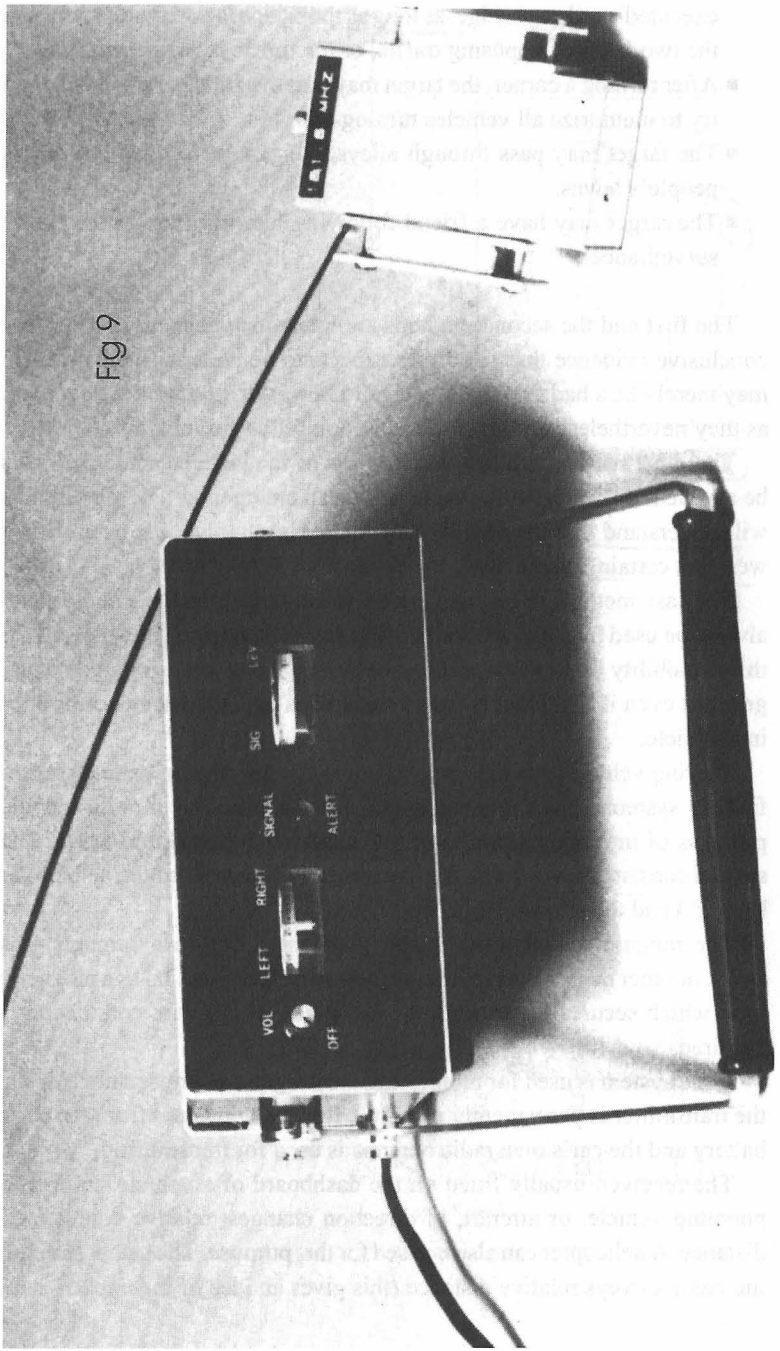


Fig 9

speed) and a visual/audible signal alert distinguishes the transmitter's signal from outside interference.

The receiver's antenna is magnetically sealed to the car roof and permits observation up to one and a half kilometers during ground to ground surveillance. Air to ground reception range may be as high as 80 km.

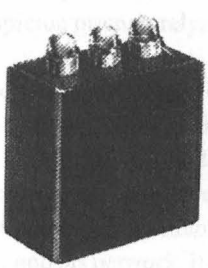
The transmitter is crystal controlled so as to ensure that the signal is not lost if the transmission drifts in frequency.

The transmitter is however easy to detect by a physical search. Another possibility is to use a field strength meter. This is a device designed to measure the relative radio frequency energy which is present at a certain point. With the meter in hand and, if it is suspected that a permanently placed transmitter is used, the vehicle's ignition on, it is easy to check in, on, and especially under, the car. In the middle of a city, however, it might be necessary to first normalize the meter to the local environment, as there probably is a high level of radio frequency background energy.

It is also possible to secure an infrared strobe light (Fig. 10) at the rear of a car. This will emit invisible infrared light, which can be easily detected by for example a pursuing driver wearing infrared goggles. This technique is quite useful at night. For further information on this, see chapter 9.

In a fixed surveillance, or stakeout, it is the target that remains stationary. The surveillant may move around for closer observation of the area as well as to evade discovery.

Fig 10



When only one surveillant is detailed to watch a place with more than one exit (a most unfortunate situation), the surveillant may have to move about considerably in order to maintain the proper surveillance.

When preparing for a fixed surveillance, the base of operations should be well planned. It may be a shop, apartment, house, car, or truck. A thorough, but cautious, reconnaissance should be conducted of the area or building from which the surveillance is to be made. Necessary equipment such as binoculars, cameras, electronic equipment, and sound recording devices should be provided, if available.

Specific arrangements should be made for such mundane matters as food and drink, and access to toilets for the surveillants. It is also necessary to provide relief for the surveillants, if the surveillance is to proceed around the clock. Communications contact with headquarters might also be necessary to arrange, if there is a headquarters to have contact with.

In situations in which the surveillant cannot observe from a fixed base it may be necessary for him to assume a role such as a salesman, telephone repairman, newspaper vendor, street sweeper, or any other occupation that will not attract undue attention.

The use of disguised vans and trucks as observation posts in fixed surveillance should also be considered. Such an observation post is very suitable in most situations, because of the inherent mobility.

5

Protracted Missions

Protracted missions are performed in order to recruit native agents, or to plant "sleeping" agents in the target country. Native agents are usually divided into two different types: ordinary agents and agents of influence.

Ordinary native agents collect information about their own country, by either legal or, more often, illegal means. They deliver this information in various ways to the field operatives, who deliver the information to the analysts in the intelligence service headquarters.

Agents of influence are native agents who never collect information or participate in illegal activities, and therefore need no illegal contacts with the field operatives. These agents only strive to attain a position of influence in their society, where they, upon orders from the intelligence service headquarters, act in a manner favorable to the controlling country. Agents of influence can often be found among politicians. One such example was the Norwegian politician Arne Treholt, who was arrested in 1984 at Oslo Airport, on his way to Vienna to meet his KGB contact.

Sleeping agents are field operatives, or native agents, who infiltrate the target country and maintain their cover for several years, or even decades, until in a crisis situation they are activated by orders from the headquarters. Until then, they execute no intelligence missions whatsoever, as this could cause them to fall under suspicion prematurely, thus spoiling maybe years of preparations.

Field operatives assigned to protracted missions must frequently work undercover for long periods of time. This may cause serious psychological problems, such as loneliness, depressions, and difficulties to distinguish between cover and real background. These problems may lead the field operative to seek relief in romantic attachments, which later may cause the exposure of the operative and his network. It has happened that security services try to ensnare suspected foreign agents by enticing them to fall in love with beautiful police agents.

Another problem is that the operative might keep mementos from his

real family, in this way compromising his cover. If this is detected by the enemy security service, the result will be the same as mentioned above. The operative and his network will be exposed.

Problems of this kind are common and must not be neglected under any circumstances. Many otherwise successful operatives have been exposed by this problem only.

Recruitment techniques

The recruitment of native agents is the most hazardous and difficult task of all intelligence activities. The field operative finds himself at a serious disadvantage from the very first step, as he has to expose his own role even before the intended agent has given his reply. If the answer is negative, the field operative has given himself away. This necessitates the most careful planning and delicacy, as well as ability to judge men correctly, on the part of the field operative.

The first step therefore consists of research. It is first of all necessary to determine whether the intended agent is able to deliver the needed information or if he instead might be of any potential future value.

Then the life story beginning with the childhood, school years, and so on must be researched to determine his character traits. All kinds of weaknesses and vices, his moral character, ambitions, views and beliefs, but also his private life, friendships and relations are necessary to study in detail. It is also necessary to determine the right approach to the person and, if possible, the proper person, such as a friend or colleague, to work through in the initial contact.

If this part of the operation is not executed in a satisfactory way, the entire operation will be put at risk. One classical example of how a recruitment is not supposed to be executed, was the Soviet attempt in 1969 to steal the French fighter-bomber aircraft Mirage IIIE from Lebanon, at that time (before the civil war began in 1975) a modern and civilized country.

Two Soviet GRU operatives, Vladimir Vasiliev and his senior officer Aleksandr Komiakov, had received the mission to recruit a Lebanese combat pilot, who could be persuaded to fly a Mirage IIIE to the Soviet Union. They consulted an already recruited agent, Hassan Muhammad Badawi, a Palestinian who had been a flight instructor in the Lebanese Air Force. Badawi in his turn contacted one of his ex-students, Lieutenant Mahmoud Matar, who was currently flying the Mirage. Badawi offered

him three million dollars (later cut down to two million dollars), to simulate a crash during a routine flight and then fly the aircraft to the Soviet Union.

The GRU operatives did not see any need to do any research in Matar's personality and character. They believed that an Arab would never be able to resist such a tempting monetary offer. That was their first mistake. Matar actually went straight to his commander and reported the recruitment attempt. The Lebanese security service, Deuxième Bureau, decided to beat the Russians at their own game, and asked Matar to pretend to accept the deal, as well as try to live up to the stereotyped image of Arab mentality, which the GRU seemed to believe in.

Finally the negotiations between Matar and the two GRU operatives were successfully concluded. GRU had even promised to fulfill Matar's condition, that the advance payment was to be paid with a bank cheque worth two hundred thousand dollars, written and guaranteed by the Moscow Narodny Bank office in Beirut. It had also been decided that the final meeting would take place in Vasiliev's apartment.

Those were two more mistakes. A clandestine meeting must never take place in the home of one of the operatives. Furthermore, the Moscow Narodny Bank cheque was definite evidence that the Soviet Union was involved in the deal. The operatives could easily have avoided this by insisting on paying in cash, or with a cheque from a foreign bank.

The final meeting was suddenly interrupted when Lebanese soldiers raided the apartment. After a short gunfight, in which both Vasiliev and Komiakov were wounded, the two operatives were overpowered and arrested. Their final mistake had been that they did not even try to look for any electronic bugging equipment, such as the radio transmitter which Matar was carrying on his person. Because of this, the Lebanese had been able to listen in on the entire discussion. In this way, they had ascertained which was the best moment to raid the apartment.

The responsibility for all these mistakes was undoubtedly with Komiakov. The leadership of the GRU must have been of a similar opinion, as Vasiliev in due time was permitted to continue working abroad. His next assignment, in 1976, was in Canada. Apparently the GRU had decided to keep him out of the light for a few years, so that the mistake in Lebanon would be forgotten.

Most people agree to become spies for one or several of the following reasons:

- Idealistic purposes.
- Money, career enhancement, and other motives of personal gain.
- To conceal a committed crime and escape the responsibility for committing it.
- Homosexual deviations and other vices.
- Romantic attachments.
- Love of adventure, or search for a purpose in life.

The most common targets in recruitment operations can therefore be characterized in the following way.

The ***idealist*** believes so strongly in the policy of the field operative's government, so that he shuns no sacrifice, personal or monetary, in order to further his ideal. These people are usually the most reliable and frequently refuse money for their cooperation. They do tend however to leave the idealistic phase when they grow older and then they often become more interested in personal gain.

This kind of person is not so common among the western nations nowadays. They are uncommon among the Russians, too. They can still be found in less developed countries, however.

The ***alienated intellectual*** is honestly concerned about social and economic problems, as well as contemptuous of his own society, but he is also an intellectual snob, susceptible to individual bribery such as study grants, consultancy fees, access to top decision-makers, etc. He is generally more concerned about personal security and welfare than the idealist.

The ***greedy government employee*** has no sense of guilt if he offers his services to anybody willing to pay the price (this may actually include several rival governments). These individuals often tend toward egotism, and they also tend toward promiscuity, alcoholism, and other vices. These characteristics frequently stem from an unwillingness or inability to compete in an open society.

The ***spoiled brat*** frequently desires career enhancement or becomes a traitor in order to conceal committed crimes. This person is characterized by an unwillingness to sacrifice his own security, while his privileged upbringing, free from problems due to parental indulgence, makes him indifferent to the needs and desires of others.

The ***lonely secretary*** is characterized by an inferiority complex, which makes her (or him) susceptible to romantic, or in some cases homosexual,

affairs. Such affairs tend however to be short lived, but may in a few cases turn out to be profitable for the recruiting field operative.

The ***corrupt civil servant*** frequently began his career by taking bribes on a small scale. When he has reached the top, the only difference is that the bribe now has to be bigger. Bribes need to be understood literally, however. It is quite possible that privileges and various advantages, belonging to a certain position, will be used in this way. It is very common that politically appointed civil servants are susceptible to such bribes.

The ***homosexual*** can be found in any position, and is frequently characterized by a stronger loyalty to other homosexuals than to his own government.

The Soviet intelligence services frequently exploited homosexual "operatives" in order to recruit foreign, homosexual senior civil servants. It has happened several times, that the intended agent, even when he refused the recruitment attempt, declined to report it, either because he feared to be known as a homosexual or because he did not want to expose a "brother", that is another homosexual.

The ***adventurer*** has a dangerous love of adventure, often coupled with a search for a purpose in life, apparently not provided by his own society.

Many people combine several different character traits from these general character types, and most individuals have at least one of the unsympathetic traits, even if only in a weak form. It is however important to remember that all individuals are just that, individuals, and therefore different. In some cases one of these traits is countered by a stronger, positive trait. The operative must carefully analyze his victim before he makes a recruitment attempt.

Despite this warning, individuals of these types are the ones to search for. Furthermore, it is often easier to recruit men of high position in society than ordinary, humble people, as the latter tend to be more loyal and honest than the former, who generally have had to rid themselves of most loyalties in order to reach their high positions.

The professions searched for in recruitment operations do naturally vary according to the needed type of information. Remember, though, that secretaries, code clerks, and cleaners often have as much access to secret information as politicians, diplomats, and high military officers.

The second step consists of the first contact. This must be brief in order not to alert the potential agent. The location and means of contact are of

paramount importance. Everything learned during the research step must be utilized in order to put the potential agent at ease.

A mutual interest in hobbies, athletic contests, or other leisure time activities may provide a medium for getting acquainted with the potential agent. The field operative should not pose as an authority on a subject, however, unless he is well qualified. Many times an admitted lack of knowledge but an active interest in a given subject will cause an advance by the potential agent so that he can display his superior knowledge.

The third step consists of cultivating the potential agent's acquaintance by creating a friendly relationship and, most importantly, a debt of gratitude to the operative. The potential agent must be given gifts, expensive dinners, and friendship. In due time the field operative will ask for some favors such as freely available information, which is not secret in any way.

At this stage, it is a wise precaution to try to give a clandestine character to the relationship with the potential agent. This should be done as soon as possible. Tell, for example, the potential agent not to call you at work. Mention a reason, which seems valid to him, such as that your boss disapproves. Instead, try to arrange more or less clandestine meetings in safe places, such as parks, restaurants, and other public places.

There are two reasons for introducing this secrecy. First. it gradually conditions the potential agent to the next step in the recruitment. Second, it minimizes the risk that an enemy security service will notice your activities, and warn the potential agent not to have any contacts with a foreigner.

It is also sometimes a good idea to visit the home and family of the potential agent. But it must be remembered that the wife of an agent may be a stumbling block, if she worries about her husband's relationship with a foreigner.

But it is also possible that the wife of an agent might encourage him in his work. This is also true of recruitment attempts. One of the first successful cases of industrial espionage, executed by the NKVD (one of the earlier names of the KGB), could only be successful because of the skillful manipulation of the wife of a certain Herr Worm, a discharged inventor from the Krupp factories.

The discharge was caused by the fact that Worm had actually created his private company, competing with Krupp, at the same time as he was employed by the latter. After the discharge, the Worm family had however

got into serious economic difficulties. This felt especially bad for Frau Worm, the inventor's wife, as she desired a high standard of living.

The Soviet operative noticed this, and thereby managed to persuade her, by the help of promises of consultancy fees to Herr Worm as well as more direct, advance cash payments to his wife, to persuade her husband to go to Moscow and sell his invention. This she managed to do, despite the fact that Worm was a rabid anti-communist.

The fourth and final step is the most dangerous. The field operative must actually approach the potential agent. As this is the vital moment, everything must be thoroughly prepared. The operative is exposing himself to the potential agent before he can be certain of the potential agent's reaction to the recruitment attempt. The danger in this situation is readily apparent, and must be minimized by all possible means.

One way to avoid exposing oneself is to hide the recruitment as a consultancy job. Many potential agents are quite prepared to sell their information as long as they believe that it is an ordinary and legitimate procedure, such as selling an article to a newspaper or a report to a company. If the readership of the newspaper is very limited, the potential agent is also flattered into giving away even more information, as he is proud of the fact that he and nobody else is chosen as information source.

One case, illustrating this, took place in Japan during the 1970s. An operative from the KGB, Stanislav Levchenko, had been ordered to recruit a successful Japanese author and political commentator working for the newspaper Yomiuri Shimbun. At first, this turned out to be difficult. The Japanese had no apparent weaknesses, and he was quite wealthy. After a thorough study, Levchenko realized that the Japanese author only had one exploitable weakness. He was vain, and enjoyed being complimented by other people, especially politicians who needed his advice.

At this time, Levchenko was working under the cover of being a journalist for Novosti. Therefore he managed to get acquainted with the Japanese author, and after a few preliminary meetings, invited him to write articles for a confidential news bulletin.

This news bulletin, Levchenko said, did not print any really secret information, but it was still considered highly informed, as many of the world's top journalists and political analysts were writing for it. The circulation of the news bulletin was very limited, he continued, only about two hundred copies, distributed to the most exclusive inner circle of the Soviet top political leadership. Naturally an impressive remuneration was

also offered for writing for this exclusive news bulletin. Furthermore, the payment was to be calculated per page of text.

The Japanese author was very flattered by the fact that he was regarded as that knowledgeable about the politics in his country. He promptly accepted the offer. As his first article turned out to reach almost fifty pages, Levchenko realized that the Japanese actually was quite interested in an extra income. Soon their cooperation increased, and Levchenko had recruited a new agent, this time without the need to risk his own position.

One point to consider is to be always friendly to the prospective agent. Always listen to him carefully. Most people want to talk about their own ideas and thoughts. This will make him appreciate you as a good listener and consequently a good friend. Do not forget to smile at him.

The location of the recruitment attempt is also very important. The potential agent's own territory, such as his house, office, or car should be avoided, as he will feel more secure there and consequently be more resistant to the recruitment.

Blackmail can be used as a recruitment technique but should generally be avoided because of the uncertainty that it will work. Furthermore, blackmail makes the agent an enemy of the field operative. This may later provoke the agent to expose the operative.

Because of this reason, it is better to be straightforward and helpful in all dealings with the agent. This will create an atmosphere of mutual trust which will ensure effective cooperation at all times. Too many agents have voluntarily surrendered to the security services of their countries simply because they were insulted by rude and arrogant field operatives.

Already recruited agents are encouraged to provide information on the service records and personal lives of their friends and colleagues. This is to assess the possibilities of further recruitments. If carried out, these subsequent recruitment attempts must not be executed by the agent himself, as a failure then would expose an already trusted agent. The agent can however try to learn how the intended agent reacts to the recruitment attempt. If the already recruited agent notices that the potential agent calls on the police or the security service, he must warn the recruiting operative at once.

Another reason why already recruited agents should not be trusted to recruit their colleagues is that the people ready to betray their own country usually are of such a low character that they are not suitable for such delicate work as is required during a recruitment attempt. Usually neither

their intelligence nor their ability to correctly judge other people's character is sufficient for this task.

One case, clearly demonstrating the significance of information received from an agent about his colleagues, took place in a European country. This case also demonstrates one of the few times blackmail can be profitably used as a recruitment technique.

A senior official within the security service of the country in question had been recruited by the KGB. At one point he reported that the security service had managed to obtain certain documents, proving that an important member of the government was deeply involved in organized crime. He was evidently mainly involved in the narcotics trade, but he also owned part of an exclusive brothel, located only a few blocks from all the government offices.

But this was not all. The agent also reported that the member of the government in question was so influential that the director of the security service did not dare or want to act against him.

But the KGB was not afraid to act. Relying on information supplied by the agent, certain KGB operatives broke into the archive in which the compromising files were kept. The files were stolen. Soon after this break-in, during a reception at the Soviet embassy, the Soviet ambassador showed the errant government member photos of the stolen documents. At the same time the ambassador assured him, that this was only a friendly gesture, so that the distinguished politician should not get any trouble and have to resign.

In this way, without any great risks and most importantly, without alienating the prospective agent, the KGB managed to recruit a valuable agent in the most influential circles of the government, able not only to supply information but also to actively shape the policies of his country.

All agents must receive some training in clandestine techniques in order to be able to recognize and elude surveillance. Furthermore, the agent must be taught which information is needed, and whether the wanted documents should be stolen, copied, or simply memorized and later reported orally.

For security reasons, the chief field operative in a large network consisting of several field operatives and agents must never expose himself to any of the agents. His own field operatives should always act as go-betweens. But the chief field operative must know all agents by sight. For that purpose he will sometimes go to the meeting place when

one of his operatives meets an agent. There he will not reveal himself but only take a good look at the agent. The chief field operative must also know the biographical data of each agent, his occupation and place of work, how he has been recruited, his accomplishments, and the degree of his reliability.

The chief field operative must also devise and memorize a special password with which he can approach the agent in case of emergency, such as the death, arrest, or defection to the enemy of the field operative normally controlling the agent.

A typical case, when this procedure saved the life of a valuable agent, took place in Hitler's Germany. At that time, one of the most valuable agents of the Soviet intelligence service was a professor in chemistry, working at the Kaiser Wilhelm institute in Berlin on behalf of the German War Ministry. The Soviets found out that the professor was secretly being followed by the Gestapo. This meant that the professor was suspected of treason. Unfortunately the ordinary operative controlling the professor was at this time hospitalized. But the agent had to be saved, and he had also to receive the order to destroy the special equipment he had received. Finally, the professor had to be persuaded to leave Germany before the Gestapo arrested him.

The Soviet Resident, that is the chief of all secret intelligence operations in Germany, was now the only one who knew the important agent. He went to the Kaiser Wilhelm institute, accompanied by a German girl, whom the Russians sometimes used for minor intelligence work. When the two arrived at the institute, they sat down, waiting for the professor to return home after work.

When the Resident recognized the professor, he and the girl first of all followed him for some distance in order to ascertain if the professor was followed by the Gestapo or not. This was not the case, so the Russian sent the girl forward. She identified herself by the secret password and told the professor about what was going on. She also handed over an envelope with a sum of money, a forged German passport, and instructions on how to escape. The German professor followed the instructions and left Germany the same evening.

But there is always the possibility that an agent for some reason will turn into a double agent and betray his controller. Therefore the field operative must always remember certain rules in his dealings with the agent. This is especially important when the two meet for handing over or

returning stolen classified documents or otherwise compromising equipment.

When meeting an agent in order to receive secret documents, or compromising material, the field operative must never accept the documents at the meeting place. Instead, he is always to walk or preferably drive away together with the agent to make sure that they are not being followed. Only then will he accept the documents.

Naturally the field operative must really satisfy himself that he is not being followed, if he detects or suspects any enemy surveillants. If so is the case, it is imperative that he knows how to evade his enemies. One operative who did not do this was the Soviet intelligence officer Valentin A. Gubichev, operating in the U.S. during the years 1946 to 1949, when he was arrested and expelled. Gubichev was employed by the United Nations.

One of Gubichev's agents was Judith Coplon, a civil servant from the Department of Justice. On the day the two were to be arrested, she met the Russian to hand over some stolen documents. At the meeting, Gubichev did suspect that he was under surveillance, so he did not dare to accept the stolen documents at once. Instead he and Coplon went on a long ride by subway and bus. Unfortunately, he still did not manage to lose the surveillants.

Finally the surveillants grew tired of the game and arrested the two. As Gubichev did not carry any stolen documents on his person, he was merely expelled. But he was still considered unsuccessful. His subway ride was of course not enough to evade his surveillants, as they too easily could follow the subway.

Also when going to a meeting to return or to deliver secret documents or compromising materiel, the field operative must never carry them on his person. Before he sets out to keep the appointment, he will give the documents to another operative with instructions to wait for him at a certain place, for instance in a restaurant, approximately five to eight kilometers away from the meeting place. Only then will he go to the meeting place. If the agent does not appear and the operative is arrested, the enemy will have no evidence against the operative, but he will know that the agent is a double agent.

If the agent does come, and the meeting place seems clear, the field operative takes a ride with the agent in order to check for any surveillance. Only when he is completely satisfied should he drive to the restaurant,

absent himself for a few minutes, pick up the documents, and deliver them to the agent.

One operative who did not take this rules seriously was the Soviet attache and lieutenant colonel of the GRU Petr Ivanovich Shiroky. He managed to get in touch with a Swedish physicist. After several meetings with the Swede, he decided that the time was ripe for a formal recruitment. Shiroky told the Swede not to call him openly. Instead they should communicate by visual signals and clandestine meetings. The Swedish physicist accepted this and also delivered several documents to the Russian, who paid handsomely.

But Shiroky did not know that the Swede already-after the initial meetings-had contacted the secret police, Säpo. The security officials had prepared all the delivered documents and also documented the meetings on video tape. Shiroky was soon expelled from Sweden.

A similar, but even more mismanaged case, took place in Moscow. The KGB had succeeded in deceiving one western military attache into recruiting a double agent. Naturally all the contacts between the military attache and his "agent" were supervised by the KGB. The military attache managed to make several mistakes. The biggest, and final, mistake was to meet the agent in a crowded bus, during the rush hours.

Inside the bus, the agent handed over a notebook to the attache, who in his turn handed over some money. But the attache did not know that the bus was literally crowded by KGB officers. They promptly arrested him. He was taken to a nearby police station, where he was asked to become a Soviet agent. The arguments ranged from threats of violence to promises of huge amounts of money. The persuasion attempt failed, however, and the attache was expelled instead.

It was certainly the act of a madman to use a crowded bus as the scene for a clandestine meeting. When trapped in a bus, there are of course no possibilities to escape or change one's mind. And, as was proved by this incident, it is easy for the enemy security service to monitor such a meeting-place. The attache had evidently remembered the advice to hide in the crowds during clandestine activities, but he had never understood that the reason for hiding in a crowd is that the operative then can disappear quietly, without anybody noticing him. In a bus, this was of course impossible.

The greatest danger in the life of a field operative often occurs when

the enemy succeeds in planting a tempting bait in the path of the operative, and the latter yields to wishful thinking and swallows the bait.

Such a bait is a potential agent, apparently excellently positioned in order to supply the information of most use to the operative. But the potential agent is planted by the security service in order to deceive the field operative into exposing himself.

It is extremely difficult to recognize a properly prepared bait, but here follows some general guidelines.

- If the potential agent is "too good to be true", then perhaps he is not true.
- If the potential agent approaches the field operative, instead of vice versa, the potential agent may be a bait. This is especially probable if he approaches the operative again, despite an initial rejection.
- An unknown agent, working only through a middle-man, must never be accepted except under exceptional circumstances. The field operative may however pretend to be interested while he tries to determine the identity of the unknown potential agent.

The last rule applies not only because of security reasons. As the authenticity and significance of information received from agents often cannot be confirmed by other intelligence sources, it is frequently necessary to evaluate the documents only by examining the degree of reliability of the source, through which the information has been obtained.

If a completely trustworthy agent, who previously has proven his value, brings a document or oral information, this information can generally be relied upon. Otherwise it is risky to trust information, not possible to confirm from other sources.

A competent security service can devote an incredible amount of work on planting a double agent in a way impossible for the foreign field operative to see through. A classical example of this occurred in France during the 1930s.

A young Russian NKVD operative, who operated in Paris with the cover of being a student from Czechoslovakia, enrolled at the University of Sorbonne for a course in anthropology. He did this mainly for improving his command of French, but also because he wanted to spot individuals suitable for later recruitment as agents.

It so happened that the operative met and made friends with a French

student, as both of them were avid billiard players. They met many times. As the French student was poor, the Russian usually paid for him too. At times, he also lent a hundred francs to the Frenchman.

The two never discussed politics, but the operative nevertheless noticed that his friend read the socialist newspaper Populaire.

Finally the Frenchman told his friend that he had to abandon his studies and find a job, as he now had to support himself and his sick, old mother. He also promised to repay the approximately eight hundred francs he owed as soon as he was able to do so. The operative assured his friend that he was in no hurry to receive his money, and promptly lent him another five hundred.

After this, the French student no longer attended the lectures. Three months later, however, the operative happened to see his old friend, as he was crossing the Avenue de l'Opéra some distance in front of the operative. The latter hurriedly followed his friend, and called out to him. Both of them were happy to meet again.

The Frenchman said that he with some help from the man who would be his future father-in-law had managed to get a position as photographer working in the Second Department of the General Staff (Deuxième Bureau, the department responsible for military intelligence). However, he said, the salary was so poor that he could never hope to get married and at the same time take care of his mother. Therefore he would try to find another, better paid job somewhere else.

The operative was overjoyed. Deuxième Bureau was the one place he definitely wanted to infiltrate. Besides, the young Frenchman was both a good friend and a socialist, so the operative was confident that he could persuade him to become an agent, especially as his economy was so bad. Finally, nothing at all indicated that the young Frenchman was a double agent. Every contact had been initiated by the operative himself, including the last one. The French student had never asked any awkward questions, such as a double agent might be expected to do.

The operative naturally checked the story of his friend. Everything seemed to be correct. His fiancee's father was an old non-commissioned officer, now employed as office manager in the War Ministry, where he had much influence. The Russian did also meet the girl, actually even financing the engagement rings. Everything seemed to be in order for a successful recruitment. The Russian prepared to make his move.

Before he had the time to do so, however, something unexpected

happened. A French police officer in the Sûreté Générale, the secret police, had previously been working for the Russians. His colleagues had never found out that he was a Soviet agent, but he had on his own initiative cut all contacts with the NKVD. But this had naturally also meant that the NKVD had ceased paying him. By chance, he now decided to resume contact with the NKVD, as he once again wanted to receive his earlier so lucrative extra income. He met his old contact, and handed over some documents. One of these documents was a secret memorandum about a Czechoslovak citizen, who in reality was a Russian NKVD operative and studied at Sorbonne. Sûreté had learnt this from an informer within the French communist party. According to the memorandum, the Sûreté had dispatched a young officer to Sorbonne in order to try to ensnare the NKVD operative.

This message soon reached the leader of the NKVD network in France. He immediately realized that the young NKVD operative in question was in danger of recruiting a double agent. A message was despatched to the operative, arriving in the last possible moment. He realized the danger of the situation and left the country in time before he was arrested. He naturally never tried to complete the recruitment of his French "friend".

The entire affair had been very skillfully prepared by the Sûreté. It is interesting to speculate how many times the French officer had actually endeavored to be seen by the operative in the weeks before they once again met on the Avenue de l'Opéra. It was naturally of the utmost importance that the Russian himself believed that he had initiated the contact.

If an agent has not yet proven himself, the intelligence headquarters must try to check every piece of information as carefully as possible. This is because some agents, greedy for money and recognition, try to falsify secret documents or invent secrets, which they claim to have uncovered. This is especially true if the agent knows that a specific fact is desperately needed to confirm the existence of a certain suspected but still not confirmed fact.

It has already been pointed out that recruitment of native agents is the most difficult and most dangerous mission in intelligence work. The most hazardous recruitment mission is to recruit agents in the enemy intelligence service.

The personnel in such an organization are themselves often trained field operatives and also, most of the time, extremely loyal to their own organization. Therefore, both the initial contact, and all subsequent meet-

ings, until the agent has proven his reliability, should be conducted in neutral or allied countries. The safest way to infiltrate an enemy intelligence service is to plant a reliable person, such as an ordinary native agent or a sleeping agent, in that organization.

Communication with a native agent within the enemy intelligence service is not always so difficult, however. In 1936, a high officer of Abwehr, the German military intelligence service, in Berlin voluntarily offered his services to the Soviet intelligence service. The reason was that he had embezzled large amounts of money and saw the Soviets as his only chance of escaping a court martial.

The information provided by the Abwehr officer turned out to be very valuable to the Soviet intelligence service. Communication with the agent was much facilitated by the fact that he worked in the "Russian" section of Abwehr. The Soviet intelligence service arranged for the German to "recruit" a female secretary at the Soviet embassy in Berlin. Every time the Abwehr officer met the Russian "agent", she produced a report of some trivial occurrences at the embassy, while he handed over rolls of film with definitely more valuable information.

It must nonetheless never be forgotten that important information can often be collected by the field operative himself without the use of formally recruited agents. Some people will be useful as informers either voluntarily or on a free-lance basis, while other people, such as journalists, often can be used as "unknowing sources", i.e. informers who do not realize that they are being questioned for intelligence purposes.

"Unknowing sources" and ordinary informers, especially free-lance informers who only work for money, must naturally never be trusted with secret information of any kind.

6

Security

Correct security measures are usually the key to successful covert field operations. Without adequate security precautions, it is quite probable that the enemy, who generally has more resources than the team of field operatives, will successfully counter the operation. Thus, maintaining security is vital not only for the personal safety of the field operatives but also for the success of the operation.

In this chapter, the security precautions normally adopted as standard procedure will be described. First, however, a few general rules.

- The operation must never be discussed in public places.
- When the operation is to be discussed (in a safe place), it is advisable always to let the water flow or to use a radio as a "sound screen" to hide the conversation from enemy bugging.
- The operation must never be discussed with persons who are not known to be completely reliable.
- If possible, the conversation should always be paraphrased in order to hide the real intentions. This means that code words and code names will be used whenever possible. An example of this is when the operatives call an enemy headquarters for example the "grocery store" and enemy operatives "colleagues". Any code word can be used but it is important that the uninitiated will not find the conversation remarkable, should he overhear it.
- A telephone or a radio communicator must never be used while discussing covert operations.
- The use of a personal car registered in the name of the field operative, either the real name or the cover name, must be avoided at all costs, as this is, due to the licence plates, the same as openly displaying the operative's name and address for everyone to see.
- If an operation must be discussed in a place where there is a risk for eavesdropping, remember that it is easier to overhear a whispered

conversation than a mumbled one. The reason for this is that it is easier to distinguish between higher tones than lower ones. For the same reason, female voices are more easily overheard than male voices.

Travels

Maintaining security during travels is usually not difficult, as long as the field operative has the right travel documents and heeds the following advice.

The field operative should always use secondary railway lines, local buses, etc., if at all possible. When travelling by train or long-distance bus, he should always board and leave at secondary stations. The main stations are more likely to be subject to enemy surveillance. Also, it is more common to check passengers on express trains than on slow trains while the train is in motion.

Air travel should be avoided as the security checks are often rigorous and the passenger's name and travel route will be registered.

If staying for the night, the operative should always try to stay with friends who are unconnected to his organization. Naturally, this only applies as long as he is not being followed by enemy operatives.

If the operative has to stay in a hotel, he must always stay in the cheapest and worst hotels he can find, if possible in a brothel. These places are unlikely to ask questions about his name and identity. If they do ask, he must try to leave as little correct information as possible.

A case, demonstrating both the advantages and the disadvantages of staying in a brothel, took place in Madrid in 1943. One of British Intelligence's Yugoslav agents, a certain Marquis Frano de Ruda from Dubrovnik, had for some time been working for the German intelligence service, Abwehr. At the same time, he had been active as a secret British agent. Now he was on his way to Britain.

However, it turned out that he had to wait for four days in Madrid while the British intelligence service MI6 prepared his new cover and new passport. This was dangerous, as Madrid at that time was literally crowded with German agents. The Marquis solved the problem by moving into the city's most well-reputed brothel. He stayed there without ever going out for the four days he had to wait.

Unfortunately, the Marquis also contracted certain diseases during his stay in the brothel. The British physicians got plenty to take care of when

he finally reached Britain. After this incident, the British always referred to the Marquis by using the code name FREAK. The Marquis survived the war, and after some time in the United States, where he bought a hotel, he retired in Italy.

The operative staying in a hotel must always check the room carefully. He must be suspicious of mirrors and furniture permanently attached to the wall, as they might be bugged or used for hiding video cameras. This kind of bugs generally use wires instead of transmitters, so they are not easily discovered.

The operative must also check the possibilities of locking the room from the inside and find a suitable escape route, if he should be attacked or confronted with enemy operatives or police during the night.

The travelling operative must always bring as little luggage as possible and keep it in his bag at all times. He must always be ready to move quickly. If he of some reason carries and uses more than one weapon, he must only clean one at a time, so that one is always available for use.

The operative must never leave secret or compromising material in the hotel room, not even when he is having breakfast in the hotel restaurant. If possible, he should hide the compromising belongings in a safe place unconnected to him. Deposit boxes in railway stations and other public places are not suitable for this purpose as they are easy to open and put under surveillance.

If the field operative carries a gun or other forbidden or compromising equipment, he must always be prepared to "lose" (hide) it if he is confronted with a sudden police checkpoint or search. Such surprising searches are especially common in occupied areas, where a street may suddenly be blocked in both ends in order to search the belongings of everybody trapped on the street. This is to detect any resistance members of guerrilla fighters.

The operative must avoid contact with other travellers and strangers. To avoid his falling into conversation, he can pretend to sleep, read a newspaper, lock himself in the lavatory, or even in extreme cases appear deaf and dumb. The drawback with the last method, however, is that such individuals are often remembered at a later time.

If in an enemy country, he must never whistle or hum tunes from his own country. During the Second World War, this led at least on one occasion to the capture of escaping prisoners-of-war.

Naturally, the operative must not use or display any foreign equipment

unavailable to the ordinary citizens in the country, such as foreign clothes and watches.

The operative must always study the customs of the country and try to follow them in order not to appear as a foreigner. Especially eating habits are important to imitate.

One example of how important this is in order to successfully infiltrate a country is a case from St. Petersburg during the years before the Russo-Japanese War of 1904-05. As the Japanese navy needed intelligence on the tactics and numbers of the Russian navy, they sent two operatives to St. Petersburg, as the Russian Admiralty was located there. The two operatives were two lieutenant commanders, Seiko Akiyoshi and Kenzo Kamamura.

The two Japanese studied the Russian language, way of life, and habits. This also included eating habits and the rituals of the Orthodox Church. After a long time of study and preparations, the two men traveled to St. Petersburg, where they managed to find employment in a shipping line, posing as Russians.

The two operatives were active for a long time. They managed to find and send to Japan many important pieces of intelligence, especially concerning the Russian navy. This turned out to be one of the reasons why the Japanese were so successful in the war against Russia. The reason for their success was that they managed to convince the Russians that they too were countrymen, despite their obviously alien appearance. People simply satisfied themselves by observing the correct behavior in all situations of the two foreign-looking men. Everybody assumed that they too were Russians. Of course, there were a few Orientals among the Russian population, but their number among the population of St. Petersburg was very small indeed.

Akiyoshi and Kamamura were later arrested, however. The probable reason was that the Russian security service had managed to crack the Japanese diplomatic cryptographical system.

If the operative is travelling by car, he should always park so that he has a fast exit from his parking space, if he must make his escape hurriedly. Furthermore, he should keep his gas tank at least half full. A spare gasoline can in the trunk is also a good precaution.

If his car has been left alone, for example during a night in a hotel, the operative must check it thoroughly for any signs of tampering before he uses the vehicle for driving. The reason is that it is nowadays very easy

either to bug or to bomb a car. Such methods are commonly used by the enemy to get rid of an exposed operative.

It is also prudent to avoid one's vehicle, if suspicious people are observed waiting in the area around it. This may mean that enemy operatives have marked the vehicle and now prepare to ambush the operative.

If genuine and correct travel documents are not available, there are still ways to travel, but the field operative must expect it to take a much longer time, compared to travel on correct travel documents.

If the field operative is able to dress, behave, and speak as a local inhabitant it is often possible to bluff his way through checkpoints.

The most interesting example of this kind of bluffing is the Jew, who escaped from Hitler's Germany by simply walking all the way while pushing a wheel-barrow. In every checkpoint, he merely said that he was working in the farm "over there" and he had left his identification at home. Nobody ever bothered to check this fact, as they could not imagine a suspect escaping with a wheel-barrow.

If travel documents are unavailable and the operative is travelling at daytime, the following rules should be adhered to.

The operative must never appear "furtive", as this arouses suspicion. Instead he must put on a bold and self-confident front.

If possible he should also obtain inconspicuous clothing and assume a definite identity, such as belonging to a definite group of people. This is most easily done by carrying a spade, a tool chest, or a similar piece of professional equipment. In this way the operative will not at once be classified as a "traveller" which often causes suspicions and draws unnecessary attention to the operative. This is especially important in war zones.

It is also important that the operative keeps clean and shave regularly. A tidy appearance assures a good treatment. It also gives the impression that the operative has a permanent residence somewhere in the area.

Bicycle or cargo train is the safest means of transportation, if there are many and frequent police checkpoints on the ordinary roads. Note that the destination of trains is often marked on the bottom left hand corner of trucks. It is however imperative to keep away from stations, as these are the places most susceptible to being watched by the enemy.

Large rivers should also be avoided, as they too will be watched, especially so in wartime.

Finally, the operative must keep away from children and dogs. Especially children have a remarkable ability to identify strangers.

If moving by night, which might be necessary in the most closely guarded areas and in areas where fighting is still prevalent, it is necessary to follow the following rules.

The operative must memorize the route, so that he does not need to use light in order to consult the map. Even a small light is visible for a long distance at night, and might betray the operative.

Roads must also be avoided. If crossing a road, the operative should locate sentries and if necessary use a diversion, such as crossing immediately after a vehicle has passed. The vehicle will create noise and light, which will temporarily blind the sentries unless they shut their eyes to the light. It does not matter whether they get blinded or shut their eyes, in any case the operative can cross the road in relative safety. When the vehicle is approaching, the operative should shut one eye, thereby retaining his night vision on that eye, while he with the other eye looks out for the vehicle and the guards.

Bridges must also be avoided as they definitely will be watched in times of war. As previously stated, this also applies for larger rivers.

In hilly areas, ridges are the most easily travelled routes. They must not be used, however, as the operative is likely to be silhouetted and seen from a long distance from below. After crossing a skyline the operative should change direction on the way along a downwards slope and check if he is detected and followed by the enemy.

At night, it is usually necessary that the operative keeps away from the local population. People usually get alarmed if strangers arrive during the night. Even if the local population is friendly to the operative, this might cause enough commotion to alert an enemy patrol.

If more than one operative are travelling together, a leading scout should always be used as far forward as possible. If the forward scout suddenly is confronted by the enemy, then at least the other operatives might escape.

The operative must avoid walking in mud, through fields of standing crops or in any other place where obvious tracks will be left. He must also avoid leaving litter or any other signs of his being in the area.

Enemy positions can usually be located by observing the area for a couple of hours. Once a position is located it is advisable to pass as near

to it as is safely possible. In this way it is possible to avoid undetected positions.

Enemy positions will nearly always be near roads, as enemy transports then can be quickly deployed by them. This will not be the case, however, if the enemy has access to helicopters. If helicopters are heard at night, expect enemy positions to be located on low ground, so that the soldiers can observe the higher areas. An alternative method is to position the soldiers on high ground, where they can observe the area by shooting flares at the areas below.

In daytime, positions are usually located on hilltops, so the soldiers are able to observe large areas. This was for example the method used by the Soviet Spetsnaz units in Afghanistan, when they tried to locate the trails used for smuggling arms into the country from Pakistan.

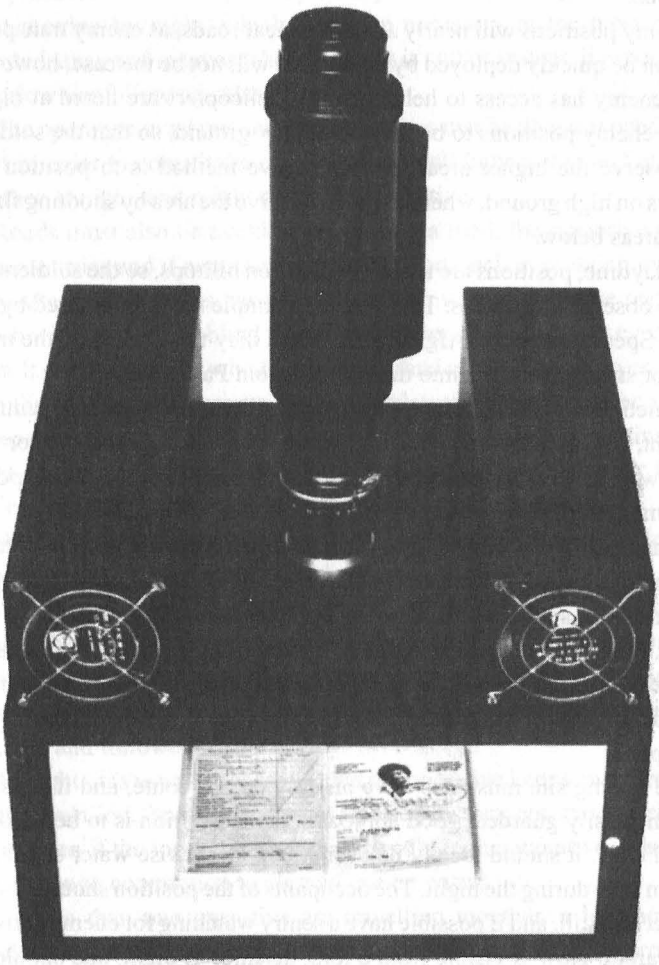
Sometimes it is necessary to imitate the silhouettes of enemy sentries. At night, this is most easily done if in particular the headgear looks correct. In this way, the operative can quickly imitate a killed or otherwise disposed of enemy guard.

If the operative needs to spend some time resting in the terrain, isolated cover such as groves and oases, must be avoided, particularly if they are marked on a map as they then are the first places in which the enemy will search. Furthermore, a thick hedge or a field of tall grass or crops is often better than small woods. The site should be concealed not only from the ground but also from the air, if the enemy has access to aircraft or helicopters.

The resting site must also have an easy escape route, and if possible only one easily guarded, good approach. If the position is to be used for several days, it should ideally be near water. Otherwise water should be taken in only during the night. The occupants of the position should always be quiet and still, and if possible have a sentry watching for enemy activity.

Cigarette glow is visible from a long distance at night, and should be avoided. Also remember that smoke is visible both by day and by night.

If only forged documents are available, the field operative must be very attentive during security checks, if the officer in charge brings his documents into another room. This usually means that he will scrutinize them carefully, perhaps with the help of a quartz-mercury-vapour lamp (the old method) or an infrared fluorescence detection system. The latter (Fig. 11) is designed to detect alterations to passports, share certificates, cheques or other security documents by differentiating between what appear on the



surface to be identically colored inks. It works by revealing the inherent differences in the intensity of the infrared fluorescence characteristics of the inks.

The suspect document is simply placed in a closed box, and spectrally controlled light is directed onto it. The operator can then easily detect the forgeries by direct observation when viewing through an image intensifier connected to the box. This will reveal all except the best forgeries.

Another method to detect alterations is to photograph the documents with infrared sensitive film. Naturally, this method requires much more time but the technique is basically the same as the one described above.

This technology can also be used for reading burned or stained letters and documents. It is therefore imperative that all important documents, when they are no longer needed, be both burned and either shredded before or at least mixed afterwards so that the burned fragments cannot be read in this way, if the enemy should find them.

Safe houses

It is necessary to maintain several safe houses in the area of operations. These are places where important meetings can be held, and where field operatives can go underground temporarily, or even permanently, if necessary. Such places are usually seldom used apartments, warehouses, private houses belonging to trusted people, and vacation cottages.

A safe house might not be used often, but the place must be checked at regular intervals to determine its continued safety and suitability. The following points must be strictly adhered to:

- There must be no enemy surveillance of any kind in the vicinity of the safe house.
- The safe house must contain food, water, and all other necessities of daily life, if an operative should need to stay there for a longer period of time.
- No compromising materiel may be kept or stored in the safe house.

As safe houses are not always in use, it is important that security is maintained by the use of visual signals. See chapter 8 for more information on this.

If the safe house is to be used for important meetings, individual buildings are unsuitable, as they can be more easily surrounded and raided

by the enemy. Row houses are more suitable for this purpose. Blocks of apartments should also be avoided for the same reason, and because they generally have only one exit point.

Hide-outs

Hide-outs are similar to safe houses, and safe houses can also be used as hide-outs. However, there is one significant difference. A hide-out is a place where the field operative can go underground for an extended period of time even if his network is partially exposed. All field operatives (not the native agents, however) in an area know the safe houses. Therefore, sooner or later the safe houses will be exposed to the enemy. This will for example be the case if an operative is arrested or turns into a double agent.

To counter this, every important field operative must find an individual hide-out, known only to him and, ideally, to the headquarters of the intelligence service (but not to his superior in the field, as he also might be arrested).

Alternatively, only the operative knows the position of his hide-out, but a communications channel is established through which the headquarters may contact him.

As a last resort, it is even possible to hide on a long-distance train. By going back and forth, avoiding the main stations, it is possible to sleep and live on the train for a considerable period of time. If the schedule is known in advance, it is even possible to arrange meetings and letter drops aboard the train. See chapter 8 for more information of the latter.

It is however not suitable to hide on trains in this way, if the surveillance of such communication lines is strict.

Clandestine meetings and counter-surveillance techniques

During operations in the field, an operative must consider every move as carefully as if he was a soldier on combat patrol duty. The only difference is that a battle usually lasts only for a short time, but the period of time in which the field operative must be alert may last for several weeks, or even years. This brings enormous psychological pressure, and the only way to live like this for a prolonged period of time is to be aware, but relaxed. A tense and nervous operative should be relieved before he breaks.

I believe that every field operative always will remember his first moment of clandestine work on enemy territory. The feeling is difficult to

describe. The tenseness is felt in the entire body. In other dangerous occupations, this might last for only a few seconds, but in the life of a field operative the feeling will remain for maybe several days. It is common that several hours must pass, before the operative again is able to relax. But at that time, the mission might not yet be over. As long as the operative remains on hostile territory, he must always be aware of every detail in his own and others' behavior. A small mistake, and he might face death or a long time in prison.

Before the field operative leaves his home, he must first of all check the street to see if his home is under surveillance. On the street, he must try to "melt into the crowds" while at the same time he must watch out for persons who might be shadowing him. As faces are usually difficult to remember, he must concentrate on clothing. This is also easier to do more inconspicuously than to watch people's faces.

The operative must not forget, however, that a skilled surveillant may change his dress, for example by switching from a coat to a jacket.

Although a good surveillance officer can appear in any guise, alone or with a family, it is always prudent to look out for individuals who do not carry anything in their hands. Plain-clothes police officers very often appear in this way, their eyes continually moving in all directions. Ordinary people, however, tend to carry bags and they usually consider it impolite to look into the face of a stranger, at least as long as he is not an obvious foreigner.

It is also good to remember that ordinary plain-clothes police officers tend to overdo their disguise, if they try to dress as criminals. This is especially true of countries, in which films are very popular. Somebody who looks like a Hollywood street crook might very well be a police officer trying to appear as one. Most criminals are dressed in fairly ordinary clothes, unless they belong to an organization which consciously try to emphasize their membership. This is for example the case with the Yakuza, the Japanese mafia, whose members often are easy to recognize due to their style of dress, often combined with tattoos.

When checking to determine whether he is being followed or not, the field operative must not turn around in a conspicuous manner. Instead, he should casually glance to the rear while crossing the street, lighting a cigarette, entering or leaving a shop, or in any other natural situation.

Also, by using public transportation systems, especially during rush

hours in big cities, he is more difficult to follow. All possibilities to shake off the enemy must be exploited.

Before a clandestine meeting, both field operatives must at all costs establish whether they are being shadowed and to make sure that they have come to their rendezvous completely "clean" and that neither of them has brought a "tail" behind himself. If one of the operatives notices that he is being shadowed, he is not permitted to keep the appointment.

When off duty, every field operative must periodically check whether he is under surveillance. This is most easily done by taking long walks or rides to secluded places where the traffic is very light and it is easy to determine whether one is being shadowed or not. This method is naturally only used to check for surveillance, not to try to shake off the enemy.

In all these situations, it must always be remembered that a surveillance team usually consists of several members and several different vehicles.

To shake off the enemy, there are several methods. The operative can for example enter a department store or a big hotel, loiter a few minutes not far from the elevators and suddenly jump into one of them seconds before it goes up. If nobody enters the elevator after him, he can be sure that no surveillant has caught up with him. Then, on one of the upper floors, he crosses to another elevator, the escalator, or the stairway, comes down, and leaves by a different exit.

This method is sometimes referred to as the "filter-method". It is especially effective in modern department stores, as they often have exits on different floors. The best case is when it is even possible to enter a subway station straight from the department store.

After a meeting, the field operative must once again check for surveillance, because he can never be completely certain that the other operative arrived at the meeting place "clean". Also, there is always the possibility that the other operative has become a double agent due to some unknown circumstances.

Sometimes, it is advisable to shadow subordinated field operatives in order to test their alertness. Sometimes this may even reveal that the subordinated operative is being followed by the enemy without his noticing it.

Such a case took place only a few years ago in Moscow. A foreign operative was approached by a Russian inside the, by Soviet standards, huge toy store Detsky Mir. The Russian claimed that he wanted to sell military secrets to a western intelligence service. The operative knew,

however, that Detsky Mir was located very close to the KGB headquarters in the old Lubyanka prison. Maybe because of this, Detsky Mir had been used several times for approaching foreign tourists and trying to implicate them in illegal activities.

For these reasons, the operative decided to be very suspicious indeed. A colleague got the mission to follow the Russian immediately after the meeting. It turned out that the Russian soon joined two other men, who had been waiting in the vicinity. Together they stepped into a car, and drove off in the direction of Lubyanka. Naturally, there was no follow-up meeting with that Russian.

When on important missions, such as going to a meeting, the field operative needs support from other operatives. First of all, it is easier to determine if the key man is being shadowed, if he is also being followed by one of his own men. This man will quickly notice if the key man is being shadowed by the enemy. If this is the case, he can sometimes cause an accident, which will involve the shadow and cause him to lose sight of the key man.

If alone, one way to determine if a suspected man or vehicle is a shadow or not is to walk or drive in a "square pattern", i.e. turning left (or right, if this alternative is chosen) four times within a short period of time. This makes the operative travel in a circle, and no ordinary man walks or drives in this way unless he is thoroughly lost.

The term "square pattern" refers to the appearance of this route on a typical city map. Unfortunately, this method also reveals to the surveillants that the operative tries to detect them.

Other common techniques for detecting and evading enemy surveillants, and how these techniques might be countered, are described in chapter 4.

Secondly, it is advisable to always use an outer security ring around the meeting place. The members of the outer security ring will be positioned some distance from the meeting place. They will observe access routes and warn of the approach of enemies either on foot or in vehicles. Known enemy buildings and garages should be watched to ascertain if more vehicles than usual are leaving. Warnings can be passed on through several methods, but telephones are the most common means of communication in this case. It must be remembered, though, to use innocent-sounding code words, so the call cannot be identified if it is monitored.

The members of the outer security ring frequently pose as road workers,

guests in restaurants, persons resting or reading newspapers in a park, lovers, or other people customarily remaining in place for longer periods of time. If possible, women and children should also be employed in this role.

In addition to this, there will be an inner security team usually armed with pistols or submachine guns. They will also observe the area through windows on the upper floor, if the building has more than one floor. Before the meeting, it is also necessary to determine escape routes and cover stories, if such are to be used instead of fighting in case of detection.

Clandestine meetings between only two persons can be held in many places, such as safe houses, hotels, restaurants, cars, offices, libraries, museums, and physicians' or dentists' offices. Many of these places are suitable for silent meetings. These are devised to eliminate the obviousness of the communication between the two participants and to deceive the surveillants.

For instance, two field operatives, apparently unknown to each other, pretend to be studying some reference literature at a library. Both, independently of each other, make notes while sitting side by side or opposite each other. Then one of them departs and, instead of picking up his own notebook, he takes that of his neighbor. The other operative calmly waits for some time, and then departs alone.

Or, while checking several books, one of them slips an envelope into a certain predesignated volume, which his neighbor retrieves a little later.

Other variants of this method can also be devised, for example when two operatives independently of each other enter a cinema and take adjacent seats, passing material to each other under the cover of darkness.

Yet another common method is for the two field operatives to independently of each other sit down on the same bench in the park. One of them brings a newspaper which he puts on the bench between himself and the other person. When nobody is around to notice it, the other man picks up the newspaper with the hidden material inside it, and walks away.

Generally, visual and audible signals are used to transfer messages of many kinds during these meetings. The most common signal is the warning signal, which warns the other operative that the meeting must be cancelled, as the signalling operative is under surveillance by the enemy.

There is one further point, which must be remarked upon, even if it appears to go without saying. When naming a place for a meeting, it is absolutely vital that both parties make sure that they have in mind the same

place, that such a place really exists, and that it will be accessible at the time of the proposed meeting.

For instance, if the meeting is scheduled to be in a hotel, it is vital to determine if there are several hotels with the same name, and if so, that the intended meeting place is clearly agreed upon.

Furthermore, it is important to choose only such places where it is highly unlikely that somebody will recognize any one of the participants of the meeting.

Professor Hugh George Hambleton of Laval University in Quebec, Canada, was for many years active as an agent for the KGB. In June 1970 he was to meet his new KGB controller, an operative known as "Paula". The meeting was scheduled to take place in Vienna, and Hambleton had received very detailed instructions on how the meeting was to be executed. The meeting point had been decided to be in a certain spot near the Danube, in the center of Vienna. Hambleton was to go there at a certain time, carrying a yellow book in his left hand. Unfortunately, when the KGB had made the plan for the meeting, they did not know that the Danube would be flooding at the time scheduled for the meeting.

Hambleton found the correct meeting place, but he also noted that the planned meeting spot was now covered by water. What was he supposed to do now? Anyway, he wanted to follow the orders to the letter. He resolutely waded out into the shallow water, despite the amazed looks of the passers-by. When he reached the correct spot, he halted, waiting for his KGB contact to show up. As he was instructed, he also held his yellow book in the prescribed manner.

A crowd soon gathered around the madman out in the water. Hambleton felt a little embarrassed, but he remained in place until he noticed that a man, standing behind the crowd, was desperately waving his hand at him. Hambleton waded ashore again, and stepped up to the man who had been waving.

The man said, exactly according to the plan, the following words:

"I have brought some etchings for you."

Hambleton, despite the fact that the crowd still was watching the remarkable couple, answered in the prescribed way.

"Thank you, I already have some from London."

Nonetheless, despite the terribly mismanaged beginning, the meeting could then proceed according to the plans. Nobody called the police,

probably because none of the spectators could imagine that real operatives ever acted in such a crazy way.

Professor Hambleton was later exposed in Canada. He was also arrested by the British, when he tried to enter Britain in 1982.

It has many times happened that two operatives planned to meet in a certain hotel, but without actually checking whether there are more than one hotel of that name in the city. One such incident took place in New York. Two Soviet GRU officers, Stern and Gorev, had planned to meet in the St. George Hotel. One of them ended up in St. George Hotel in Brooklyn, while the other ended up in St. George Hotel, Manhattan.

Another, typical incident also happened to the Soviet intelligence service. An operative was going to Paris in order to meet another operative. The meeting was scheduled to take place in Restaurant Duval on Rue Madeleine. The Soviet officer had earlier worked in Paris, and at that time he had often visited that restaurant. Now, to his astonishment, he could not find the restaurant he was looking for.

The Soviet operative turned to a police officer and asked about the Restaurant Duval. The police officer laughed, and answered that the restaurant was closed since more than one year ago, but remarkably enough, the man asking him now was actually the second tourist asking for the Restaurant Duval in less than five minutes. The police officer pointed out another man in the vicinity, who was currently standing further down the street, reading an advertisement. That's the other tourist, he said.

Naturally, the other "tourist" was the other Soviet operative.

No matter how carefully the meeting is being planned, things are bound to go wrong, if nothing else perhaps due to enemy surveillance. Therefore it is prudent to set two or three consecutive appointments at different places and times to make sure that at least one meeting will come off.

This cannot be emphasized enough. During the civil disturbances in Burma in 1988, two Burmese resistance leaders crossed the border to Thailand in order to meet a well-known opposition leader currently in Bangkok.

The two Burmese only knew a telephone number. They had planned to call up the opposition leader in Bangkok, and in this way learn further details for the meeting. Unfortunately it turned out that they had got the wrong telephone number. Instead of writing 80 as the last two digits, they had mistakenly written 18. This number only took them to a large, international company, whose switchboard operator was extremely sur-

prised when she was told that a Burmese was supposed to be employed by the company.

The two resistance leaders were desperate. How could they find the correct number? They knew only one other person in Bangkok, who would possibly know the correct number. But this person was a Thai journalist, Thaworn (fictitious name). But if they contacted him, it would be tantamount to informing the entire world that the two opposition groups now were in contact with each other. Luckily, one of the Burmese found a solution.

He checked when Thaworn would be out of his office. Then he phoned Thaworn's number. As he expected, another journalist answered the call. The Burmese introduced himself as a foreign journalist, representing a well-known news agency. Thaworn, he said, had promised him the telephone number of the Burmese opposition leader, as he wanted to record an interview with him. This had been decided two weeks earlier, he continued, when he and Thaworn had met at the border. The colleague of Thaworn quickly agreed to help the other "journalist", and he soon found the desired number among his colleague's papers.

Also, if several appointments should be missed, it is common practice to establish a "control meeting" at a certain place on a certain day, or days. There, the one who has failed to keep the previous appointments must give a sign as to whether he can be approached, and if he can, the meeting takes place.

If the operative due to some reason does not give the correct signal, it means that he is no longer able to contact his colleagues. The reason is usually that the enemy has forced him to become a double agent, but he still is reliable and therefore avoids all contact.

Bug detectors

There are several different types of electronic counter-surveillance equipment. The most common one is the counter-surveillance receiver, used for sweeping an area for transmitter bugs. The field operative might however find himself in a situation in which no such equipment is available.

Furthermore, there are also other types of bugs. While the disposable transmitter bugs can be easily detected, other types of bugs utilize wires of different kinds. They are sometimes called audio line bugs. Such bugs are often permanently installed, built into walls, ceilings, or other perma-

nent locations. These bugs are often virtually impossible to detect, except by a time-consuming search with a non-linear junction detector, i.e. a device which is able to detect non-linear junctions, such as diodes, transistors, and other solid state components found in all electronic devices including bugs. But all kinds of bugs, except the most sophisticated models, can be jammed by masking noise. This noise is of a slightly higher sound level than ordinary voices. This makes it more difficult to receive clear speech from the bug. Masking noise can be created by playing a tape-recorder or a radio, or by retiring to the bathroom and turning on all the taps.

Some models of sophisticated bug eliminators, available commercially in several countries, can generate a very wide band of electronic noise interference. This jams the transmitter bugs but not the audio line bugs. There is also special equipment available to jam hidden tape-recorders in a similar way.

As has been noted, transmitter bugs are easily detected by sophisticated bug detectors. If such specialized equipment is unavailable, transmitter bug detection can sometimes be performed with improvised equipment, as long as the transmitter is broadcasting in the right frequency range. For instance, an ordinary battery-operated FM radio receiver is able to check the frequencies in the frequency range of 88-108 Mhz. Certain parts of the UHF band may be checked by an ordinary television set. Other frequency bands may be checked if a receiver able to receive these frequencies can be found.

If improvised equipment is to be used, the operative should follow this procedure.

First of all, switch on the receiver with the volume control at a fairly high (loud) setting. Pull out the folding antenna and then very slowly sweep the tuning dial from the lowest part on the scale to the highest. If there is a transmitter bug nearby, then there will suddenly be a point where a "howl" starts to build up on the receiver, provided the set is reasonably close to the bug, i.e. within about five meters. The howling sound is caused by feedback between the microphone of the transmitter and the loudspeaker in the receiver. Now increase the volume control. The howl should become very loud, prolonged and penetrating at this one spot on the tuning dial. This is the frequency of the hidden transmitter.

To check whether this transmission emanates from a bug or not, the transmission must be compared to the noise in the room. Reduce the

volume control until the howl has just stopped, but so that there is still a slight "shushing" noise from the receiver. Clap your hands two or three times or tap with a pencil on a nearby desk. If the bug is close, the noise will be instantly heard on the set. It is easier to hear if the operative puts his ear near the loudspeaker or if he uses a headphone.

This procedure must be repeated until the bug has been found. Even if a bug has been found by this method, the check should be run several times also in other parts of the area. More than one transmitter may be hidden in the building.

If the radio receiver has a signal strength indicator, this makes it easier to tune to the critical point. Also, the sound check of pencil tapping will be heard more clearly with the help of a headphone.

The commercial models of bug detectors work in the same way. The only difference is that the operative with these models can perform a silent search, as the commercial model is fitted with a meter, indicating the presence of any bug. Naturally the commercial models are also better, as they cover a broader frequency range.

As was noted above, the UHF band can be checked with an ordinary television set. The television set is used in the same manner as the already mentioned radio receiver. The correct frequency is determined by the screen showing a pattern of dark wavy lines that move in relation to the voice of the person performing the check.

It must however be emphasized that such improvised bug detection techniques are not particularly useful for detecting contemporary transmitter bugs. The reason is that nowadays these bugs tend to operate in other frequency ranges. And what may be worse, the use of these techniques for detecting bugs is highly compromising, if the search is noticed by the enemy. If the operative is actively searching for bugs, this may confirm the enemy's suspicions. Even if a transmitter bug should be found, the howling will certainly alert the surveillant to the fact that the bug may have been detected, and he may then position a new one, operating in another frequency band.

It is therefore safer to assume that all places always are monitored, and instead use the communications techniques described in chapter 8.

Most contemporary transmitter bugs use the frequencies above 120 Mhz, as these transmitters do not require as long antennas and as these frequency ranges are less crowded by civilian traffic.

It must also be remembered that a transmitter or receiver does not

perform well when placed inside a car. The metal enclosure acts as a shield which reduces the strength of the transmitted signal. This means that a transmitter totally enclosed in a metal container is completely ineffective. This fact can sometimes be used to deceive the enemy.

For instance, it may be suspected that the enemy has concealed a transmitter in a package of secret documents delivered to an operative by a not yet exposed double agent. Then it is enough to place the package in a metal suitcase, as this will render the transmitter useless.

However, in this case the enemy might be able to use another technique. It is reported that the KGB has developed a method to cover documents with radioactive powder. It is supposed that they then can track the document by measuring the level of radiation.

Electronic surveillance can also be performed by utilizing other technologies, such as laser or infrared transmitters. These transmitters cannot be detected in ordinary ways, but they can be avoided as they require a direct line-of-sight to the target. By eliminating this, for example by using heavy curtains, these techniques are rendered ineffective.

7

Escape

A field operative must always be prepared for a situation in which he must make good his escape, either from the security service in the country in which he is operating, an enemy intelligence service, or any other group which might want to cause him harm. In all those situations, a quick escape might turn out to be the only way to avoid arrest, imprisonment, or death.

Several different escape situations will be described in this chapter. In all of them, however, the operative might be required to discard his cover and his passport, and all other documents of identification. There are certain emergency methods to produce makeshift documents of identification. They will be detailed here.

In some countries, temporary identification documents are issued to those who lose their permanent passports, travel permits, or change of residence permits. Such temporary documents are frequently typewritten affairs varying from area to area. Sometimes they are even issued by government institutions or business concerns employing the person in question. If this is the case in the country of operations, any well worded and impressively stamped document might be sufficient to fool an ordinary checkpoint.

If no photocopying machine is available, a time-consuming method of forging printed documents is to place a flat sheet of glass over the document to be copied. Then make a tracing of the lettering with some paint, preferably not black. When the tracing is dry, turn the glass over and retrace the previous tracing with a slow-drying ink or black paint. The sheet of glass can then be used to print a paper copy of the original document. Additional copies can be done by cleaning off the black paint and repeating the process.

In most cases, a photograph is also required. The main requirement is that the photograph is of the right size, appears in the correct position on the document, and carries an impressive stamp. Sometimes an official-looking signature is also required. If these conditions are fulfilled, some

discrepancies in the appearance of the operative and the man in the photograph will not cause any serious trouble.

Official-looking stamps can be made by cutting out in reverse the outline of a seal or lettering from any suitable object, such as the rubber heel of a shoe or, more easier still, a raw potato. If the operative is in possession of a genuine document, he can sometimes transfer an impression of its rubber stamp to his forged document by pressing a damp piece of paper against the genuine impression. He will then get a reversed impression which he can transfer to the forged document. It might however be necessary to touch up the stamp. Remember, though, that many real stamps are quite weak as the stamping official might have been careless when stamping.

Trains and vehicles

The techniques and methods described in this chapter are all very demanding physically, and should not be attempted unless the operative has received special training in their use. This is extremely important, as a failed attempt to use one of these methods in an escape situation certainly will lead to the capture of the operative by his pursuers.

Furthermore, the operative will probably also accidentally kill himself, or at least be seriously injured, if he attempts one of these techniques without proper training. This will naturally even more assure the success of his enemies.

If the operative is recognized by the enemy on a moving train, or if he understands that so will be the case, he is in a very dangerous situation. His enemies can easily search one compartment at a time, and if they know their business, they will not let anybody hide, for instance in the toilets. If the operative is confronted by this situation, he must endeavor to leave the train.

Of course, it is always possible to stop the train by using the emergency brake, but this brings several disadvantages. First of all, the enemy is then bound to realize that the operative has left the train at exactly this time and place. An efficient search will then be easy to arrange. Secondly, the fleeing operative will suddenly almost always find himself in the middle of the countryside, far from all means of transportation as well as all possibilities of melting into the crowd.

The last disadvantage is often impossible to avoid, unless the operative knows already before he begins his journey that the train will be searched

while in motion. The first disadvantage is however possible to avoid, as long as the operative has learned how to jump off a moving train.

With some training, starting at a slow speed such as 10 KPH, it is possible to learn how to jump off vehicles travelling at a speed of 70 KPH or more, although in a real situation the operative always strives for jumping when the train slows down. This is often the case when the railway track is curving, or just before the train has to pass a bridge.

A similar technique can also be used for jumping out of moving cars and other vehicles.

The technique used for this is performed in the following way.

The field operative must jump backwards and in the opposite direction to the way the train is moving. This means that he should step down to the lowest step below the carriage door, face toward the engine, and while still facing the engine, jump backwards.

When he hits the ground, he has to remember several important points. First of all, he must land with his legs doubled up, parachuting style. The legs should function as shock absorbers. He should also keep his teeth clenched together, so that the teeth will not get damaged by being forced together violently because of the shock when hitting the ground. He should also try to keep his balance without touching the ground with his hands, as the legs are much stronger and thereby more reliable in this situation. The hands might break or at least get hurt, if they are used as shock absorbers.

Instead, as the operative hits the ground, he should make a violent effort to "push it away" so that he once again returns to an erect posture. He should then, in the same movement, continue to run alongside the train for a few seconds, while he gradually slows down.

It is important to avoid touching the ground with one's hands. The leg muscles are the strongest muscles possible to use in this way, and they should be utilized. If the field operative loses his equilibrium, so that he needs to use his hands to regain it, there is a serious risk that he will upset the rapid rhythm of his leg movements, necessary for succeeding in running alongside the train for a few moments. This may cause him to fall.

Another common situation nowadays is that the field operative is recognized or pursued by his enemies while driving a car. Such a situation makes heavy demands upon both the driving skill of the operative and the performance characteristics of his vehicle.

If the field operative can choose a car for his mission, he must try to

find one with powerful performance characteristics. But very often he has to accept whatever he can find. This is not so bad after all, as most cars can be used in emergency situations.

The only cars which are completely unsuitable, and therefore should be avoided if at all possible, are jeeps and similar types of vehicles. The reason is that they have a tendency to tip over during turns if driving at high speed. Of course, jeeps and similar vehicles are excellent for going off the roads, so this alternative should be chosen rather than trying to outspeed the enemy, if the operative finds himself driving a jeep pursued by the enemy.

The ideal vehicle is one that is both powerful, easy to handle, and above all else, reliable. A European car, such as a Volvo, Saab, or Mercedes-Benz is often the best choice. The oversized American cars should definitely be avoided.

East European cars are not very often reliable, but in those countries they are often the only choice, unless the operative really wants to advertise his movements. Converted police cars always have good characteristics, however, and this also holds true of Soviet cars.

As the car often must be used for surveillance purposes, obviously foreign, extraordinarily expensive, and otherwise exotic cars should be avoided as they stand out too much on an ordinary street. Furthermore, the licence number should preferably not be easily memorized, as this may alert the target to the fact that he has seen the car before. The best option is usually to rent a car, preferably in a fictitious name.

Several modifications to an ordinary car are possible if an attack is expected. Here follows a list of the most useful ones. Several of these features are actually in common use, except in the most inferior cars.

The best possible radial tires should be used as they offer increased durability, as well as increase the handling characteristics. They also decrease the fuel consumption to some degree. Radial tires are also to some extent bullet resistant. All four tires should be slightly overinflated (2.8 kg/cm2) and filled with run flat foam, as this will allow continued driving for some distance even after the tire is punctured.

A heavy duty radiator allows hard driving in hot weather, and on inferior roads, without overheating the engine. Heavy duty shocks and springs will also improve the handling of the car.

Brake lines of the type used in competitions are much superior to ordinary ones, and might be installed to raise the efficiency of the brakes.

The steering system must be of the highest quality. If the steering system is not of the same high quality as the rest of the car, its handling characteristics will be decreased considerably.

If the car uses old-fashioned headlights, they should be replaced by modern ones, as modern headlights sometimes give off twice the light compared to the old types. This enables the driver to drive much faster at night.

Additional lights may also be mounted. In that case, they should be mounted low and angled slightly outward.

A reliable alarm system should also be installed, as this will not only protect against theft but also obstruct tampering. This might render it more difficult for the enemy to for instance bug the vehicle, or bomb it. It must however be remembered that no car alarm system is totally reliable.

A locking gas cap is naturally a necessity, as this prevents or at least makes it more difficult for the enemy to put explosives in the gas tank.

All the above-mentioned features are inconspicuous and not strange in an ordinary car. The following features should also be considered, but they may draw attention to the vehicle and should therefore only be added to the vehicle if the situation so allows. A few of the modifications mentioned below are impossible to use in almost any situation, as they immediately would draw the attention to the car in a most unfavorable way.

It is for example possible to mount four or five high intensity spotlights high on the vehicle. These can be used for temporarily blinding an attacker. Three of the spotlights should be directed to the front, one aiming straight ahead and the other two angled slightly outward. The remaining one or two should be aimed to the rear.

Switches enabling the driver to independently control each light on his vehicle should be installed. The addition or elimination of various lights at night will alter the appearance of the car, which may help to lose a pursuer or fool the person the operative is tailing.

The dome light in the car should also be disconnected, so the operative can enter and exit the car without the enemy noticing it.

It is of course also possible to armor the vehicle. But there are several disadvantages in doing so. Adding armor to a vehicle will increase both the cost and the weight of the vehicle to an extraordinary degree. The increased weight will also decrease the handling characteristics of the car. Furthermore, no armor is completely reliable. Especially the glass can only be made bullet resistant, not bullet proof.

A simpler solution, and also often a more efficient one, is to affix a 12.5mm thick aluminium plate to the back of each seat. In a pursuit situation, this will at least offer protection against most submachine gun and pistol rounds. A car is not supposed to be used as a tank, so this is often sufficient.

A heavy iron bolt put through the tailpipe and welded into place will prevent a bomb from being placed in the exhaust system. But it must not be forgotten that it is easy to put bombs also in other parts of or beneath the vehicle.

Some kind of communications equipment is always useful, if the operative is not acting totally on his own. A radio or cellular telephone is most commonly used for this purpose.

A heavy duty battery is sometimes required if additional lights or communication equipment will be added to the car.

Either wide angled or electronically controlled mirrors will allow the driver to see what is going on behind him without turning his head. As such behavior might reveal his noticing a surveillant, such extra equipment is sometimes useful.

If the operative is pursued by the enemy, and this is really not a common situation unless both the operative and his enemies act clumsily, then various modifications can be used to lose one's pursuers. For instance, a smokescreen pump can be used. This system works by pumping for instance castor oil into the hot exhaust manifold of the vehicle.

Another possibility is to install a device which sprays oil onto the road behind one's vehicle. This is an unexpected way of forcing the enemy to lose control over his vehicle.

Another method is to throw caltrops behind one's car. These are metal spikes constructed so that one point is always up. Caltrops, especially if used in massive quantities, might flatten the tires of pursuing vehicles. Caltrops have been used in warfare for more than two thousand years and are still effective today.

The front bumpers can be reinforced by welding or bolting extra supports from the vehicle frame to the bumper. Further reinforcement can be made by welding a 5 cm thick metal pipe to the vehicle frame, right in back of the bumper. Such extra reinforcements are useful if ramming ever becomes necessary.

Naturally, a first aid or a survival kit should be in every vehicle. If the situation allows it, a gun is also a good addition.

In some cases, kidnappers have been known to throw the victim into the trunk of his own car. If that may happen to the field operative, he should keep a crowbar and preferably also a weapon in his trunk, so that he can escape from such a situation. This might be the case in certain countries, but as the field operative generally is active against an enemy security service, this precaution is not much useful and may backfire, if the enemy searches his car.

If the field operative will operate in an area where he will be expected to often travel by car, he should prepare himself by learning how to handle the car if he is directly confronted by the enemy. The confrontation may be of any type, such as an assassination attempt, an attack which develops into a chase, or an attempt to stop the operative for either arresting or killing him. The different situations, which might occur, will be detailed below.

If the operative finds himself in a chase situation, which by the way is the result of the failure of the enemy to properly implement what they might have planned, one of the most important techniques is how to handle corners.

The vital point about taking a turn in a car is that the speed at which you exit the corner is more important than the speed at which you take the corner itself. Assuming that both the operative and his enemy drive identical cars, the car which exits the corner at the greater speed will be going faster on any straight stretch of road that follows after the turn.

The apex of any turn is that point at which the wheels of the car are closest to the inside edge of the corner. By choosing a relatively late apex, the driver can exit a corner at a greater speed than if he had chosen an early one.

One of the most common types of turn, particularly in urban areas, is the 90-degree turn. This turn is begun as far outside (i.e. away from the curb) as possible. Obviously, if there is a lot of traffic on the road, the driver must adjust his turn accordingly. In that case, he should drive as far to the outside as he can within the confines of his lane.

When approaching the corner, the operative should gradually increase braking pressure. He must be careful not to lock the brakes, as all this does is prevent him from steering. If he feels any of the wheels locking up, the operative must immediately let off the brakes for an instant, and then reapply them.

After downshifting the gear, he must gradually release the brakes into

the first third of the turn. Then the operative should gradually increase the throttle to full acceleration, reaching it upon exiting the turn.

The 90-degree turn is analyzed in Fig. 13.

- Gradually increase braking pressure.
- Shift into low gear, and gradually release the brakes.
- After releasing the brakes, gradually increase acceleration.
- Full acceleration at apex. Shift into high gear.

The turn depicted above is supposed to take place in a country practicing right-hand traffic. But it is naturally necessary to adjust the turn if there is any traffic coming in the opposing lane.

An S-type turn need not be a turn at all if there is only light traffic on the road. If possible, the field operative should go straight through it and take full advantage of any straight that might follow (Fig. 14).

The constant radius turn, or "hairpin" turn, is handled in a way similar to the 90-degree turn. It is however prudent to remember not to go too fast, as this turn may easily let the careless driver end up off the road.

The constant radius turn is analyzed in Fig. 15.

- Gradually increase braking pressure.
- Shift into low gear, and gradually release the brakes.
- After releasing the brakes, gradually increase acceleration.
- Full acceleration at apex. Shift into high gear.

This turn, too, as it is depicted above is naturally supposed to take place in a country practicing right-hand traffic. But in the same way as was noted above, it is necessary to adjust the turn if there is any traffic coming in the opposing lane.

There are however two important disadvantages by taking a late apex in a corner. If the driver is not familiar with the road on which he is driving, it is difficult to prepare for the optimal apex, as he may not know what the turn looks like until he is already in it.

Furthermore, if he is pursued, and if the pursuing vehicle takes an early apex while he takes a late one, there is a small chance that the pursuer will actually catch him in the turn, as the pursuer in fact gets through the corner quicker than him. The pursuer will not be going as fast after the turn, however, but then the damage is already done.

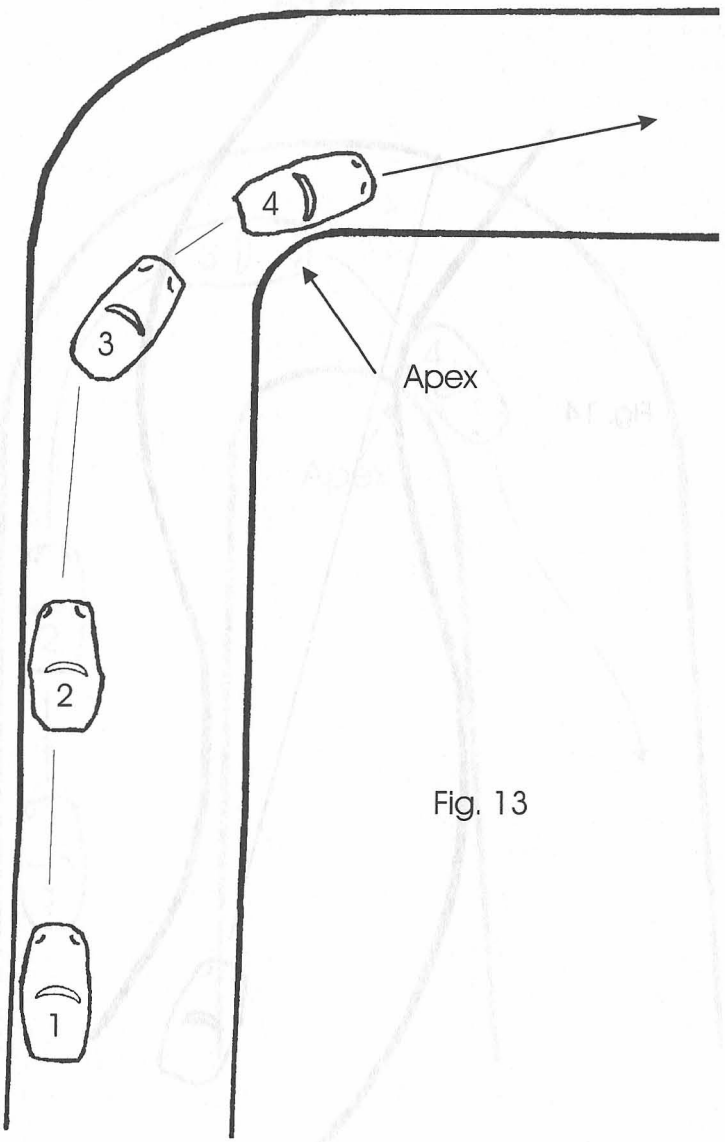


Fig. 13

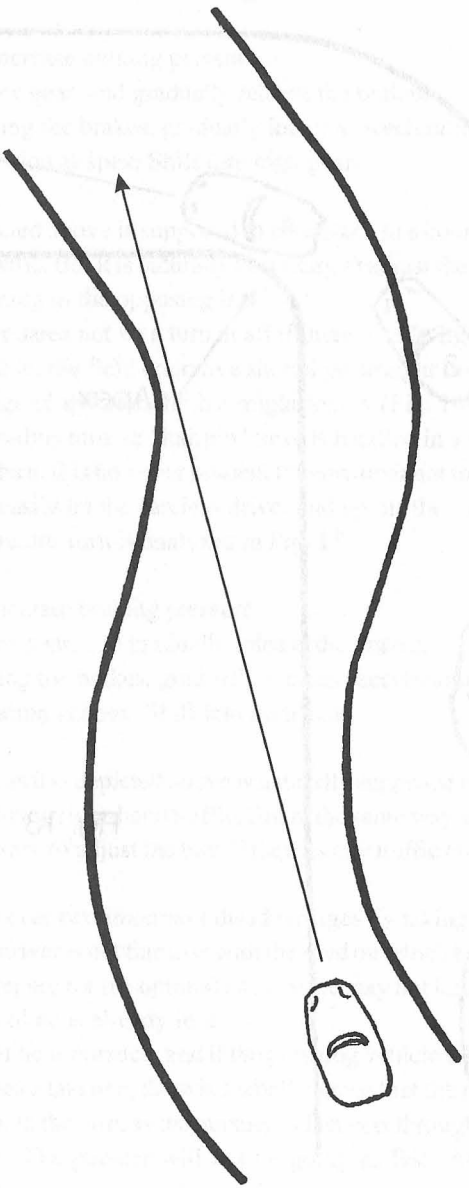
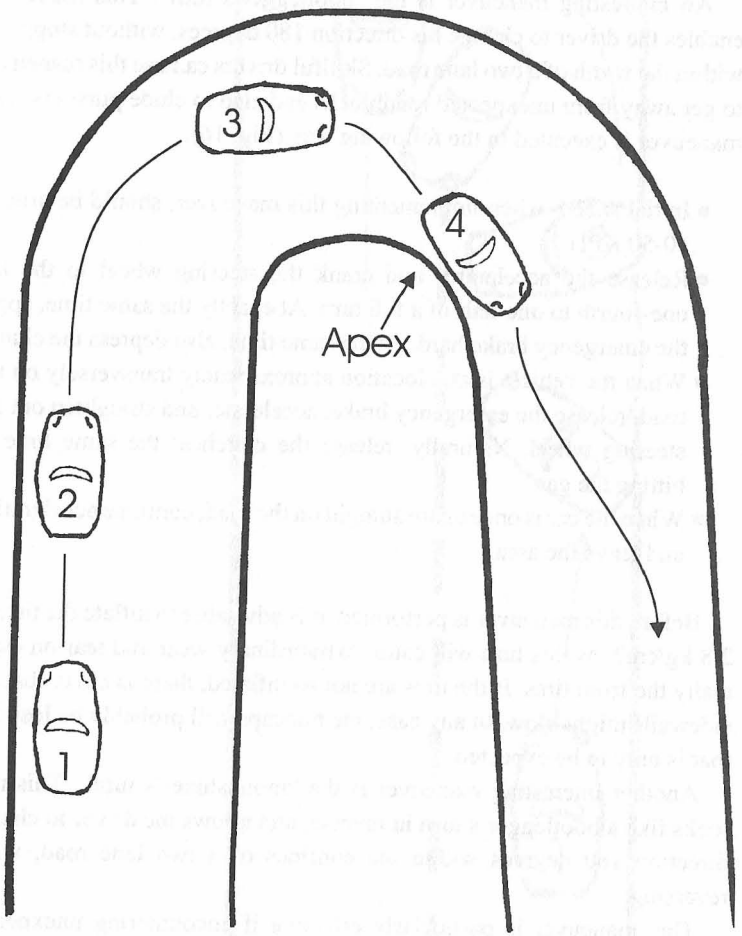


Fig. 14

Fig 15



This means that if the operative is in a superior car to that of his pursuer and if he has a big enough lead on him, at least a couple of car lengths, it is usually worthwhile to take the turn by taking a late apex.

However, if the operative is in an inferior car or a pursuer is right behind him, it is extremely important not to let the pursuer pull up alongside one's own vehicle. By taking an early apex, the operative as a consequence prevents him from doing so.

An interesting maneuver is the "bootlegger's turn". This maneuver enables the driver to change his direction 180 degrees, without stopping, within the width of a two lane road. Skillful drivers can use this maneuver to get away from unexpected roadblocks and also to elude pursuers. The maneuver is executed in the following way (Fig. 16).

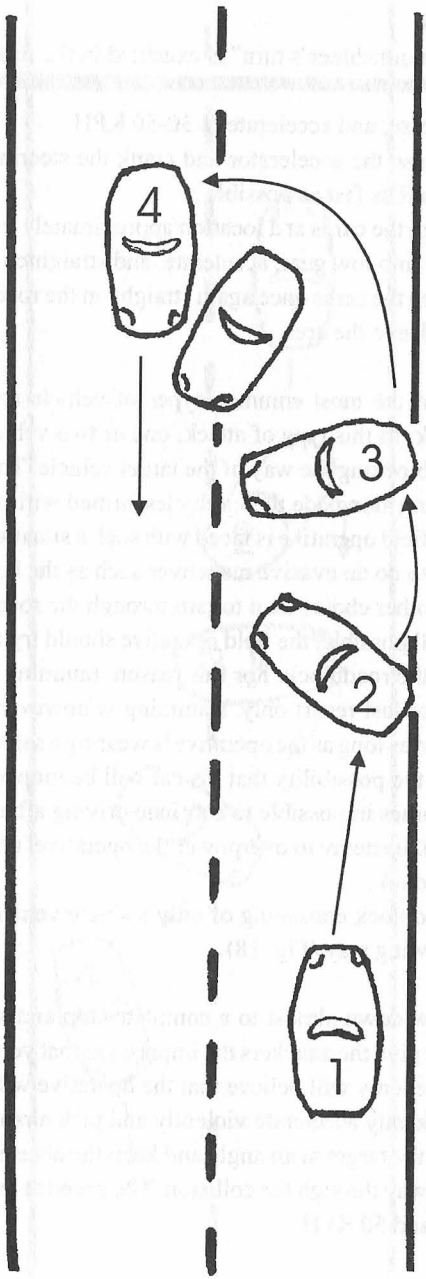
- Initial speed, when implementing this maneuver, should be around 40-50 KPH.
- Release the accelerator and crank the steering wheel to the left one-fourth to one-half of a full turn. At exactly the same time, apply the emergency brake hard. At the same time, also depress the clutch.
- When the vehicle is at a location approximately transversely on the road, release the emergency brake, accelerate, and straighten out the steering wheel. Naturally, release the clutch at the same time as hitting the gas.
- When the car is once again straight on the road, continue accelerating and leave the area.

Before this maneuver is performed, it is advisable to inflate the tires to 2.8 kg/cm2, as this turn will cause extraordinary wear and tear on especially the front tires. If the tires are not so inflated, there is a risk that the sidewalls might blow. In any case, the hubcaps will probably be lost, but that is only to be expected.

Another interesting maneuver is the "moonshiner's turn". This turn looks like a bootlegger's turn in reverse, and allows the driver to change direction 180 degrees within the confines of a two lane road, while reversing.

This maneuver is particularly effective if encountering unexpected roadblocks at night. Often the attackers manning the roadblock will use high-intensity spotlights to blind the victim as he approaches. By using

Fig 16



this turn, the victim can hurriedly direct his field of vision away from the spotlights.

The "moonshiner's turn" is executed in the following way (Fig. 17).

- Reverse, and accelerate to 30-50 KPH.
- Release the accelerator and crank the steering wheel all the way to the left as fast as possible.
- When the car is at a location approximately transversely on the road, shift into low gear, accelerate, and straighten out the steering wheel.
- When the car is once again straight on the road, continue accelerating and leave the area.

One of the most common types of vehicle ambush is the stationary roadblock. In this type of attack, one or two vehicles are lined up across the road blocking the way of the target vehicle. The attackers will usually be standing alongside their vehicles, armed with automatic weapons.

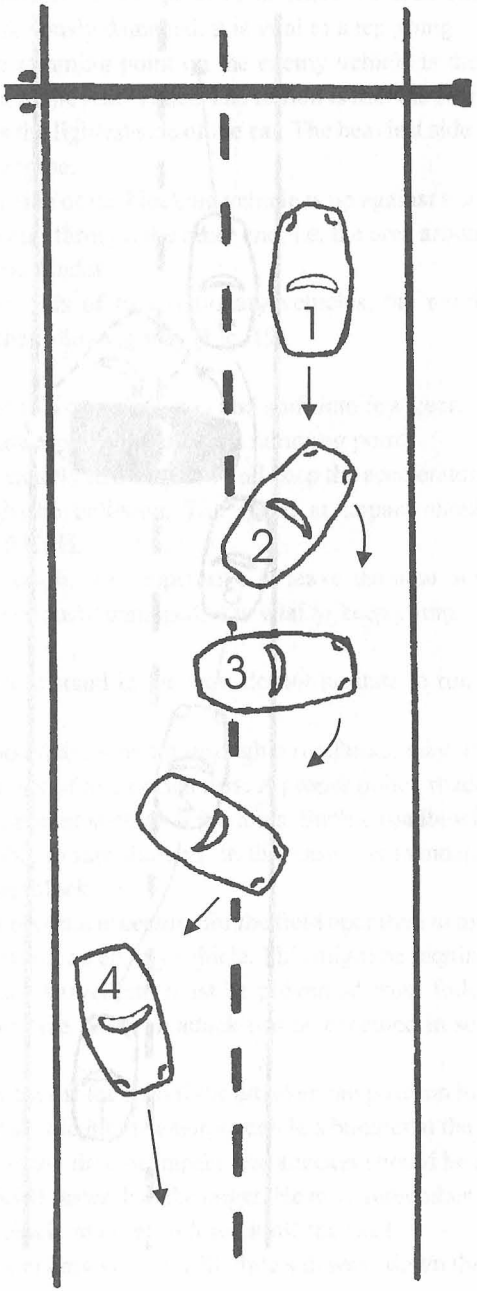
If the field operative is faced with such a situation, and he does not have the time to do an evasive maneuver such as the bootlegger's turn, he will have no other choice than to ram through the roadblock.

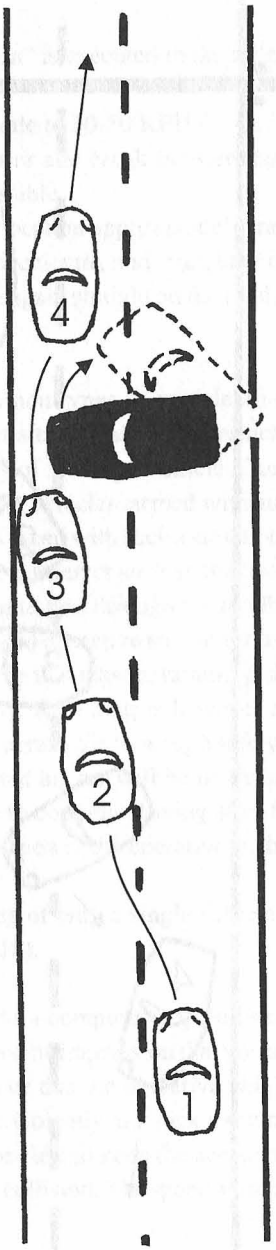
If at all possible, the field operative should try to go around rather than through the roadblock. For this reason, ramming should be considered a method of last resort only. Ramming is however not so dangerous as it may seem as long as the operative is wearing a safety belt. The main danger is rather the possibility that his car will be inoperable after the collision. If it becomes impossible to continue driving after the collision, it will be easy for the enemy to overpower the operative, as he then literally will be a sitting duck.

A roadblock consisting of only a single vehicle should be rammed in the following way (Fig. 18).

- Slow down almost to a complete stop and shift into low gear. This will give the attackers the impression that you are going to stop. Thus, the enemy will believe that the operative will be an easy target.
- Suddenly accelerate violently and pick a ramming point.
- Hit the target at an angle and keep the accelerator fully depressed all the way through the collision. The speed at impact should be between 25 and 50 KPH.

Fig 17




4
3
2
1

- After breaking through, it is imperative to leave the area quickly. Even if the car is seriously damaged, it is vital to keep going.

The most favorable ramming point on the enemy vehicle is the area around the rear wheel and the rear fender. The reason is that the rear side, in most types of cars, is the lightest side of the car. The heaviest side is the one incorporating the engine.

However, if the rear side of the blocking vehicle is up against a curb or wall, it is necessary to ram through the other end, i.e. the area around the front wheel and the front fender.

If the roadblock consists of two stationary vehicles, the roadblock should be rammed in the following way (Fig. 19).

- Slow down almost to a complete stop and shift into low gear.
- Suddenly accelerate violently and pick a ramming point.
- Hit the roadblock exactly in the middle and keep the accelerator fully depressed through the collision. The speed at impact should be between 25 and 50 KPH.
- After breaking through, it is imperative to leave the area quickly. Even if the car is seriously damaged, it is vital to keep going.

If any attackers should stand in the way, do not hesitate to run them over.

It must be understood that ramming through a roadblock may work if the blockade only consists of one or two cars. A proper police roadblock frequently utilizes equipment such as spike mats. Such a roadblock will definitely not be possible to ram through. In this case it is mandatory to try to go around the roadblock.

Sometimes it might become necessary for the field operative to himself take the initiative and attack an enemy vehicle. This might be required for instance when an enemy surveillant must be prevented from following another, important operative. Such an attack can be executed in several, different ways.

It is easy to knock a car off the road if the attacker can position himself behind it. The attacker should hit the enemy vehicle's bumper at the angle illustrated in Fig. 20. At the time of impact, the attacker should be going approximately 15-30 KPH faster than the target. He must remember to hit, not push, the enemy vehicle in order to force it off the road.

After the impact, the enemy vehicle will glide sideways down the road

Fig 19

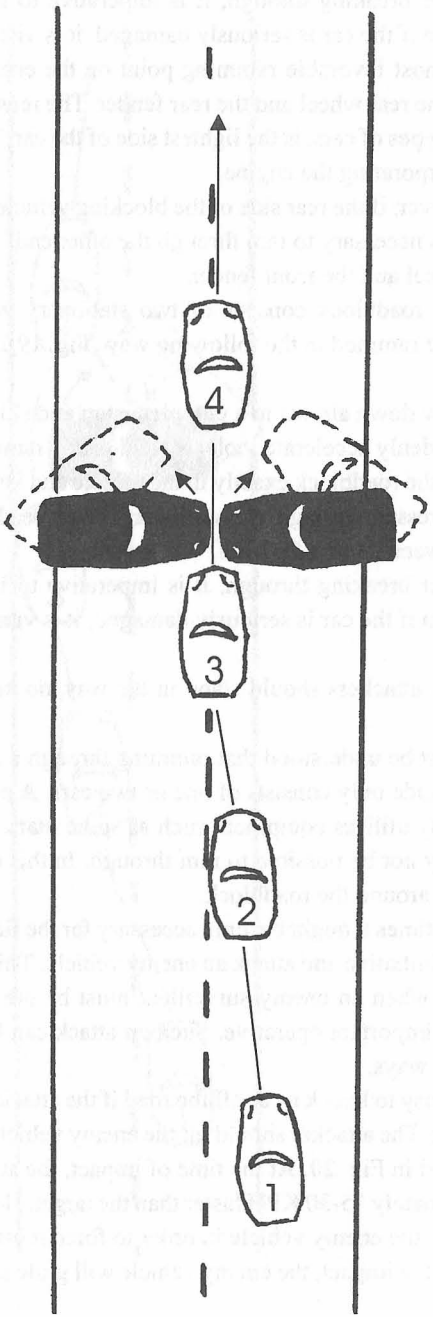
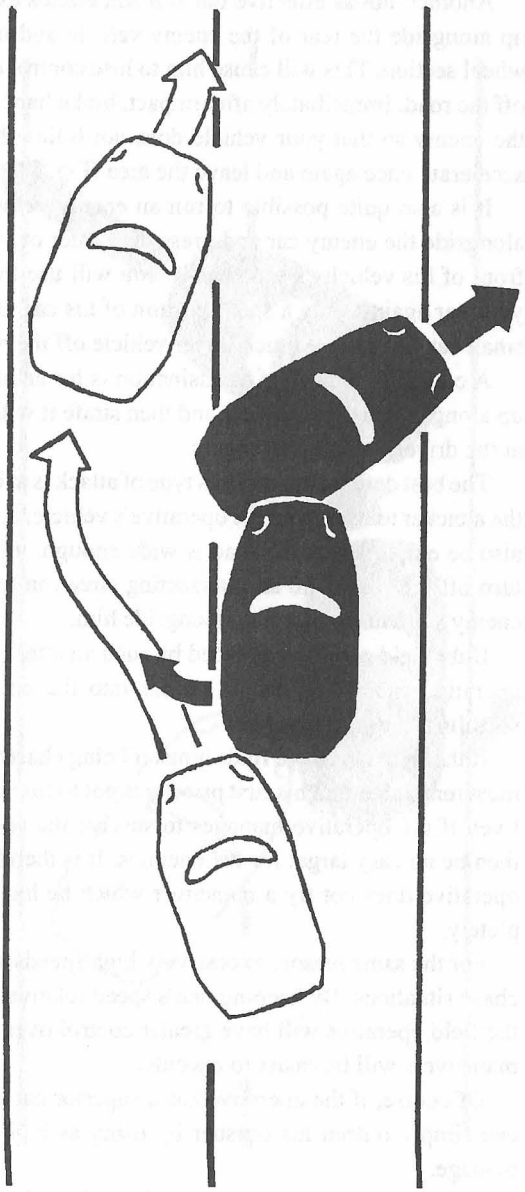


Fig 20



until its tires regain traction. When this happens, the enemy car will move in the direction its wheels are pointing, i.e. off the road.

Another, not as effective but still sometimes useful method, is to pull up alongside the rear of the enemy vehicle and then crash into his rear wheel section. This will cause him to lose control over his vehicle and go off the road. Immediately after impact, brake hard and break contact with the enemy so that your vehicle does not follow him off the road. Then accelerate once again and leave the area (Fig. 21).

It is also quite possible to run an enemy vehicle off the road. Drive alongside the enemy car and press the center of your vehicle against the front of his vehicle. By doing so, you will use the total body weight of your car against only a small portion of his car. By using this method, a small car can force a much larger vehicle off the road (Fig. 22).

A common method of assassination is for an attacking vehicle to pull up alongside the victim's car and then strafe it with automatic fire, aimed at the driver and the passengers.

The best defense against this type of attack is to brake violently, causing the attacker to overshoot the operative's vehicle. A bootlegger's turn could also be employed, if the road is wide enough, or he could make a quick turn off the road, into an intersecting street, in the same moment as the enemy vehicle is pulling up alongside him.

If the field operative is faced by such an attack from a motorcycle, the operative can simply crash his car into the enemy, killing or at least disabling him in this way.

If the field operative finds himself being chased by enemy vehicles, he must remember that his first priority is not to lose control over his vehicle. Even if the operative manages to survive the resulting crash, he would then be an easy target for his enemies. It is therefore imperative that the operative does not try a maneuver which he has not yet mastered completely.

For the same reason, excessively high speeds are not recommended in chase situations. By keeping one's speed relatively low, below 100 KPH, the field operative will have greater control over his vehicle and evasive maneuvers will be easier to execute.

Of course, if the operative has a superior car and the road is good, he can simply outrun his pursuer by using as high a speed as his car can manage.

If an enemy vehicle tries to pull up alongside the operative's car, the

Fig 21

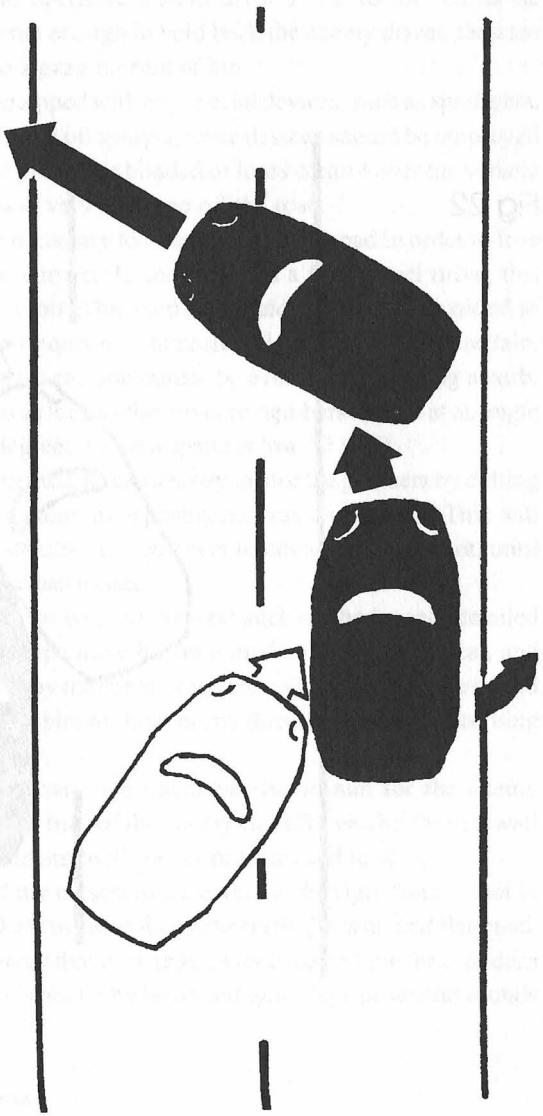
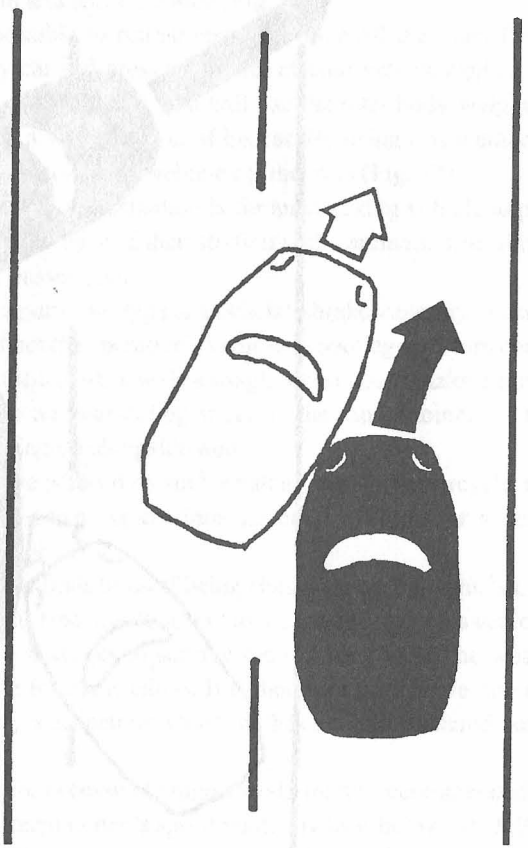


Fig 22



enemy is either going to shoot or try to run the operative off the road. Both these alternatives must naturally be avoided at all cost. As it is likely that the enemy will try to overtake on the left side (in a country practicing right-hand traffic), the operative should drive as far to the left as he possibly can. If this is not enough to hold back the enemy driver, then the operative should try to zigzag in front of him.

If one's vehicle is equipped with any special devices, such as spotlights, a smokescreen pump, or an oil sprayer, these devices should be employed just before turns. If the pursuer is blinded or loses control over his vehicle just before a turn, he will very likely go off the road.

At times, it may be necessary to oneself go off the road in order to lose a determined and able pursuer. If one's car has a four-wheel drive, this may be used as a last resort. This method should however be avoided as there is a great risk that the operative himself will get stuck in rough terrain.

A roadblock in a street can sometimes be avoided by jumping a curb. A curb is easily jumped as long as the driver remembers to hit it at an angle of approximately 45 degrees and at a speed below 70 KPH.

If the operative is pursued, he can also try to lose the pursuers by cutting just in front of traffic coming in opposing lanes in a crossroad. This will make it almost impossible for the pursuers to continue the pursuit, until after all opposing traffic has passed.

Other methods can also be used. Several such methods were detailed in chapter 4. If the field operative has an armed colleague in his car, and he expects to be attacked by the enemy, then the colleague should be seated in the back, as this allows him to shoot in any direction without disturbing the driver.

If a gunfight is necessary, the operative should aim for the enemy vehicle driver or the front tires of the enemy car. If he can hit the sidewall of one of the tires, the enemy will sooner or later need to stop.

Especially the front tire closest to the curb, i.e. the right front wheel in right-hand traffic, is likely to cause the car to crash if it is hit and flattened. It should however be noted that it sometimes takes some time for a modern radial tire to flatten if it is not hit by heavy shotgun slugs or several rounds at the same time.

Dog evasion techniques

The dog has been used in warfare for thousands of years. The evasion techniques employed to counter guard and tracker dogs have changed very

little. Nowadays it is possible to produce chemicals to help evading dogs but such means are not always reliable. If chemicals of this type are available, they should be used in addition to the following techniques and not as a replacement.

Sometimes it is possible to use make-shift "chemicals" such as crushed, strongly smelling cigars, or gasoline, kerosene, or oil. Especially the last three products are fairly efficient as the dogs do not like the smell of them. Fugitives have been known to escape by walking through areas polluted in this way. Some gasoline put on the soles of your shoes may help to evade the dog.

The dog relies very little on sight during ordinary activities. Its attention is however drawn by movement and if the dog's interest is roused in this way, it will follow up with its most important senses, namely hearing and smell.

At night the dog is able to detect movement mainly due to its low position, looking up at the skyline.

The dog's hearing is very good, and it will be attracted by noise not heard by its handler. This can be partially countered by approaching from down wind. As the wind carries both sound and smell, this is also good for avoiding being detected by the dog's smell.

The dog's sense of smell is excellent and it is able to detect a source of scent either by following air currents or tracks left on the ground.

The main smell of the human body is made up of body odor produced by the sweat glands. This particular odor is increased by quick movement, tension and nervousness, various types of food, and bad personal hygiene. Another source of smell comes from clothing (especially leather, for instance shoes), deodorants, and chemicals such as gasoline.

It therefore follows that in many respects it is possible to control one's flow of body scent. If chemicals are avoided, it is possible to lessen the scent by keeping cool, calm, and clean.

Ground scent, the scent remaining in the tracks of a person, which is used by tracker dogs, is more difficult to control, however.

It is made up of both body scent, and scents from other sources such as crushed vegetation and insects, as well as gas and moisture allowed to escape by the breaking of the surface by the weight of the man on the ground. An experienced tracker dog can follow this scent up to forty-eight hours after the track has been made in untouched, humid terrain.

The dog can also find the direction of the track, as the toe part of the

impression is deeper, and remains in contact slightly longer. Even if the fugitive tries to fool his pursuers by walking backwards, it is possible to track him as then the heel part of the impression will be deeper. In any case the dog will detect it.

The dog has an excellent sense of smell, but there are many factors which affect scent, and consequently a dog's scenting capabilities. The efficiency of the dog can therefore to a great extent be influenced by the fugitive, if he has a good knowledge of the factors influencing the dog's sense of smell.

The dog's sense of smell is increased if the ground is moist, such as if by dew, light rains, mist, or fog. Humidity also facilitate tracking for the dog. Still, stagnant water, such as in swamps and bogs, also simplify matters for the dog, as humidity and moisture of all sorts retain a scent for long periods of time.

In order to simplify for the dog, the terrain should consist of forest areas or other areas covered by vegetation, such as grass, or fern. Light winds are acceptable, but stronger winds are not, as the scent will then be dispersed more quickly.

If the quarry is slow moving, this also facilitates for the dog. This is even more true if the quarry consists of a number of persons on the move, or if the fugitive is carrying a heavy burden, or if he is nervous and has excessive perspiration.

But there are also many unfavorable factors for the dog. If for instance the ground is arid, lacks vegetation, is covered by metalled surfaces, sand, or stone, or is crisscrossed by animal scents and tracks, the situation for the dog will be much more difficult.

Factory areas, workshops, and pollution, also from motors, disturb the scenting abilities of the dog. The dog's nose is also irritated by dry terrain and dust.

Other terrain characteristics which also diminish the scenting abilities of the dog are recently ploughed ground, as the ground scent then is lost or weakened (but remember that footprints on newly ploughed ground will be easier for the handler to notice), ice, snow, and water obstacles of all kinds. Strong winds, preferably of gale force, will also reduce the tracker dog's efficiency to a great extent.

Finally, the fact that the quarry is continually changing direction and otherwise taking evasive steps may result in the dog hesitating so often that the handler loses confidence in his dog. This may convince him to

abandon the search, despite the fact that the dog unknown to him is on the right track after all.

The following advice will help the field operative attempting to evade tracker dogs.

Before any contact is made with the enemy, it is important to associate oneself as much as possible with the surroundings. This can be managed by spending time among grass or trees, especially those with a strong smell. It is also necessary to avoid all artificial scents, such as deodorants, perfumes, and other chemicals.

The operative should also endeavor to travel only over ground already used by humans or animals.

If several operatives are travelling in a group, they should split up every now and then in order to join at a predetermined meeting-point. This needs to be done for only a short distance, but will be sufficient to slow the dog down, as it must first of all identify all the new tracks.

If food is to be prepared, the operative must take care as to the direction of smoke and fumes. Litter should be handled as little as possible, and buried without touching the ground. When digging, metal instruments should be used instead of one's hands. If possible, the litter should be sunk in deep water, for example in a lake or river.

If the operative stays some time in one place, he should make false trails around the perimeter of his position. He should also enter and leave the position from different directions, so that he does not create a path.

If the operative travels along animal tracks, he should follow to the side of them so as to avoid leaving footprints.

If, despite all these precautions, the trackers manage to make contact visually from a distance or locate the track of the fleeing operative, he must think of the following advice.

He must endeavor to cover as much distance as possible in a short time in order to tire the dog and undermine the handler's confidence.

If a group of operatives are travelling together, they should immediately split up and arrange a later rendezvous at a predetermined spot, proceeding there by different routes.

The operative should also endeavor to follow a route across varied surfaces and types of terrain. If possible, metalled surfaces, or areas covered by rocks or concrete, should be crossed and recrossed at intervals.

The operative should also pass through fields which contain, or have

contained, animals. In this way the dog will have to keep track of many varied scents, not only the scent of the fleeing operative.

If travelling through woods, bush, or scrub, the operative should change direction frequently. This will cause the handler problems, as the dog is usually on a line. The line may get entangled, and in any case the dog and its handler will have to slow down, if forced to change directions at several times.

If there are any streams in the vicinity, the operative should cross them several times. The best way is to walk along the stream for a short distance and make a few false exit and entry points. As long as the dog finds a track, however short, on the other side of the stream, the dog handler will often wrongly assume that the fugitive has crossed the stream at that point. Therefore, the fugitive operative should prepare a false trail on the opposite side of the stream while in fact he returns out into the stream and follows it for a short distance, after which he returns to the original side.

Walking too far in water is to be avoided, however, as this will slow down the operative's own progress too much.

If the operative can do so without exposing himself to increased risks, he should make a number of false trails, enter villages, follow roads, and in every way try to mix his own tracks with others. Of course, while doing so, his own progress may not be further endangered or slowed down.

If, despite all these attempts, the enemy is in close contact, i.e. the dog is in position to be released and able to attack, it is important that he takes the following safety measures.

First of all, he must get out of sight of the handler, so that he does not release the dog.

Then, if possible, he must immediately change direction. He should also use metalled roads, stone and rocks, or rough surfaces whenever possible to make it harder for the dog.

It is also an advantage if the operative can run through for instance a herd of animals. Climbing over fences and other obstacles will also slow down the dog.

In order to confuse the dog, the operative can discard articles of clothing, food, or any strongly-smelling object. If chemicals of the type mentioned above are available, they should be used at this stage.

If the dog is let loose, the operative must endeavor to part the handler from the dog. If the dog catches up with the operative, he must try to kill

it silently, so that he does not reveal himself to the handler and the other enemies hunting for him.

The ***guard dog*** is trained differently from a tracker dog. It is trained to attack and detain an intruder, trying to enter the guarded area. Guard dogs are operated in one of two different ways. Either it operates with a handler on leash, or else it is roaming free in a compound.

The guard dog will in any case rely primarily on its hearing and scenting abilities to detect any intruders. The dog's sight will be used only as an auxiliary sense, as the dog will mainly be attracted by movement in its field of vision. Stationary objects or persons might not be detected by the dog's sight.

The guard dog will attack and retain its grip on its quarry until ordered to leave. This simplemindedness makes it extremely vulnerable to the intruder, who can counter the guard dog in the following way.

The intruder must first pad himself by wrapping some kind of protection, such as a belt, heavy canvas or cloth, or a similar material, around his arm. He should also always have a layer of softer material inside as well as outside his main protection. The inner layer is to absorb some of the pressure of the dog's jaws, while the outer layer is to give the dog something to grip on.

When the dog is approaching, the intruder should present his arm as a target to the dog. The dog will recognize this as a situation similar to its training. Therefore, the dog expects to succeed in attacking the target. When the dog has gripped the arm, it will not release its grip until so ordered. In this way its only weapon, as well as its ability to sound the alarm, will be lost, and the intruder is free to kill the dog, silently if necessary.

In many countries the dog is trained to not even touch the intruder, as long as he is not moving and apparently surrendering. This will make the dog even more vulnerable, as it then will be an easy target for an intruder, for instance armed with a silenced pistol.

The dog must be allowed to make firm contact on the first run in. If it fails, falls off, or is prevented from attacking, it will look for an alternate target. This will destroy the intruder's initial advantage, and a deterred dog will also bark or growl, thereby drawing the attention of the guards.

There might also be dogs trained to kill and not only restrain an intruder. These dogs are however very rare, as the handler himself runs a risk when training his dogs. Therefore, there is no reason to expect this kind of dogs

in any installation, except possibly in the worst prisons of the most oppressive dictatorships.

The silent killing of a trained dog is however by no means a simple matter. It is sometimes easier to immobilize the dog by either tying it to a strong object, or binding its front legs. The dog must always be muzzled. When the dog is immobilized in one of these ways, it can be killed if this is required.

Actual killing may be performed in any of the following ways. Either the operative can stab it through the abdomen, aiming from rear to front, or he can deal a severe blow to the dog's skull. Yet another method is to chop at the back of its neck just before the shoulders.

If it is not necessary to kill the dog silently, the easiest way is to shoot the dog through its skull, aiming above, and in the center of a line drawn diagonally from ear to eye. Another alternative is to shoot the dog through its back and spine.

The best solution is generally to use a silenced pistol. One example of a successful use of such weapons was the Soviet Spetsnaz units during the war in Afghanistan. These soldiers were often armed with silenced pistols. Those weapons were however not used for assassinating famous Mujahideen leaders, as many foreign observers believed, but for silently and efficiently eliminating the many wild dogs always prowling about the Afghan villages and camps.

When killing a dog, it must be remembered that the dog's skeletal system is such that a considerable physical strength must be brought to bear in order to kill it. It is advisable to aim for the soft spots, such as the abdomen, or the point beneath the chin but above the breast bone.

Sometimes it is not necessary to kill the dog. Several intelligence services, among them the CIA, have been known to use dog repellant gas to turn a dog away from an intruder or fugitive. This gas, a Freon-derivative of very low temperature, will cause the dog's eyes to burn, thus temporarily stunning and frightening the animal. The dog repellant gas is loaded into an atomizer, and the spray is aimed into the dog's face, when it is charging the operative.

Tear gas has also sometimes been used for the same purpose, but is not really efficient, as the dog is highly likely to continue its attack despite the gas.

Of course, another means of disposing of dogs, especially guard dogs, is to feed them poisoned meat, either lethal or non-lethal. Tranquilizer

darts, of the same type as used in zoological gardens and scientific research, can also sometimes be used for drugging guard dogs. In this case it is however necessary to remember that the drug requires some time before it will work, thus putting the dog asleep. If the dog is merely put asleep, it is sometimes possible to evade discovery altogether, as the dog will wake up later, thus obliterating the evidence of the intrusion.

To avoid detection when entering an installation guarded by dogs, these rules should be followed.

First of all, the operative must always approach from down wind. Naturally, he must be as silent as possible. As dogs have a very good sense of hearing, he should also keep all garments and pieces of equipment securely fastened in order not to create any unnecessary noise, caused by the different objects rubbing against each other.

The field operative should also proceed slowly in order to lessen his excretion of sweat, and thereby body odor. If it is necessary to stop for any reason before entering the perimeter, he should do so well outside the 200 meter mark, as dogs may detect intruders within this distance by their smell only.

The operative should also keep as low as possible and use all natural hollows in the terrain, as the air scent in this case will be obstructed by undergrowth or physical barriers from spreading over larger distances. If the dog is very close, however, it might be better to try to pass it along a higher terrain feature. This is because the average guard dog will have difficulty in detecting a person located on a higher point than they are themselves. Even if they do detect the intruder, they have difficulties in pinpointing his location. This delay may give the operative enough time to execute his mission.

As this also means that the scent may be obstructed by barriers in the form of buildings, the field operative must be aware of changes in scent direction caused by for instance open gates or the empty space between buildings. Even if he so far has not been detected by the dogs, they may do so when he passes in front of an open gate.

It is always safest to approach the dogs from an area where the operative knows other humans to operate in, or approach from. The dog pays less attention to areas where it expects there to be persons or vehicles. Even if the dog is actually attracted, its handler may misinterpret the situation and remain inattentive.

When within the perimeter fence, remember that the dog relies mainly

on sound and scent, but its attention will be drawn also by movement. If the field operative is in a position down wind and the dog is passing, he must keep still. Guard dogs have been known to pass within 10 meters of a hidden man without being attracted.

Search dogs, are trained to more or less independently quarter an area, searching for a fugitive with only a minimum of commands from its handler. On location of an intruder, the search dog is to bark, or return and collect the handler and the patrol naturally supporting the dog handler. A dog of this type relies mainly on locating the source of airborne scent.

If the field operative is confronted by such a dog, when hiding in a fixed position, it is therefore necessary to observe the following rules.

To avoid spreading airborne scent, the operative should keep as close to the ground as possible at all times. If at all possible, he should stay in a depression in the ground.

The field operative should also cover himself by his clothes, allowing the earth to absorb the scent from his body. Furthermore, he should only breath down into the ground, or at least into the undergrowth. Naturally, he must also remain still and silent.

If the operative is burying items, he should do so underneath himself, so that all smells are kept down by body and the clothes he is covering himself with.

Smoking and fires must of course be severely restricted, and usually not allowed at all.

As the search dog is more inclined to circle and bark, or collect the handler, instead of attacking at once, it is necessary to depart immediately after the dog has found the operative. Normal evasion techniques should be used. If escape is not possible at once, the dog must be killed.

When dealing with any type of dog, it must be remembered that the dog is relying on commands from its handler. These commands may be voice, whistle, or hand signal. Sometimes a combination of all these methods will be used. The signals may not be continuous, or obvious, but they are always necessary for controlling the dog.

It is this fact, that the dog relies on the human, that creates an advantage for the evader. If the dog and its handler are parted from each other, the dog will begin to lose confidence. If the dog's surroundings are changed, its sense of security will be immediately weakened. Both these factors can be used to evade a dog.

Therefore, the field operative must always aim to do three different things if he is confronted by a dog. He must destroy the confidence of the handler in his dog. He must also destroy the confidence of the dog in its handler. Finally he must destroy both the dog's and the handler's confidence in themselves and their ability to find the fugitive operative. If the operative succeeds in all this, he will also succeed in evading the dogs.

Escape from handcuffs

Handcuffs are not made for keeping a person prisoner for extended periods of time. They are only supposed to hold the prisoner during transportation to jail. This means that the lock is not very complicated, and picking it is fairly easy even with improvised tools. Often there is not even any need to actually pick the lock, as other methods can be just as effective.

The locks which secure each side on a pair of handcuff always open with the same key, as the mechanism is identical in both of them. Furthermore, the key is usually the same in all handcuffs made by that specific manufacturer. This is not really helpful, however, as there are still many hundreds of types of handcuffs, all with different keys.

Despite this, handcuffs are fairly simple to open, as the lock mechanism is less complicated then for example in a padlock. A padlock will only open when all the levers are lifted to specific but different heights. The handcuff lock, however, will open when only one or in some cases two levers are lifted to the same height. Compared to most other types of contemporary locks, the locks in handcuffs are really very old-fashioned.

Almost all handcuff locks have only one lever. A minority of them have two levers. The only exception to this general rule are a few types of handcuffs fitted with pin tumbler arrangements as locking mechanisms.

The most common type of handcuff in use today is the swing-through handcuff (Fig. 23). This type of handcuff is adjustable to fit any size of wrist. The shackle, or bow as it is generally called, is capable of swinging through the locking mechanism any number of times, as long as there is no wrist to stop it. Movement backwards is impossible, however, as a ratchet will prevent it. This will keep the prisoner in the handcuffs. An advantage of this type of handcuffs is that the mechanism is unable to accidentally lock, as long as there is no wrist in position. This makes it easier for police officers and other professionals who need to apply the handcuffs quickly in a stressed situation.

One way of breaking loose from this type of handcuffs is simply to smash them on the floor or with any heavy object. The captured operative must be certain to only hit the points marked in Fig. 24. By doing so, it might be possible to make the ratchet jump all the teeth in the bow, one at a time, until the operative is no longer held by the handcuffs.

Another way of opening this type of handcuffs is to use the method sometimes called shimming. A flat sliver of plastic, steel, or any other hard material is inserted into the handcuff, between the bow and the ratchet. This will lift the teeth of the bow out from the ratchet, thereby enabling the prisoner to escape (Fig. 25).

As this is a fairly common method of escaping, some handcuffs of this type are fitted with a device, intended to stop any shimming attempts. This device is actually only a small projection at the point in the handcuff case where the prisoner is likely to insert his probe. The projection is intended to deflect the sliver used by the prisoner away from the teeth.

This safety measure is quite easy to defeat, however. Simply push the bow inwards. Be careful not to push it a full notch, as this will make the handcuff more tight around your wrist, and accomplish nothing. The bow should instead only be pushed slightly inwards, as this will enable the sliver to be inserted at the same time. The sliver must be inserted at exactly the same time, as insertion is only possible when the ratchet teeth are slightly raised, thus allowing the sliver to avoid the projection and slide in between the teeth.

By this process the handcuff can be pulled open, but only if the sliver is kept moving. Otherwise the captured operative must restart the entire process.

Some types of handcuffs with pin tumbler locks can also be opened by shimming in this way.

It should be noted that some better types of handcuffs are fitted with a double locking mechanism. This will be further explained below. Handcuffs fitted with this mechanism cannot be shimmed open, as long as the double lock is really locked. As will be explained below, this is not always the case, so it might nevertheless be worth a try.

The swing through handcuffs can also be opened by applying force. This is actually true of all types of handcuffs. If the weakest point can be found, it can often be used for breaking the handcuffs, either through prying open the rivets or sometimes splitting up the entire handcuff case.

Any suitable object found in the location where the captured operative

Fig 23

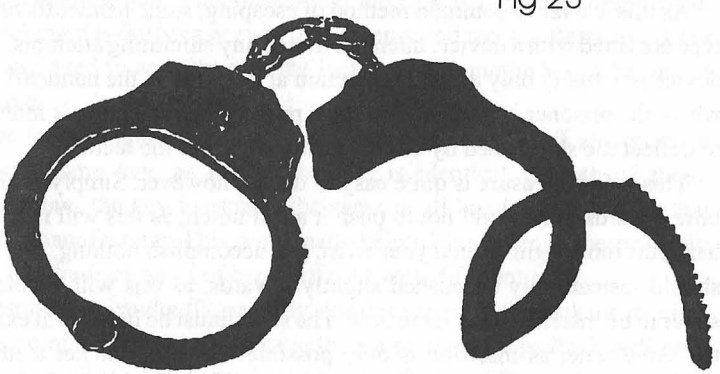


Fig 24

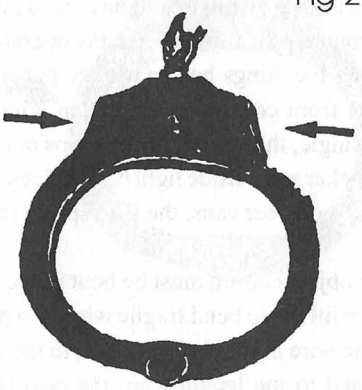
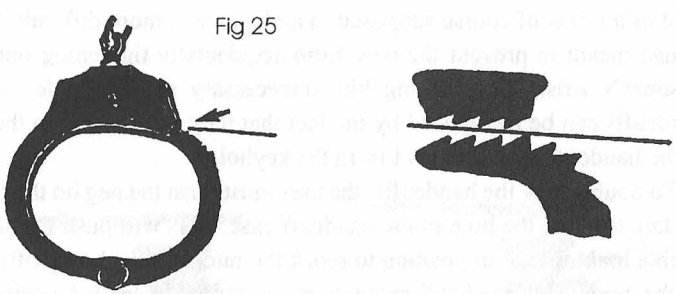


Fig 25



is kept can be used for this purpose. This object, for instance the edge of a central heating radiator, is forced between the two halves of the handcuff case. Then the case can be split into two by a powerful twisting motion (Fig. 26).

If the captured operative is unable to force the handcuffs open in any of the ways described above, he might still be able to pick the lock. A pick can be improvised from almost any object in the operative's possession or in his vicinity. Among the things he can use are paper clips, pin needles and safety pins, wire from coat hangers, garden wire, electric cables if composed of only a single, thick wire, pocket clips or coiled springs from ballpoint pens, the thicker wire inside light bulbs, electric switches, ladies' hair pins, ring pull tabs on beer cans, the flint spring in cigarette lighters, and so on.

The wire or other object chosen must be bent in the correct shape. The operative must be careful not to bend fragile wires too many times, as they might then break. The wire is simply bent once, to the correct length. The length should be equal to the length from the post (the part the key is supposed to turn on) to the lowest part of the keyhole. The bent part of the pick is then inserted into the lock, and turned around to open it. Most locks open if the pick is turned clockwise (Fig. 27).

An alternative method is to simply push any thin wire, such as the metal or plastic end of one's shoelace, into the lock. If pushed upwards, or slightly upwards to the right, there is a good chance that the ratchet will be engaged and simply lifted out of the bow, which then will be released.

As was mentioned above, some better handcuffs also have a double locking mechanism. The double locking mechanism fulfills two purposes. First of all, it is of course supposed to make escape more difficult. But it is also meant to prevent the bow from accidentally tightening onto the prisoner's wrist, thus causing him unnecessary pain. Double locking handcuffs can be recognized by the fact that they have a hole in the side of the handcuff case, different from the keyhole.

To double lock the handcuffs, the user must push the peg on the end of his key through the hole in the handcuff case. This will push the sliding double locking bolt in position to block the ratchet from being lifted out of the bow. The handcuff mechanism in a double locked position is illustrated in Fig. 28.

This mechanism can be picked by inserting the pick, or any piece of wire, into the lock, and then push (upwards and to the right) the double

Fig 26

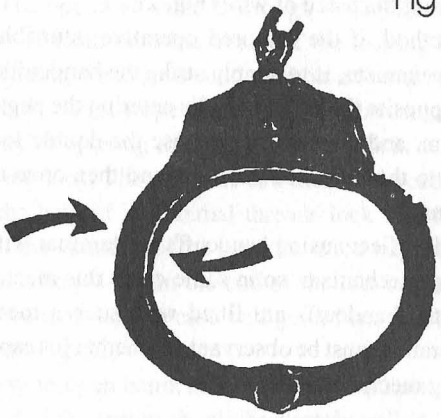
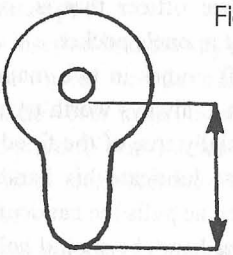


Fig 27



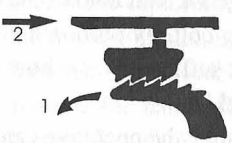


Fig 28

Fig 29

locking bolt away from the ratchet. When the ratchet is free to be lifted, it may be so by using the piece of wire (Fig. 29).

Yet another method, if the captured operative is unable to pick the double locking mechanism, is to simply strike the handcuffs to the left of the keyhole, i.e. opposite the small hole for entering the peg of the double locking mechanism, and thereby try to cause the double lock bolt to fly back to the right, to the unlocked position, and then open the handcuffs by any other means.

Actually, not all officers using handcuffs are familiar with how to use the double locking mechanism, so in some cases this mechanism can be ignored, even if the handcuffs are fitted with such a mechanism. The captured field operative must be observant of whether his captors are using the double locking mechanism or not.

The other main type of handcuffs is the British type (Fig. 30). This type of handcuffs is different from the previously described. A disadvantage with this type, for the police officer that is, is that this type might accidentally lock, while kept in one's pocket.

As this type of handcuffs comes in two main types, either with an adjustable or a fixed bow, it is always worth trying to slip the handcuff over the hand. This is especially true of the fixed bow type. First of all, the escaping operative must lubricate his hands with soap, washing detergent, grease, or oil. Then he pulls the handcuff down as far as he can onto the hand. With his other hand, he should hold on to the base of the thumb and the back of the hand, pressing them firmly together. This is very painful, but can make the hand into about the same size as the wrist. The handcuff can then be slipped over the hand.

This type of handcuffs can also sometimes be opened by the use of a piece of string, or shoelace. The operative must form a slip knot, and then pass this into the round keyhole, and onto the locking bolt as far as possible into the mechanism, onto the threads. Then he should carefully pull until the slip knot tightens. If the slip knot then gets a firm hold of the threads, then it is possible to draw back the locking bolt, by pulling hard on the string. When the locking bolt is drawn back sufficiently, the bow will fall out, permitting the prisoner to escape (Fig. 31).

If no piece of string or shoelace is available, the operative can tear off a piece of his clothing. Either nylon or ordinary cloth will do, as ordinary cloth can be slightly strengthened by wetting it. The strip should be

approximately one centimeter wide, and a small hole should be ripped in the end of it. The operative should, through the hole in the piece of cloth, push the piece of cloth onto the treads of the locking bolt. He can then fasten it by winding the strip around the bolt a few times. Finally he can pull back the bolt, thereby opening the lock in the same way as above.

Another way of opening this type of handcuffs is to insert a ballpoint pen case into the lock. The pen case can then be forced onto the locking bolt, and by the help of its internal threads lock into the threads of the locking bolt. If the diameter of the pen case is too large, then a small piece of cloth can first be placed on the end of the locking bolt. This piece of cloth will ensure that the pen case will get a firm grip on the threads on the locking bolt (Fig. 32).

The best way to open handcuffs of this type is however to use a steel spring. One end of the spring should be slightly pulled out, for using as a hand-hold. The spring should be long enough to allow a new coil to be pulled out and used in this way, if the old one becomes too bent or weakened by repeated attempts.

The spring is simply inserted into the keyhole, and twisted around the locking bolt in the same way as was described above (Fig. 33). Spring steel, if not too big, will however fasten more securely onto the threads, and also allow the operative to pull harder without risking the spring breaking. Such accidents are very common if only for instance cloth is available for this purpose.

Steel springs of the correct size can sometimes be found in the most unexpected places, for instance in electric motor starters, car engines, chairs, door closers, and garden furniture.

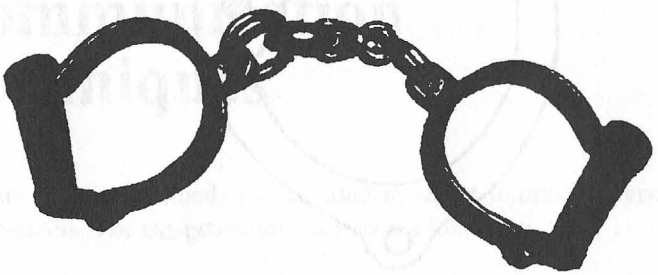
If none of the methods described above is able to help the operative to break free from his handcuffs, then he might be able to use the handcuffs as a pretext for attacking his guard.

As many types of handcuffs might accidentally tighten on the prisoner's wrists, there are guards that will loosen them up on demand from their captive. If the captured operative complains that the handcuffs are too tight, and before this unnoticeably moves the handcuff around in order to make the wrist appear red, he might be lucky enough to convince the guard to remove the handcuffs in order to loosen them. This can be a suitable moment for attacking the guard.

The operative must of course never himself tighten the handcuffs too much, as many guards then would refuse to help him. He should also be

fairly certain of his ability to overpower the guard, or else be in a truly desperate situation, warranting any attempts to escape.

Fig 30



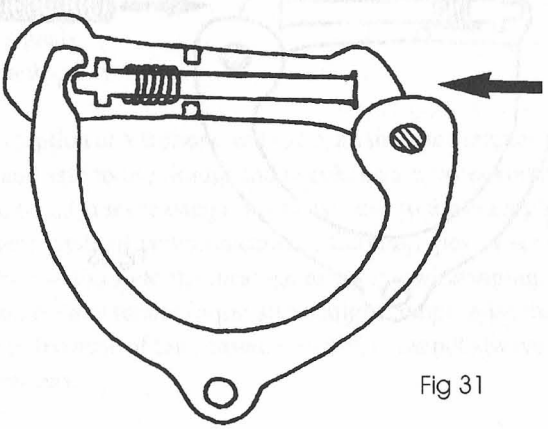


Fig 31

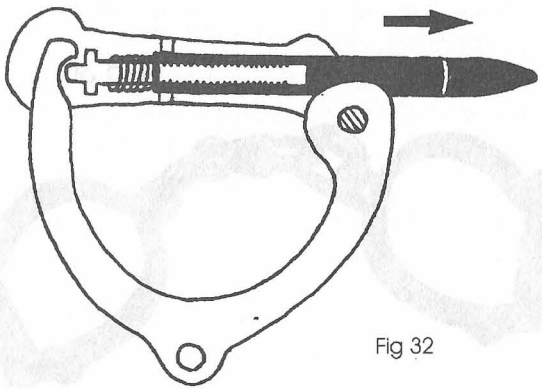


Fig 32

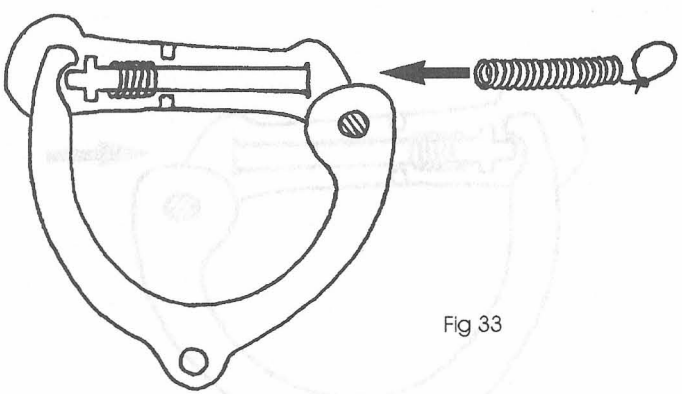


Fig 33

8

Reporting Systems And Communication Techniques

Many different methods can be used to report information and to receive orders. The most common ones are the following.

- Letter drops
- Couriers
- Civilian postal and telegraph systems
- Telephone
- Radio
- Pigeons

Certain orders and especially warning signals are frequently received by the use of:

- Visual signals
- Audible signals
- Cryptographical systems

With the exception of telephone and radio, all these techniques are very old, reliable, and safe to use. Radio and telephone are faster communications systems, but also more dangerous to use, due to the enemy's ability to monitor these types of communications. Certain types of scrambling systems can be used to hide the message to enemy wiretapping, but the very possession of such scrambling systems might compromise the operative using them. Because of this reason, scramblers cannot always be used in covert operations.

Letter drops

By using letter drops, it is possible to communicate without the sender and the receiver knowing the identity of each other, or even meeting each other. This system can be summarized in the following way.

- Coded messages take the place of personal meetings.
- Hiding places, "letter drops", are used instead of mailing addresses. Drops can for instance be a hollow in a tree, a deep crack in the wall of a building, or any other hiding place.
- A special system of "indicators" is used to orient each agent as to the specific hiding place where a message is awaiting him and where he should deposit his reports. The "indicator" consists of a number, or preferably a symbol or code word, written on an easily located object, such as a wall, a park bench, or inside a public telephone booth.
- Every operative appears on certain days, at a certain hour at a public telephone, where he is called up by his superior and given necessary instructions.

Thus, according to this plan, the operative takes a walk in the city, looks up the number or identification of the hiding place marked on a certain wall, then goes to the hiding place and, if he is not under surveillance, picks up the message, deposits his report, and later returns to wipe off the number of the hiding place on the wall and replace it with a prearranged symbol or phrase to show that he has picked up the message.

If large pieces or amounts of equipment or money must be supplied to the operative, they are cached in another place and the operative receives a message on where to find them.

This system works fairly well, but there is always the risk that some other person will find the drop, or that some accident (for instance weather, animals, etc.) will expose the message. Therefore, this system, if applied in its entirety, must be used with extreme caution. Its most obvious uses are in a wartime situation when the lives of the operatives depend on total security. In other situations, the letter drop system should also be utilized, but a certain flexibility must be built into the system.

Whatever the circumstances, the letter drops must always be chosen with the utmost attention and care, so that the chance of exposure by other people or accidents is minimized.

An example of what might happen when everything goes wrong took

place in the United States. A Soviet operative arrived at a letter drop to receive a message, only to find that the message had been dragged out from its hiding place by a squirrel. Now the message was fully visible for anyone to see. This operative was lucky, however, as nobody had found the message and read it. But of course, this letter drop was never used again.

An agent who is not completely trusted must be dealt with in the following way. He must not be told the location of the letter drop until after the message or equipment is already in place. Even if he then informs the enemy, they will have no possibility of catching the field operative when he comes to put the message in the letter drop.

Another important security measure is to always position the letter drops far away from prisons, railway stations, important military-controlled factories and industries, and government or diplomatic districts, as there generally is more police activity in these places and consequently a higher chance of being noticed.

Couriers

Couriers constitute another important means of communication. They are divided into two types. Tactical couriers are used for the internal communication in a small area, while operational couriers are used for maintaining contact between different agent networks or, more often, between a field operative and the intelligence service headquarters.

Couriers must have a legitimate reason to travel around, so as to not cause suspicions. Therefore, tactical couriers often assume covers such as salesmen, postmen, errand boys, chauffeurs, and taxi drivers. Operational couriers usually assume covers such as businessmen, railway personnel, pilots, air hostesses and stewards, etc.

The couriers are continually exposed to the danger of being apprehended while carrying compromising material. Therefore they must know as little as possible of the identities of the field operatives and the operations executed by them. This means that several security measures must be adhered to.

The couriers must never personally meet important field operatives or agents. Therefore, all contact is through liaison men or, preferably, letter drops. If a liaison man owns a restaurant or a small shop, open all day, then this is an excellent place for leaving and receiving messages.

Sometimes false information must be delivered to the couriers in order

to determine if they are being forced to work for the enemy. Such information is of the type which will trigger some kind of enemy action, if the enemy intercepts the message. If the courier delivers the message without the anticipated enemy action occurring, it can be assumed that the courier is still loyal.

For instance, if the message is about a planned secret meeting, supposed to take place at a certain time and place, then the enemy will put this place under surveillance at the appointed time, if the message is exposed to them. If this is the case, that courier can never again be trusted with real messages, although he can be used for handing over disinformation to the enemy. Naturally, the place mentioned in the message must never be used for a secret meeting.

If the message is delivered, and no such kind of enemy action takes place, then it can be assumed that the courier is still reliable.

If possible, all messages should be coded, or preferably paraphrased in a way so that the enemy cannot understand them or else will be fooled by them, if the courier is captured. The paraphrased message should appear to have an intelligible meaning, although in fact the paraphrased words have a completely different meaning, impossible to deduce. This can be done by using predetermined phrases and words.

A few examples of such paraphrased communications follow later in this chapter.

Finally, several couriers should be used on the same route but at different times. This will ensure that the route can still be used even if one courier is lost. Also, the risk of exposure is minimized by using several couriers.

The reason is that the enemy, if suspecting the route to be in use, will endeavor to identify the individuals often travelling along that route. Then they will try to figure out which of this number might be the courier. If several couriers are used, and every courier only travels along this route once again after a long period of time, then the risk of identifying him is greatly decreased. The enemy will believe that he travels along the route too seldom to be the courier they are looking for.

Civilian postal and telegraph systems

The civilian postal and telegraph systems can be put to good use as long as they are reasonably reliable. It should be noted, however, that this is not the case in all countries. In some places the post office personnel steal

either the stamps on the letters, discarding the mail, or else steal the entire letters.

To increase security, the letters or postcards should always be paraphrased so that they appear as completely normal and apparently innocent mail. Postcards are quite useful in this role, as few people expect a postcard to contain secret information.

One interesting case, in which letters were used for secret communication, took place in the United States during the Second World War. One of the agents of the Japanese intelligence service was an old lady, Mrs. Velvalee Dickinson, who owned an exclusive doll shop in New York. As she specialized in expensive, foreign dolls, she had a considerable correspondence with other countries, concerning dolls. But a part of this correspondence was actually sent to the Japanese naval intelligence.

In a letter to a Japanese contact in Buenos Aires, she reported for example that she had seen three newly-constructed warships, by in the letter mentioning "three wonderful Irish dolls". In the same way, she described one of the dolls (one of the warships) as an "Irish fisherman", which meant that it was an aircraft carrier. By the use of similar code words for other types of ships, she managed to report newly-constructed ships and repairs on already damaged ships. In every instance, she used doll descriptions as code words.

Mrs. Dickinson did however make one serious mistake. For some reason, she put the name and address of one of her normal customers as the sender on one letter. This letter was returned by the post office to the "sender", who naturally had never seen it before. The "sender", a certain Mrs. Mary Wallace, was puzzled by the returned letter and contacted the post office, which subsequently contacted the FBI. By a strict mail censorship, they recovered more letters of the same type, and finally Mrs. Dickinson was exposed. She was arrested in January 1944.

The postal system is also frequently used to signal emergencies. A field operative can send totally innocent postcards fairly often only to tell the receiver that he is well and unexposed. If the operative is arrested, this will be reported by the sudden stop in the flow of postcards.

Or alternatively, the enemy can force the captured operative to continue sending postcards, but then the operative can signal this by the addition or omission of certain words in the text.

The addition of certain, predetermined words or phrases in this way is called a positive security check. If he instead omits certain words or a

certain phrase, also determined in advance, this is called a negative security check.

The negative security check is usually the safest one, as it will also very often function if the operative is exposed or captured by the enemy security service, which itself tries to continue the correspondence by sending false information in the name of the captured or neutralized agent. Even if the captured agent or operative is forced to work for the enemy security service, it is likely that he can signal this by using the negative security check.

As an alternative method, the text on the postcard may be without any importance whatsoever while the picture on the postcard is the real message, different pictures having different meanings.

When postcards or letters are used for this purpose, it is advisable to send them to several different receivers, if possible both in and out of the country. Naturally, the addresses used must conform to the chosen cover of the field operative.

A case demonstrating the use and misuse of these systems took place in Scotland, in 1937. At that time a Scottish widow, Mrs. Jordan, was working as a hairdresser in Dundee. She had earlier been married to a German ex-soldier. Because of this connection, Mrs. Jordan was also active as an agent for the German intelligence service Abwehr. Abwehr used her as a letter-box. She received letters from certain operatives, and sent them on to other operatives or to addresses controlled by Abwehr.

It so happened that the mailman in the neighborhood also was an aspiring stamp collector. One day, he asked Mrs. Jordan whether he could keep the stamps on all those letters which she received from so many foreign countries. Mrs. Jordan got frightened by this innocent question, and flatly refused in a very definite way. The mailman was surprised over her strong reaction, and mentioned it to his supervisor.

The supervisor checked the matter, and found out that Mrs. Jordan received letters from the Netherlands, France, Sweden, and several countries in South America. But the bulk of the letters she sent out were addressed to the United States.

The supervisor found this so remarkable, that he contacted the British security service MI5. The security service decided to keep an eye on the widow's mail, and soon they had established the real reason for this correspondence. The result was that several German operatives in the United States were exposed. For some reason, which was never made

public, MI5 also searched Mrs. Jordan's home. They uncovered a few amateurish sketches of naval installations in the area. Mrs. Jordan was sentenced to four years' imprisonment in May 1938, which by the way was quite a severe sentence if the reasons given in court were the only ones for investigating her activities.

Telephone

Public telephones can be used in much the same way as the civilian postal system. As long as the message sounds apparently innocent, is in the local language and dialect, and the operative uses a public telephone instead of a private one, there is virtually no risk of exposure.

Note that in most countries, the police or security services are able to monitor all suspicious telephone calls without any chance of the user noticing it. Some countries, such as Russia, regularly tap the telephone wires in international hotels and the public telephones in their vicinity.

If the field operative is careful, there is little danger of the enemy receiving information on his current operations. But there is always the risk of exposure if he frequently calls the same person. The telephones cannot only be tapped, they can also be identified and located.

It must always be remembered to use preplanned ways of referring to places and times of meetings. For instance, if the field operative says "Tuesday, 6 p.m." he really means "Wednesday, 5 p.m.". The other operative understands this, as the two have planned in advance how to refer to times and places. Locations can be predetermined in the same way.

If the field operative fears that the telephone of his colleague is being tapped, but he nevertheless must arrange a meeting by the use of telephone, it is best if he calls the colleague from a public telephone, pretends that he phoned the wrong number, excuses himself in a prearranged way, and hangs up. This will tell the colleague that he should come to a certain public telephone in one hour sharp, or if he cannot make it, in another half an hour. There he will be contacted.

Also, certain predetermined phrases for emergency situations can be used at any time to report that the operative is under surveillance, his apartment has been searched, he is arrested, or any other emergency has occurred.

Radio

Radio communications provide instantaneous and generally reliable

communications. It is however dangerous to use radios extensively, as the transmissions are very vulnerable to interception, jamming, and direction finding. But in certain cases, radios must be used. This is reasonably safe if the following radio security measures are observed.

If possible, use only low-powered, frequency-modulated radios operating in the VHF or preferably the UHF band. Although these radio transmissions certainly are possible to monitor, their limited range makes them a little more safe to use compared to other, commonly available types.

The best type of radio transmitters are the burst transmitters nowadays often used by Special Forces in many countries. These transmitters will automatically condense the message, and then send it in one, short burst, not lasting more than a few seconds.

Last-minute control instructions in an operation can usually be sent by radio, as the enemy in any case will have no time to react, even if they are monitoring the transmission.

All references to future action, locations, and identities must be sent in code. But remember that almost any code can be broken. Therefore, use couriers if possible.

Cryptographic systems in use must be carefully guarded and destroyed before capture. Remember that simply burning them is not enough. The ashes must also be destroyed, as they might be read with special equipment.

Never transmit from the same place more than once. The transmitter must then always be moved to another location. Also avoid transmitting from obvious areas such as tops of mountains, towers, and similar places.

After transmitting, the radio site must be sterilized, i.e. all traces of the activity undertaken must be removed. Always position both an outer security ring and an inner security ring around the radio site when transmitting. Prepare a hideout about 500 meters from the site and move there immediately upon reports from the outer security ring on enemy activity.

Never place antennas where they are easily seen from a distance. Always camouflage the radio station and if possible position both the transmitter and the antenna indoors.

Make only a minimum of transmissions. Never tune the transmitter until exact contact time. If several transmissions are required, always transmit on an irregular schedule to avoid imitative deception, if the enemy

manages to break your code. Furthermore, endeavor to send short messages only, and only when absolutely necessary.

As a final note, if maximum security is necessary, position the radio station in a moving vehicle.

A scrambling system can often be used in conjunction with both radio and telephone. More information about this follows later in this chapter.

Pigeons and other animals

Homing pigeons have been used for centuries and can still be of use in certain situations. Other animals, such as dogs, can also be trained for this purpose, but they are usually not as reliable. The training of animals do however demand a fair amount of time, as well as special skills. The use of animals as messengers is not recommended except in exceptional circumstances.

Visual signals

Visual signals can be of any type. Some visual signals can be used for transmitting complex coded messages. This is possible by the use of light from electric torches, light reflected from a mirror, signal flags, and similar means.

But the most common type of visual signals is used for transmitting simple messages only. This kind of signal is frequently used as a warning system. Hideouts, homes of field operatives and agents, safehouses and similar locations must be made secure by using simple signals of this kind.

A prearranged placement of shutters, flower pots, arrangement of curtains, open or closed windows, or laundry hanging on lines, is frequently used as primary signals. They must be possible to observe from a distance to avoid any possibilities of walking into a trap. If the operative, on approaching the house, notices for instance that a certain window is open, he knows that it is safe to enter. But if the predetermined window is closed, then he knows that he must not enter, and simply walks past the house without showing any interest in it.

However, if the inhabitants of the house are unexpectedly arrested, the primary signal may be compromised or rendered out of function. Therefore, a secondary signal is also used. This must be possible to activate even if the agent is being led off in handcuffs. For example, he can "accidentally" knock over a flower stand, or take a special pair of shoes, to signal that he has been arrested, if another operative comes there later.

Many times, it is also possible to signal a simple message by such an ordinary event as having a man walk across a given street at a specified time, or any other predetermined but perfectly normal event. This method is fairly often used to indicate to a field operative or an agent whether he is under surveillance or not.

During clandestine meetings, it is fairly common to exchange recognition signals, such as carrying a specified newspaper in a predetermined hand. This is fairly often coupled with code words (audible signals). Also, a visual signal, perhaps lighting a cigarette, is used by either of the two operatives in a meeting to indicate that he is under surveillance and the meeting must be cancelled. Then the two operatives will walk on without showing any knowledge of each other.

Audible signals

Audible signals can often be used in the same manner as visual signals, and the two are often combined. Examples of audible signals include musical instruments or tape recorders playing a certain tune, vehicle horns, sirens, church bells, dogs barking, and naturally also voices, such as a conversation on a given topic.

If a prearranged dialogue is used as a password, the dialogue must be specific, so that there is no risk that, by chance, another person may use the predetermined words. But still the dialogue must sound natural and innocent.

A Soviet operative in Berlin was to meet a courier, unknown to him, in order to hand over a roll of film for transport to Moscow. The meeting was scheduled to take place at a bus stop. When the field operative arrived at the bus stop, he at once noticed a man answering to the description of the courier. The Soviet operative approached toward that man, and said according to his instructions:

"I'm here as a tourist. I admire your beautiful country."

"Yes, it's beautiful. I'm a tourist, too," the other man answered, completely in accordance with the preplanned conversation.

The Soviet operative produced his small box containing the roll of film from his pocket, and was just to hand it over, when the other man suddenly said "There's my bus!" and hurriedly boarded a bus, which quickly drove away.

It was then that the Soviet operative realized that he had been conversing with a genuine tourist, and not his courier.

Simple codes

Codes are very useful security devices but only as long as they remain unbroken and uncompromised. Most or all codes possible to use in the field can be broken. Therefore, it is often better to rely upon a simple system which can provide basic security without requiring too much time, equipment, or cryptographic training.

The most effective system is to have code words for all important messages, sentences, and words. These code words must be determined in advance and as long as they are not compromised or misused, this system is fairly effective and safe.

Another, extremely simple code is the "Book Code". It depends upon a predetermined book, sometimes a dictionary. Every word in the message is located in that book. The page on which the word is written, the line number, and finally the place of the word on the line are determined. A single word can therefore be rendered in the following way. 322084 (page 322, line 8, and word number 4) Note that the page is always written with three digits (i.e. page 12 is written 012), while the line is written with two digits and the word number with only one digit. Furthermore, all "words" written in this way are written together without any dividing space in order to provide a long and uninterrupted list of numbers. As long as the word is never repeated in the same format (there are many instances of a given word in an average book), this code is extremely difficult to break, as long as the title of the book remains unknown.

Scrambling systems

Many different types of scrambling systems are available. Government agencies and the military usually use one or more systems of this kind. But nowadays it is more and more common for ordinary business corporations to use them as well.

The most common type of scrambling device works by turning normal conversation into indecipherable words. This effectively prevents eavesdropping by wiretapping. This device can be plugged in like a regular telephone. Because of this, it is portable and can be used anywhere, as long as a telephone connection is at hand.

A device of this kind (Fig. 35) uses a sophisticated tone inversion process to scramble the conversation. The chosen code must be manually selected. Usually, a device of this type can choose between about twenty-five different codes. This is sufficient in most situations. It is however not

Fig 34

sufficient to defeat contemporary code-breaking technology. Therefore, more advanced models are also available. They use a computer for changing the code ten times every second during transmission. This device is also easy to use and it is of course also possible to alternate between clear and scrambled speech. This can be done by simply flipping a toggle switch.

An even more reliable scrambling device combines the protection of voice and data security within a single unit. This system transforms voice signals by the use of a speech digitizer into a stream of digits which are encrypted by a three-level randomly generated key system. This code may be possible to break, but the time and effort required makes the system secure for use in the field.

As this system works with digital information, it can also be used as an encryption modem when used with a computer terminal. As the device is small enough to fit into a briefcase, it is fully portable and can be used on any telephone. This will generally be sufficient to protect against wiretapping. If used in conjunction with a non-radiating computer, it is also sufficient to protect against other kinds of bugs and hidden tape-recorders.

Naturally, the system can also alternate between clear and secure speech.

If the operative suspects that he is monitored not only by wiretapping, but also through the use of hidden bugs, a scrambling device is not sufficient to protect a voice transmission, whether by telephone or radio. The field operative will speak into the scrambling device, and then his own voice will be monitored. In this case, the problem can be solved by using a non-radiating computer. If the operative writes down his message with the help of the computer, and the scrambling device scrambles and then transmits the stream of encrypted digits, it will not be possible to eavesdrop on his transmission. No longer need he read out his message aloud.

But non-radiating computers are not always available. Therefore there are also scrambling devices that work exactly as a small non-radiating computer, as described in the previous paragraph. Instead of speaking, the user types his message on the computerized keyboard. The device stores up to several pages of information and finally, when the user so decides, sends it over ordinary telephone lines or any radio transmitter, such as a walkie-talkie (Fig. 36).

Fig 35

When transmitting, a built-in scrambler automatically encodes the message and ensures that the communication is secure. The receiving device will decode the message, and the receiver will be able to read the message as computerized type on his own device. He can also receive the message in hard copy form by using a miniature printer. An ordinary cassette tape recorder can also be used to retain the information on a perfectly ordinary cassette tape. no computer disk is required.

This device can also transfer messages across the International Telex Network.

As both the scrambling device and the miniature printer are portable, this system can be used anywhere in the world.

Invisible ink

Invisible ink is generally regarded as an outdated method of secure communication, as it is extremely easy to develop. There might however be certain cases where invisible ink can still be used profitably.

The "ink" used for this purpose is generally made with special chemicals. Writing done with such ink can be developed by using another chemical, known as the reagent. There are literally hundreds of formulas for such invisible inks, many of them with their own, special reagents.

Invisible ink is generally used to write between the lines, or in lines that cut across the visible writing, in a perfectly ordinary letter. It can also be used on other innocent pieces of paper, such as tickets, or in books. Generally a tiny paint brush is used instead of a pen, so that there will be no marks on the paper caused by the pen's point. Soft, uncoated paper should be used for the same reason, so that the ink will soak into the fibers instead of drying on the surface. There are several ways of making invisible ink. None of them is perfect, so the most common methods of improvising invisible ink are listed below.

- Make the ink by dissolving potassium-ferrocyanide (potassium cyanate) in water. This produces a yellow solution, which is used as ink. To develop this ink, dissolve a fairly large quantity of ferro-sulfate (iron sulfate) in water. This results in a green solution, which is used for coating the written paper.

  It is also quite possible to use the ferrosulphate solution as ink, and the potassium ferrocyanide as reagent. A solution of washing soda (sodium carbonate) can also be used as reagent in this case.

- Ordinary lemon, orange, grapefruit, or onion juice can be used as ink. This ink is developed by heating, for instance over a hot light bulb. Ordinary fire is usually too hot, and will only char the paper.
- Rice water can also be used. Text written in this is developed by iodine.
- Another method does not require any ink at all but lots of ordinary water, thus creating a watermark that is visible when the paper sheet is wet. The writing is done in the following way.

  First of all soak a piece of paper thoroughly in water and put it on a sheet of glass or a mirror. Then put a dry paper on top of the soaked paper. The message should be written on this dry paper with a ballpoint pen or a hard pencil. The point of the pencil must not be sharp, however. An impression will be made on the soaked paper below. This is the watermark.

  After writing the message, it is important to remember to destroy the dry sheet. As the soaked paper dries, the writing on it will disappear. To develop the text, simply soak the paper once again and put it on top of a (preferably red, blue, or green) glass plate. Then the text will reappear.
- Ink made with cupric sulfate (copper sulfate), if it can be obtained, can be developed by exposing the writing to ammonia fumes.
- The main ingredient of many laxatives is phenolphthalein. One such tablet, if dissolved in rubbing alcohol, will make an efficient ink. The reagent is household ammonia, or any other strong alkaline such as washing soda dissolved in water.

9

Photography

Photography can be put to many good uses in covert operations. A few examples of this will be put forward in this chapter. The most common uses are the following.

Photography has for a very long time been used to copy documents. These might be secret documents, observed by the operative during a break-in or by a native agent, unable to remove the original due to security reasons.

In most countries nowadays, it is however easier for a native agent to copy the secret document by using a photo-copying machine. Then there is no risk that the guards will find the small camera, that he otherwise would have to bring into the secret area.

But in some countries photo-copying machines are carefully guarded and supervised for this reason. Then the agent must bring in a camera.

Another reason is that negatives are more easily hidden and stored than the real documents. If available, microfilm can also be used. Microfilm or negatives are much easier to smuggle in or out of hostile countries. Microfilm can even be made as small as the so-called microdots. Then the negative is very easy to hide for instance behind a stamp on a letter or even glued into a typed text, as a dot.

This means that even if it is easier to bring out a photo copy from the enemy building, it might still be required to snap a photograph of the copy, destroy the photocopy, and then smuggle out the negative of the photograph.

Naturally, it is also easier to hide one's own secret or compromising documents if they come as negatives. This might for instance be required if it is necessary to bring manuals, lists or registers, or other types of needed documents into enemy territory.

Intelligence collecting, and particularly target reconnaissance, is another traditional field of photography in secret operations. The reason is of course that this is much simplified through the use of photography and

then often reveals more information than the observer can interpret and remember without recording it. Telephoto techniques might be most useful for this purpose.

Surveillance and identification of individuals, finally, are much simplified by the use of photography. Nowadays small video cameras are most often used for this purpose.

In the past, only ordinary hand cameras were used in covert operations. Nowadays the video technology has advanced rapidly, producing small and efficient video cameras already in common usage among tourists and other civilians. The quality of the video recording has also increased considerably. Video equipment is therefore now a fully equal, and sometimes superior, alternative to ordinary hand cameras.

For security reasons, it is always best to develop the roll of film personally. Therefore, the cover of many field operatives includes amateur photography and development.

Hand cameras

The best is to have access to three different kinds of cameras. First of all, an automatic system camera with a telephoto lens is very useful. Preferably, the camera should also be possible to use manually. This camera is accurate for long-distance photography, but it is necessary to remember that a telephoto lens requires more light than an ordinary lens. This makes the use of telephoto techniques more limited than usually imagined, especially at night.

An alternative method is sometimes to use an ordinary lens, and then to enlarge the important part of the photograph. This can sometimes give very good results, especially if light-sensitive film is used.

Another requirement is that the shutter speed be very fast, so as to eliminate the field operative's normal tendency to tremble when under stress, caused by fear of detection or too short a time to properly adjust the camera. The use of film of a high ASA/DIN number is also advantageous.

Many types of hand cameras are available for surveillance work. Among the different brands often used for this purpose, Nikon and Minolta, both Japanese cameras, are very popular because of their high quality.

But almost any automatic 35mm system camera can be used in surveil-

lance operations, as long as the camera has an automatic motor-drive which winds the film on, allowing continuous shooting.

Actually, a system camera is not always the best choice, as many field operatives tend not to adjust the camera properly, because of tension or lack of time. In that case, a small auto-focus camera is more useful. Nowadays even auto-focus cameras have telephoto zoom lenses, which makes them highly useful for surveillance work. They are also smaller and more compact, two characteristics of ultimate importance in covert operations.

These types of cameras also frequently have the option of printing the time and date on every photograph. This is very helpful in surveillance work, where maybe hundreds of photographs may be collected by several different operatives. All these photographs are often very similar to each other, which makes a proper time and date even more helpful.

One such very useful auto-focus camera is the Yashica Samurai. The main advantage of this camera, and a few others of a similar type, is that it, because of the way it positions the frame on the roll of film, allows its user to take twice as many pictures on one roll of film compared to an ordinary camera. Using a 36-exposure film means that the operative will actually be able to snap at least 72 and more likely 75 frames.

This camera comes with a teleconverter, extending the focal length up to about 140mm. On this camera, this is actually equivalent to about 200mm on a full-frame camera. But even with this teleconverter, the camera is still compact and easy to hide.

Secondly, the field operative will often need a small, easily concealed camera. This camera can be used at closer ranges, when it is needed to hide the camera in an inconspicuous way before and after the shot. By the technique of "pressing" film (described below), this camera can sometimes be used even at night.

The Minox cameras are good examples of this kind of camera. This line combines excellent quality with a very small size. If even the Minox is too big, then the Minox EC should be considered. This is a very small and easily hidden camera. Unfortunately, it cannot use 35mm film.

Actually the Minox EC belongs more properly in the third category of cameras.

This category, consisting of very small cameras, is absolutely vital for real inside work, when there is a very real risk that the operative will be revealed if it is found out that he is carrying a camera. Sometimes such a

camera will be hidden in a wrist watch, cigarette lighter, or any similar object. This camera will unfortunately not produce perfect pictures, so if at all possible, it is advisable to try to bring the system camera. However, in certain situations this may be too dangerous.

Some cameras can be equipped with image enhancement devices, thus permitting night operations. These however are highly expensive as well as certainly compromising, as ordinary people usually do not use this type of equipment. There is a simpler method which usually can provide acceptable photos, even under poor light conditions. This is called "pressing" the film.

This is done by using for example 200 ASA-film, but with the camera set on a higher ASA-setting, thereby increasing the speed. Thus, to press 200 ASA-film, follow these instructions.

- To increase the speed by one stop, use setting 400 ASA.
- To increase the speed by two stops, use setting 800 ASA.
- To increase the speed by three stops, use setting 1600 ASA.
- To increase the speed by four stops, use setting 3200 ASA.

The more a film is pressed, the more light sensitive it will become. Unfortunately, the picture will also be grainier and turn into a slightly red nuance. Furthermore, the developing time will be increased if the speed is increased.

Pressed film can be developed by a trained photographer or in a commercial photographic laboratory, but not in an ordinary photo shop. This is usually of no great matter, as an ordinary photo shop never should be used anyway for developing secret photographs, because of the security risks.

Most brands of film are suitable for pressing. One easily obtainable type is Kodak 400 ASA (slides). Kodachrome is also good but more difficult to develop. Generally, slides will give the best result.

The one big disadvantage of most auto-focus cameras is that the user is not allowed to set his own, chosen ASA number. If this is impossible, it is also impossible to "press" the film when the light conditions are bad. It is however possible to "cheat" an auto-focus camera by changing the computer code on the roll of film. This DX-code is used by the camera for adjusting the ASA number. If the code is changed, the camera will

automatically adjust the ASA setting in what it believes to be the correct way.

The KGB is reputedly using a special kind of film. It is said to be already exposed, so if a roll of this film is captured and developed, the enemy will only see a series of totally harmless photographs. The real, important photographs can only be developed by a special technique. If the film is developed in the ordinary way, these photographs will be destroyed and only the pre-exposed, harmless photographs will appear. This method was reputedly developed in order to deny the enemy the use of captured film as evidence against a KGB operative.

Video cameras

Video cameras are nowadays in frequent use. There are many types available, in all sizes from the portable Japanese video cameras, slightly bigger than ordinary system cameras, to the small, miniaturized surveillance cameras, most commonly hidden in some place. All these types are suitable for surveillance purposes. Even the Japanese portable cameras are now in such common use among tourists, that they never attract any special attention.

Video cameras have for a long time been used for detecting unauthorized intrusion on the premises of both private houses and corporate or government buildings. But contemporary video cameras are so small that they are as easily used for covert surveillance purposes (Fig. 36).

The video camera is easily hidden, and either a wide-angle lens or a telephoto lens can be connected, to ensure that the correct area is covered. It should be noted, however, that both these types of lenses do require favorable light conditions.

Another important advantage is that the video camera can be connected directly to a TV monitor. In this way any interesting activity can be taped and reviewed later.

The video tapes used for surveillance purposes can record up to eight hours per tape. As a rule of thumb, the video recording equipment used for surveillance is generally able to record three times as long, compared to normal video recorders, on a standard VHS cassette.

Contemporary miniature video cameras are often made to function effectively even in very low light (Fig. 37). They are often able to pick up infrared sources as well.

Despite all new possibilities of the video technology, certain brands of

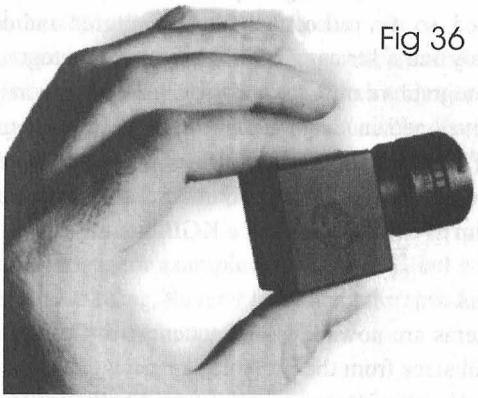


Fig 36

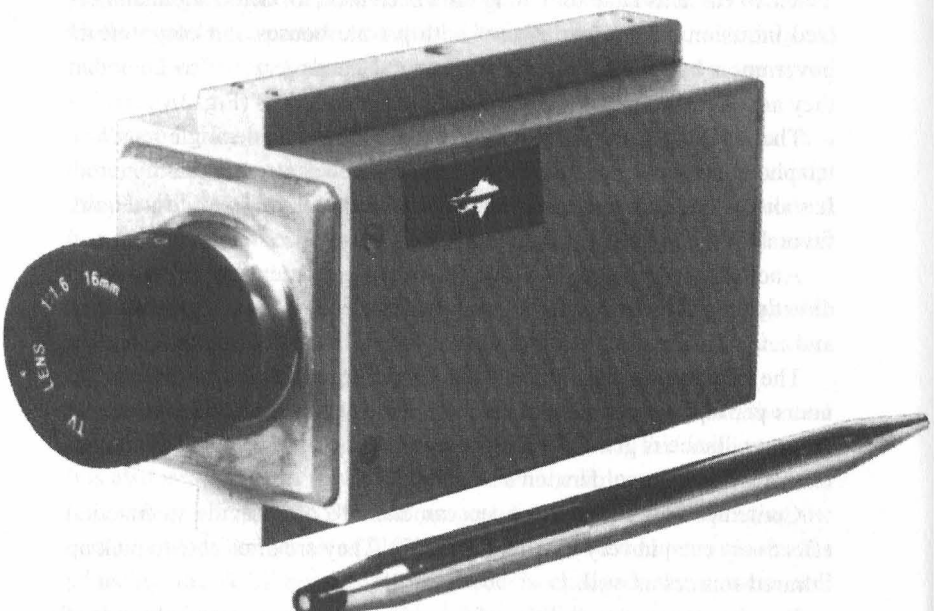


Fig 37

miniature video cameras are still susceptible to technical malfunctionings of many kinds. One example is when the camera is unable to function in bright light, as the aperture is built for mainly working at night, in poor light conditions. Many cameras are also very susceptible to vibration and shock.

Some contemporary miniature video cameras have in fact excellent infrared vision. They can be used in complete darkness, as long as the area is lit up by an invisible infrared light source. This allows complete visibility even at night.

One disadvantage of several such systems is that picture quality often is affected by the presence of ordinary light. The reason is that these cameras are mainly or even exclusively made for use at night.

Some video cameras are able to adapt to daylight as well as to total darkness (if the area is lit up by infrared light beams). Not all cameras can do this, however, as an attached filter must be used to block out all existing visible light. If this filter is not used, picture quality will be adversely affected. This type of video camera is still fairly large, however, and not so easily hidden.

One thing to remember, however, is that adverse climate conditions will seriously raise the risk of malfunctioning. Many of these cameras will only operate in a temperature of between 10 degrees Celsius and +50 or 75 degrees Celsius. This may sometimes prevent use in outdoor locations in winter. All kinds of electronic equipment are also affected by a high level of humidity, such as in some tropical countries and in saunas.

Another interesting development is the Borescope technology. This technology utilizes fiber optics to see "through" objects such as walls and doors. A small hole is required through which the Borescope, a thin fiber optics cable with a small camera lens, is inserted. Viewing, either with the naked eye or with a TV monitor, is then possible.

Such techniques can also be used to see into objects suspected of containing explosives or bombs, and into other places suspected of containing contraband or illegal equipment, such as gas tanks on motor vehicles.

Borescope equipment was for instance used by the British security service during the siege of the Iranian Embassy in 1981. By this technique, the British managed to get information on the terrorists' weapons and positions, and the disposition of the hostages. The available surveillance technology contributed to the successful conclusion of this operation.

The Borescope technology is now also in common medical use.

As always when using a tape recording system, it is prudent to first make a copy of the recorded tape. Then, if several viewings are necessary, the analyst can work with the copy. Otherwise the original tape may be worn or accidentally damaged.

Night vision devices

Night vision devices or different types are often used in conjunction with both ordinary cameras and video cameras.

Basically, there are two types of night vision devices. They are the active and the passive systems. The active type emits its own light source, an infrared beam, which is visible to the user through the infrared scope which is part of the unit. The passive type of night vision device does not emit any light. Instead they electronically amplify whatever existing light there is in the environment, such as moonlight, starlight, or any other visible light, which is why such units are sometimes referred to as "Starlight Scopes".

The advantage of the active type of night vision device is that the user can see in total darkness, since he does not have to depend on available light from the environment. Disadvantages of active night viewers are limited range, and the fact that the infrared beam is visible to anyone else looking through an infrared scope, or through a passive night vision device.

The primary surveillance purpose of night vision devices is to permit the field operative to carefully observe events at night, occurring at a large distance. Because of this, they are very useful for surveillance purposes. They are also frequently used by enemy security and law enforcement officers.

Night vision devices are frequently, with the help of adaptors, attached to the front of cameras. This is to obtain pictorial evidence, or information. Both video recordings and still photographs can be obtained in this way. Night vision equipment can also be linked with closed circuit television (CCTV) for security purposes. Then the same coverage of the area can be assured both by day and by night.

Passive night vision devices, or image intensifiers (Fig. 38) as they are frequently called, are generally divided into two basic types, too. One distinguishes between the first generation and the second generation. The method of construction decides whether the image intensifier belongs to

Fig 38

the first or the second generation. The first generation is not obsolete in any way. The two types only have different advantages and disadvantages, and should be used in different situations.

To be really useful under field conditions, the night vision device must possess certain features. An Automatic Brightness Control (ABC) is designed to automatically adjust and maintain the gain at a correct operation level. This is necessary as any light gain over the threshold limit tends to burn out the night vision device, or at least reduce its lifespan. It can also temporarily blind the operator.

The ABC will also reduce the gain to a safe level, if a bright light suddenly is directed toward the viewer. In the same way, the ABC will automatically increase the gain, if the observer looks from an area illuminated by for instance a street light to a very dark area.

Another mandatory feature is a focal plane iris. This is a separate iris, not part of the object lens, and it is located on the front of the viewer behind the lens. The focal plane iris permits the operative to manually close down, and thereby reduce, the size of the field of vision. This grants him several advantages.

The operative can for instance block out bright lights on the edge of his field of vision, thereby protecting the intensifier. Another important

advantage is that this will allow the operative to read the license plates of a car, even if the car lights are lit up. The lights usually appear as large bright areas in the scene, so that otherwise the license number cannot be obtained. But by closing down the focal plane iris, the observer can blot out the lights, thus enabling the license number to be read despite the interfering lights.

In situations where there are many bright lights, he can by using the iris observe details which would not be visible otherwise, because of the same reason. As the aperture in every situation can be manually adjusted, the operative can also look into dark areas surrounded by bright lights.

Still another mandatory feature is a closed eye cup. This is necessary, as the night vision device will emit a yellow-green light through the eyepiece lens into the eye of the observer, in order to enable him to see. However, when the observer removes or lowers the viewer from his eye, the emitted light will illuminate his face. This makes him easy to detect by the person being observed. An eyecup that snaps shut when removed from the observer's eye, thus preventing light from escaping, makes the device safe to use under all conditions.

If the night vision device is to be used with a camera, it is necessary that a proper adapter is available. Another problem with certain cameras is that it is sometimes necessary to manually take a reading through a light meter and then turn on an electric light to adjust the camera, before the photograph can be snapped. This is most unsatisfactorily as this both demands a long period of time and also gives the operative away by requiring a visible light source.

The range of the night vision device depends on the type used as well as the circumstances. The active infrared devices have a limited range. The passive intensifiers can see to the horizon, in the same way as a telescope, so here the magnification level is the real concern. The important factor is however the distance at which an object can be recognized. This depends on a number of factors, but mainly the focal length and the f-number of the lens. As the focal length of the lens increases, so does the magnification of the target. The lower the f-number, the more light passes through the lens, which results in a clearer image.

Many different lines of night vision equipment are available. The smallest are the so-called pocket scopes (Fig. 39). They are sometimes designed to also withstand a fairly high level of shock, such as associated

with rifle-firing. If this is the case, the pocket scope can also be used as a night sight for weapons.

Such a night scope is frequently supplied with a 105mm f/2.5 objective lens. It is small and of course battery-powered. The weight need not be more than 425 grams. The length of the night scope is a little more than eight centimeters. It is often also possible to use as a camera objective lens (Fig. 40).

Larger, night vision goggles are also available, enabling for example driving in darkness without needing to use the headlights (Fig. 41).

Night vision binoculars are also available. They are naturally larger than the pocket scopes, but they have a higher light-gain and are also more comfortable as they allow viewing with both eyes (Fig. 42). They are usually not, however, supplied with light secure eyecups. Because of this limitation, as well as the fact that they are ideal for long periods of observation, they are often used by security guards of for instance airports and military bases.

Similar, active infrared devices are also available. They look basically the same as the passive devices. Their range is however limited to the range of the infrared light source. Such infrared light sources generally come in three different types. An infrared flashlight, for instance, is a hand-held rechargeable halogen flashlight (Fig. 43). It can provide light up to approximately ninety meters.

The infrared spotlight (Fig. 44) is also a hand-held rechargeable unit. It can project infrared light up to around six hundred meters, which is generally the maximum range of the active night vision device in any case.

Finally, an infrared floodlight can be used. This works as an ordinary floodlight and is usually mounted on a vehicle (Fig. 45).

Most night vision devices can be connected to other lenses and sometimes to each other. This provides more flexibility, as the distance to the target and the light conditions in the area of operations can be highly variable.

Unfortunately, even when the night vision devices are compact and easily portable, the available extra lenses and cameras are often not. This can sometimes prevent their use in the field. This is especially true as this kind of equipment is highly compromising just because no ordinary people ever would use it.

Fig 39

Fig 40

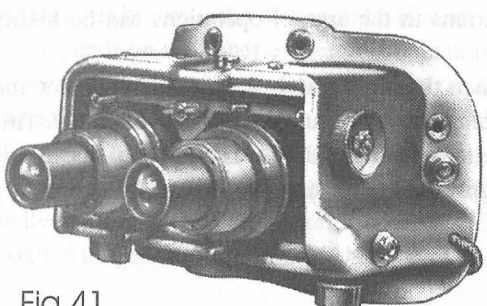


Fig 41

Fig 42

Fig 43

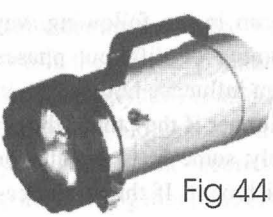


Fig 44

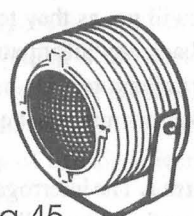


Fig 45

10

Enemy Interrogation Techniques And How To Counter Them

If a field operative is captured by the enemy, his life will to a large extent depend on what he tells his enemies about himself. If he is lucky, there is always the chance that the enemy is convinced by his cover, and he is released because of a lack of evidence against him. But if the enemy interrogators suspect that their prisoner knows more than he has said, then they will use harsher and more thorough interrogation methods.

Interrogation of that kind may include both ordinary interrogation, psychological torture, and physical torture. It is vitally important to understand this process as it may determine the life and health of both the operative and his colleagues. It is of the utmost importance that the operative has fully realized what might happen during an interrogation, even before he is captured.

The operative must be mentally prepared for what is coming. Only then is there a chance that he can withstand a ruthless interrogation. Besides, the fate of his colleagues and his native agents also depend on what he might tell the interrogators.

A thorough interrogation is usually run in the following way. The interrogation can be divided into a number of different phases. The behavior of the captive will to some extent influence how far the interrogators will go, as they tend to continue longer if they think the prisoner holds back any information. Unfortunately, some countries also practice indiscriminate torture, as a kind of punishment. If this is the case, the interrogators might not even ask questions.

Phase 1. The interrogation team, at this stage often consisting of a large number of people, will force the prisoner to sit down on a chair in their

midst. They will stand in the dark while the prisoner is blinded by bright spotlights or other lights. The interrogators will ask the prisoner lots of questions, all of them repeated many times, as they want to make the prisoner angry and despairing.

The prisoner should avoid maintaining a stubborn silence, as this will only convince the interrogators to prolong the interrogation. Instead he must always answer the questions, but in a very vague and indeterminate manner. He must say as little as possible. It is vital that he denies all accusations, even when the interrogators have evidence. The prisoner must at all cost avoid mentioning names, except of known enemies. It is most likely that any person named will also be arrested and subjected to interrogation of this type.

If the prisoner is not blinded by bright lights, he must still avoid looking the interrogator directly in the eye, as a skilled interrogator can deduce some information even without a direct answer. The prisoner should instead try to concentrate on a spot between the interrogator's eyes or on his forehead.

Phase 2. After one or more interrogations of the previous type, one of the interrogators will feign friendship with the prisoner. This is of course only in order to deceive the prisoner. Unfortunately this is one of the most dangerous tactics from the prisoner's point of view.

Even with proper training, there is a great risk that he simply out of exhaustion will throw off his guard and relax to a dangerous degree because of the interrogator's "friendly" conversation. This will easily cause the operative to reveal himself, for instance by admitting some small but vital trifle, impossible to explain by his cover. Therefore, the prisoner must never enter into discussions of any kind with the interrogators.

It is also common practice to let one interrogator pretend to be a sadistic brute, while the "friendly" interrogator tries to stop him from hurting the prisoner. Naturally, this is also a trick to deceive the prisoner.

One example of this method took place during the Second World War, in Egypt. The British security service had captured a German agent. During the interrogation, one of the interrogators suddenly prepared to use narcotics to make his prisoner speak. He was just preparing to insert the needle into the prisoner, when suddenly a group of British officers burst into the room.

"We don't use Gestapo methods!" they yelled, and hurriedly brought

the German prisoner back to his cell, while they at the same time loudly complained about the excessive methods of the first interrogator.

This incident was naturally played out in order to both frighten the prisoner, and at the same time cause him to lose trust in his own country. After this, the British officers made several efforts to engage in small talk with the prisoner, and eventually they succeeded in making him talk.

Another variant of the same method is to disguise a provocateur as a fellow prisoner, and put him in the same cell as the real captive. The cell will naturally be bugged. The provocateur will try to engage the real prisoner in conversation, thus endeavoring to make him reveal himself. The captured operative must be conscious of such efforts, and not let himself be fooled by them. It is much safer to give the impression of being taciturn and inward-looking, rather than entering any conversations.

Phase 3. If all these attempts fail, it is likely that the prisoner will be threatened, beaten, and in all possible ways mistreated. He can expect solitary confinement, confinement in dark cells, or both at the same time. The prisoner may also be confined in an extremely small cell, which will prevent him from sitting or lying down. Each time he begins to fall asleep, the guard will wake him up. This is in order to cause him excessive fatigue. It is also common that the prisoner is denied access to toilets and washrooms. The guards will often attempt to demoralize him with horrible news as well. He might also be made to suffer from hunger, thirst, and cold or excessive heat.

At this stage it is very common that the guards will physically hurt the prisoner. If he is knocked down by the guards, the prisoner must not try to stand up or to remain in their midst. Instead he should try to reach a corner of the room, so that only some of them can strike him at the same time.

The prisoner must never attempt to be brave in this situation. Unasked for bravery will only cause him more wounds. Instead he should play seriously injured, fall down on the floor and roll over onto his stomach. Thus most of his sensitive organs will be protected by the rib cage. He should also try to pull in his chin and attempt to protect his kidneys by pressing his elbows tight against his sides.

Phase 4. After this, the prisoner will be tortured. The guards will pull out his teeth and nails, burn him with lighted cigarettes, hurt his genitals

in several different ways, and if the prisoner is female, rape her repeatedly. Electric shocks are common too. Sometimes drugs are also used, or different chemicals to make the prisoner speak freely.

If after the end of this phase, the prisoner has still told the interrogators nothing (a rare but not unheard of phenomenon), there is a high possibility that he will simply be executed.

There is only one way of escaping interrogation of this kind. During the initial interrogation, and all subsequent phases, the captured operative must stick to his cover at all times. This is his only chance of survival, as the interrogators eventually may decide that he really knows nothing of importance. But then the cover must be sufficiently detailed and believable to convince them. If the captive really is unable to explain himself and his actions, then the interrogation will only progress to more ruthless methods.

If the operative is lucky enough to be interrogated without the use of torture, such as is often the case if he is arrested by the ordinary police, then he might suddenly find himself in a situation in which the interrogator clearly does not believe in his cover story, but nevertheless is unable to prove that he is a foreign intelligence officer. The reason might be that the police has uncovered evidence of the operative breaking a law, for instance by using forged identity documents. Despite this evidence, they might be unable to uncover his real identity.

In such a situation, and only in such a situation, the captured operative is allowed to leave his cover, and instead use his absolutely last line of defence. This is the emergency cover.

An emergency cover must be totally impossible to check. A fairly sound and credible emergency cover is that the operative in fact is a foreign criminal, who after escaping from jail in a foreign country bought a forged passport on the black market. Then he illegally entered the country in which he now finds himself. If using this story, it is of course vital to choose a country of origin in which it is impossible to check any criminal records.

An emergency cover story of this kind might be sufficient to convince the police that their prisoner is no foreign intelligence operative, if that is what they are looking for. After all, they have now received a confession of criminal activities, so they have reason to be satisfied. The captured operative, in his turn, will be happy to avoid further and more intense

interrogation. But he will of course also be unable to continue his work in that country.

The KGB has used an interesting variant of this emergency cover. A Soviet operative, captured in a Western country, managed to make the interrogators believe that he in fact was a wanted, Russian criminal. He was naturally expelled back to the Soviet Union, where the KGB immediately promoted him for his initiative and cunning.

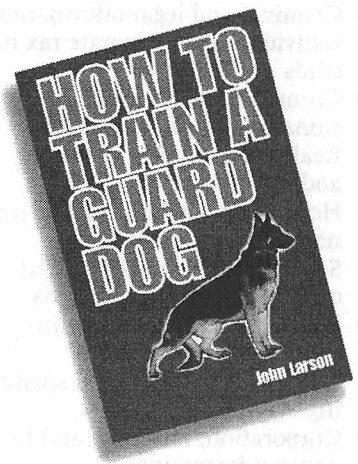
The most important rule in all kinds of interrogations and questionings is consequently this one:

"Always have a story to tell and stick to it whatever they confront you with!"

J. FloresPublications

P.O. Box 830760, Miami, FL 33283 • 800-472-2388

A complete "how-to" guide on the selection, care and training of security or "guard" dogs.



HOW TO TRAIN A GUARD DOG By John Larson

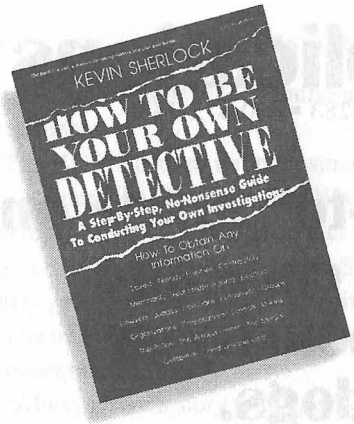
How To Train A Guard Dog By John Larson is not just another obedience training book. All steps necessary to develop a strong, intelligent dog capable of safeguarding your property and even your life, are completely outlined in a simple step-by-step, illustrated manner.

Among the many subjects covered: Principles of dog training; basic, intermediate and advanced obedience training; attack and guard dog training methods; advanced off-leash training techniques; behavior and motivation; equipment and supplies needed; diseases and their prevention; care and feeding; types of veterinary services; and dozens more!

In these times of widespread crime, a skillfully trained dog could be the best security investment you could make. Get your copy now! 5½ x 8½, softcover, illus., 108 pp. ISBN 0-918751-05-5

No. 02 $10.95

To order call toll free 1-800-472-2388 (credit card orders only) or mail check or money order to address above. Please include $5 extra per order for shipping.



HOW TO BE YOUR OWN DETECTIVE: A Step-By-Step, No-Nonsense Guide To Conducting Your Own Investigations by Kevin Sherlock

There are many good reasons for you to know how to check people's backgrounds. If you're working (or would like to be) as a Private Investigator, Paralegal, Writer, Journalist or any other profession that depends on doing research — this book will give you the edge over your competitors.

If you're going to spend money on property, a car, or medical treatment, for example, you'd certainly like to know if the providers are honest and capable.

Or what if you want to invest money or go into a business with a partner? You'd like to reassure yourself the guy is reasonably honest and didn't make his money on dope pushing, pimping, or insider trading!

Written by veteran newsman Kevin Sherlock, this book teaches you tactics hard-hitting enough for professional investigators, but easy enough for almost anyone to follow. If there's dirt on someone, this book shows you how to dig it up readily, legally, and ethically. It also shows you how to put such info to good use. None of the research techniques detailed are expensive or time-consuming.

Using actual incidents and court cases as examples ***How To Be Your Own Detective*** shows you how to find out these items and many more from the public record:

- Personal data such as Social Security numbers, addresses, phone numbers, birth, death, marriage, and divorce information and personal dirt
- Criminal and legal information
- Individual and corporate tax records
- Coroner, medical and professional malpractice records
- Real estate, zoning, planning, and land use records
- How to track white-collar criminals and sex offenders
- School taxing, spending, and quality of education records
- Political finances and politicians' personal finances
- Government taxing and spending
- Corporation, industry, and finance information
- Labor, environmental, and health code violators
- Lawsuits and other legal entanglements
- ...and much more

If you're mad at a local merchant, worried about a real estate deal or the quality of your children's education, or suspicious of a business offer; you can use this book. 8½ x 11, softcover, 244 pp
ISBN 0-918751-33-0

No. 32 $29.95

Includes IBM compatible Electronic Book computer disk version

To order call toll free 1-800-472-2388