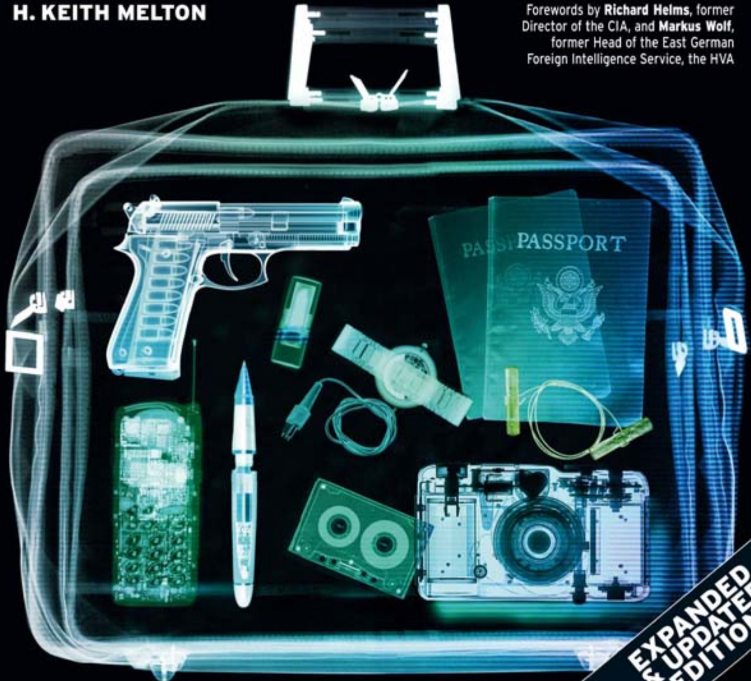
ULTIMATE SPY

INSIDE THE SECRET WORLD OF ESPIONAGE

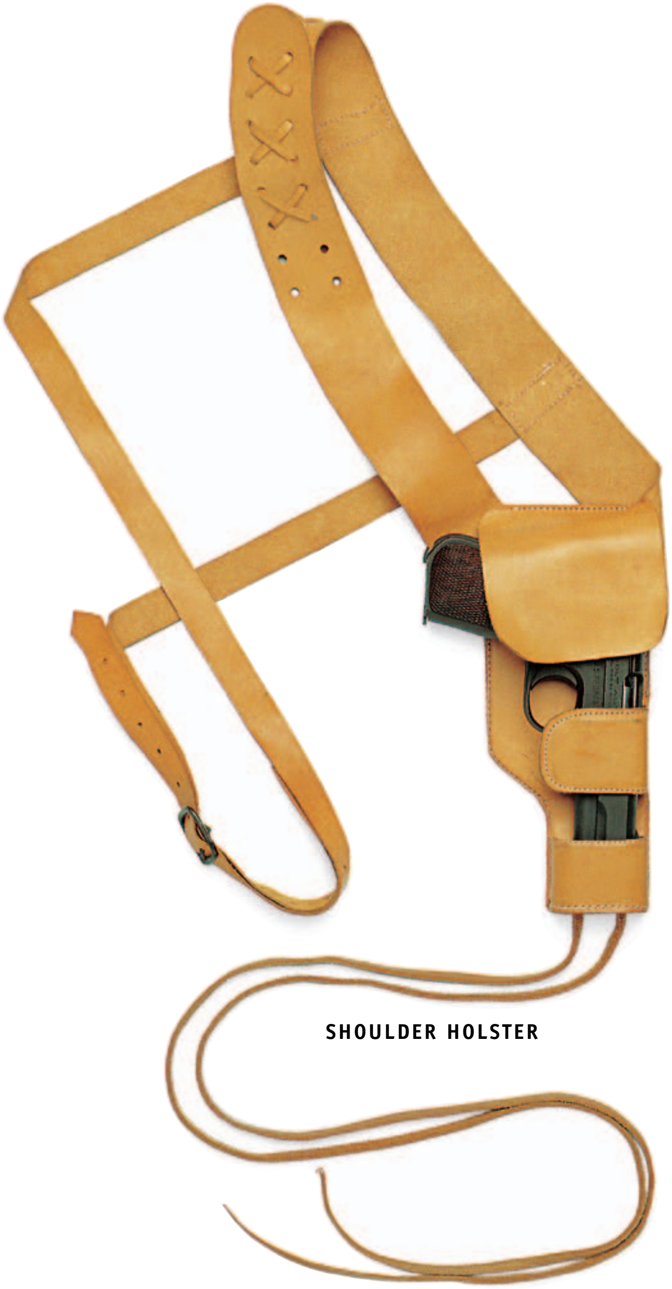
H. KEITH MELTON

Forewords by **Richard Helms**, former Director of the CIA, and **Markus Wolf**, former Head of the East German Foreign Intelligence Service, the HVA

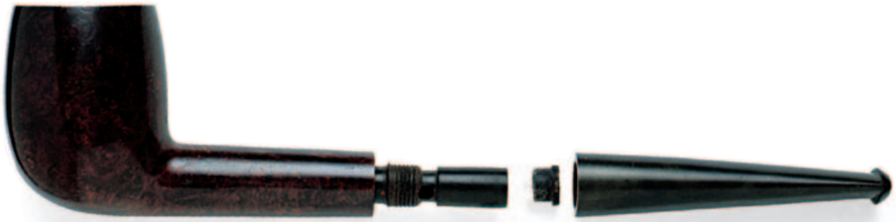


EXPANDED & UPDATED EDITION

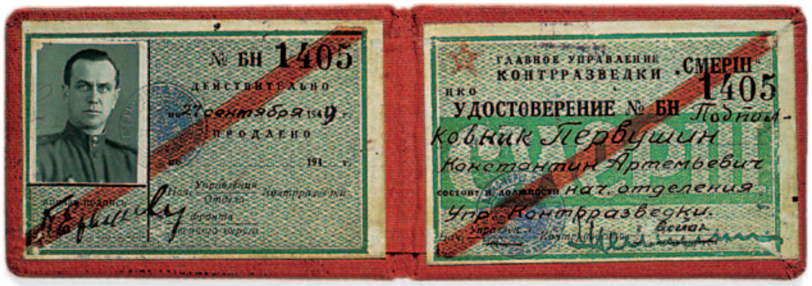
ULTIMATE SPY



SHOULDER HOLSTER



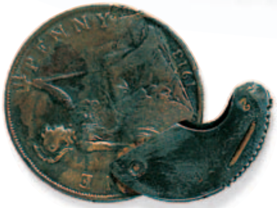
PIPE WITH CONCEALMENTS



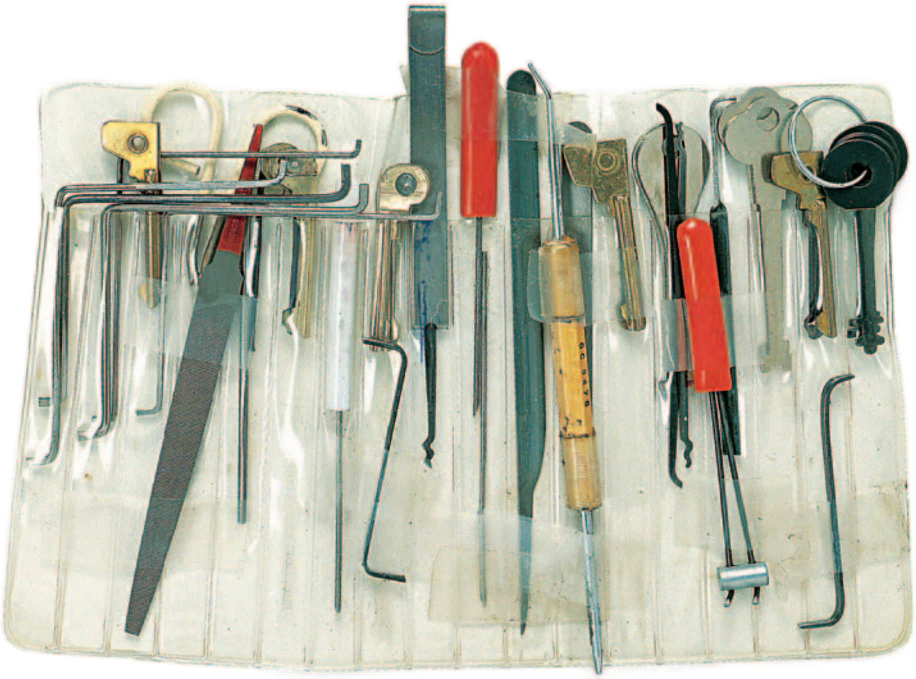
№ БН 1405
ДЕЙСТВИТЕЛЬНО
по 27 сентября 1949 г.
ПРОДЛЕНО
по 194 г.
Нач. Управления Отдела Контрразведки фронта военного округа
Личная подпись

ГЛАВНОЕ УПРАВЛЕНИЕ КОНТРРАЗВЕДКИ «СМЕРШ» НКО
1405
УДОСТОВЕРЕНИЕ № БН Подполковник Первушин
Константин Артемьевич
состоит в должности нач. отделения
Упр. Контрразведки.
Нач. Управления Контрразведки военн.

SMERSH CREDENTIALS



COIN WITH BLADE



SURREPTITIOUS ENTRY KIT

DEAD DROP SPIKE

ULTIMATE SPY

WRISTWATCH MICROPHONE

H. Keith Melton

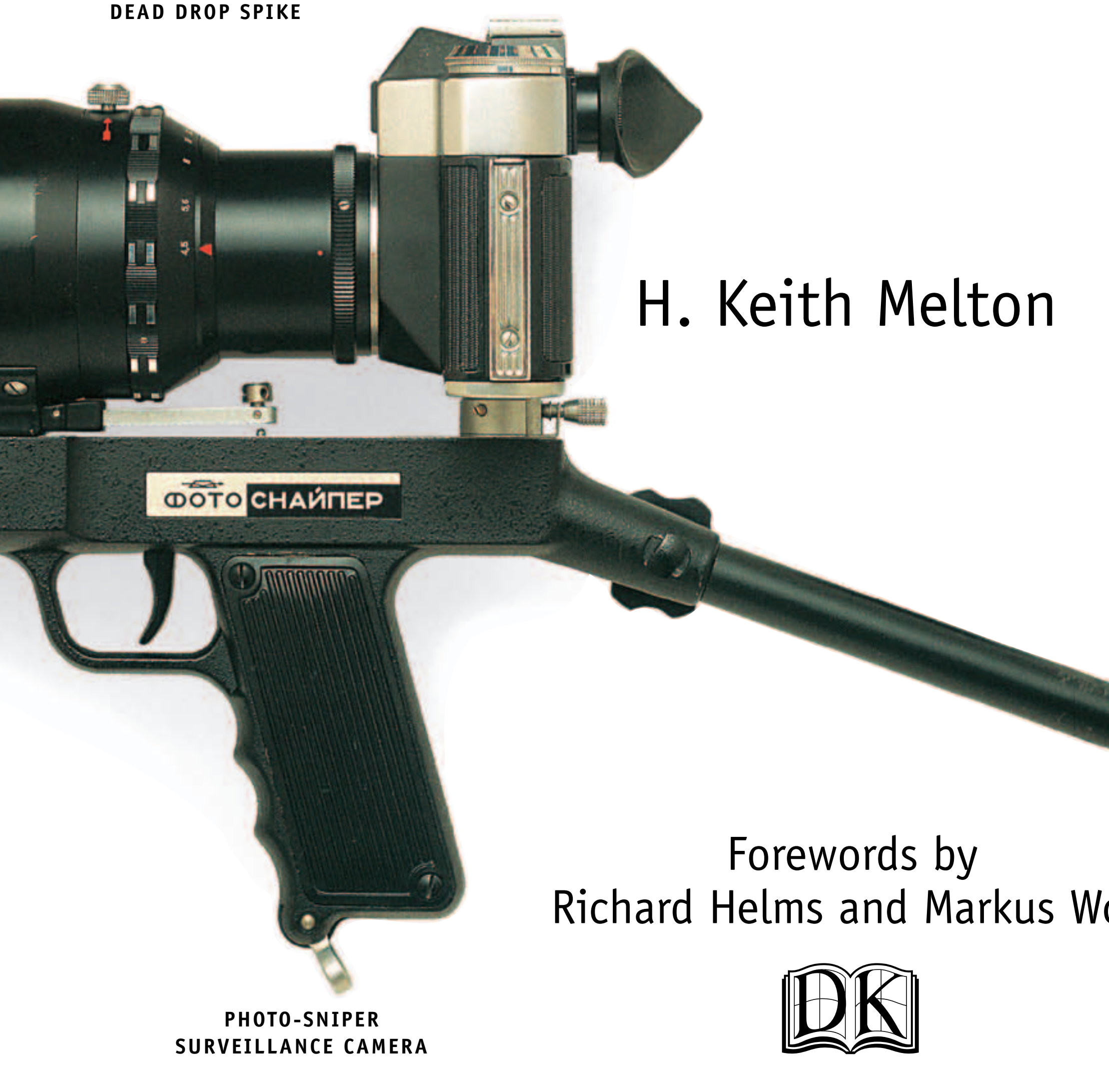


PHOTO-SNIPER SURVEILLANCE CAMERA

Forewords by
Richard Helms and Markus Wolf

DK

LONDON, NEW YORK, MUNICH, MELBOURNE, DELHI

THIRD EDITION
Project Editor Patrick Newman **Project Art Editor** Adam Walker
Editorial Assistance Manisha Thakkar
Managing Editors Camilla Hallinan, Debra Wolter **Managing Art Editor** Karen Self
Picture Research Ria Jones **Production** Luca Frassinetti

DK INDIA
Head of Publishing Aparna Sharma **Design Manager** Arunesh Talapatra
Designers Mini Dhawan, Govind Mittal **DTP Coordinator** Sunil Sharma

SECOND EDITION
Project Editor Jolyon Goddard **Editorial Assistance** Janet Mohun, Teresa Pritlove
Project Art Editor Sara Freeman **DTP Designer** Julian Dams
Editorial Manager Andrea Bagg **Senior Managing Editor** Martyn Page
Managing Art Editor Louise Dick
Picture Research Anna Grapes **Production** Louise Daly

FIRST EDITION
Project Editor Louise Tucker **Editor** Nicholas Turpin **Consultant Editors** Paul Cornish, Hayden B. Peake
Senior Editor Edward Bunting **Project Art Editor** Clare Shedden **Designer** Christina Betts
Managing Editor Martyn Page **Managing Art Editors** Philip Gilderdale, Bryn Walls
Senior Managing Editors Ruth Midgley, Josie Buchanan, Krystyna Mayer
Senior Managing Art Editor Lynne Brown
Production Alison Jones **Picture Research** Anna Lord

First published in the United States in 1996
This edition published in 2009 by
DK Publishing
375 Hudson Street
New York, New York 10014

09 10 11 12 10 9 8 7 6 5 4 3 2 1

UD166 – September 2009

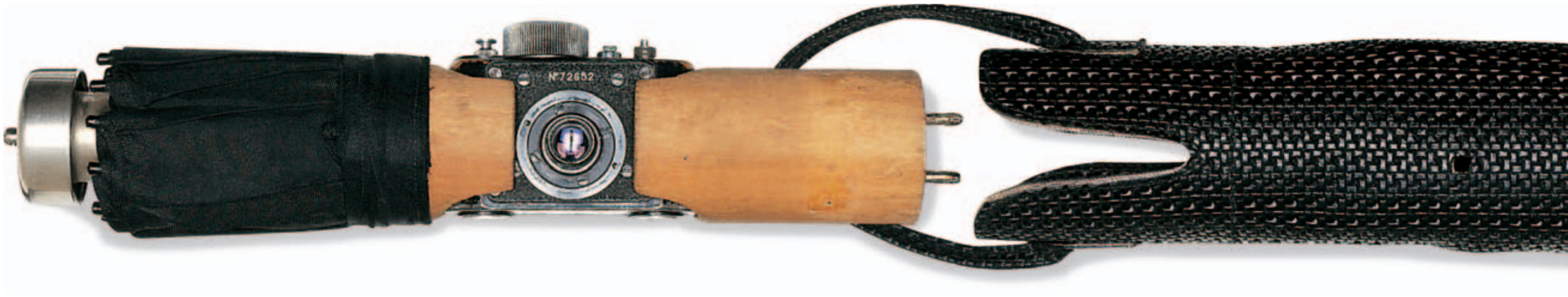
Published in Great Britain by Dorling Kindersley Limited.

A catalog record for this book is available from the Library of Congress
ISBN 978-0-7566-5576-1

Color reproduction by Colourscan, Singapore
Printed and bound in Hong Kong by Hung Hing

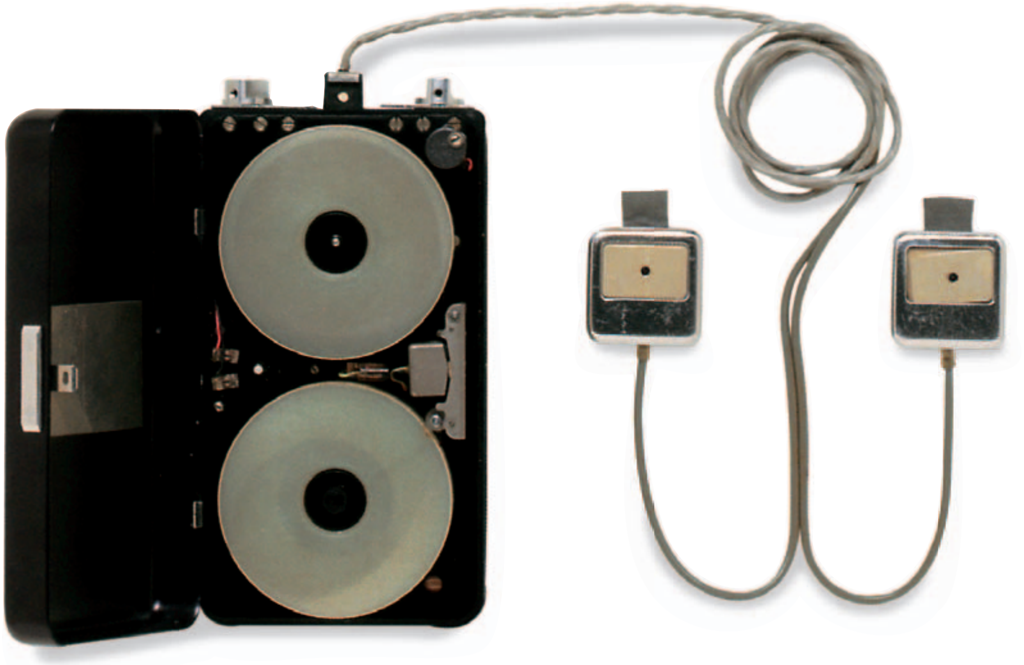
Discover more at
www.dk.com

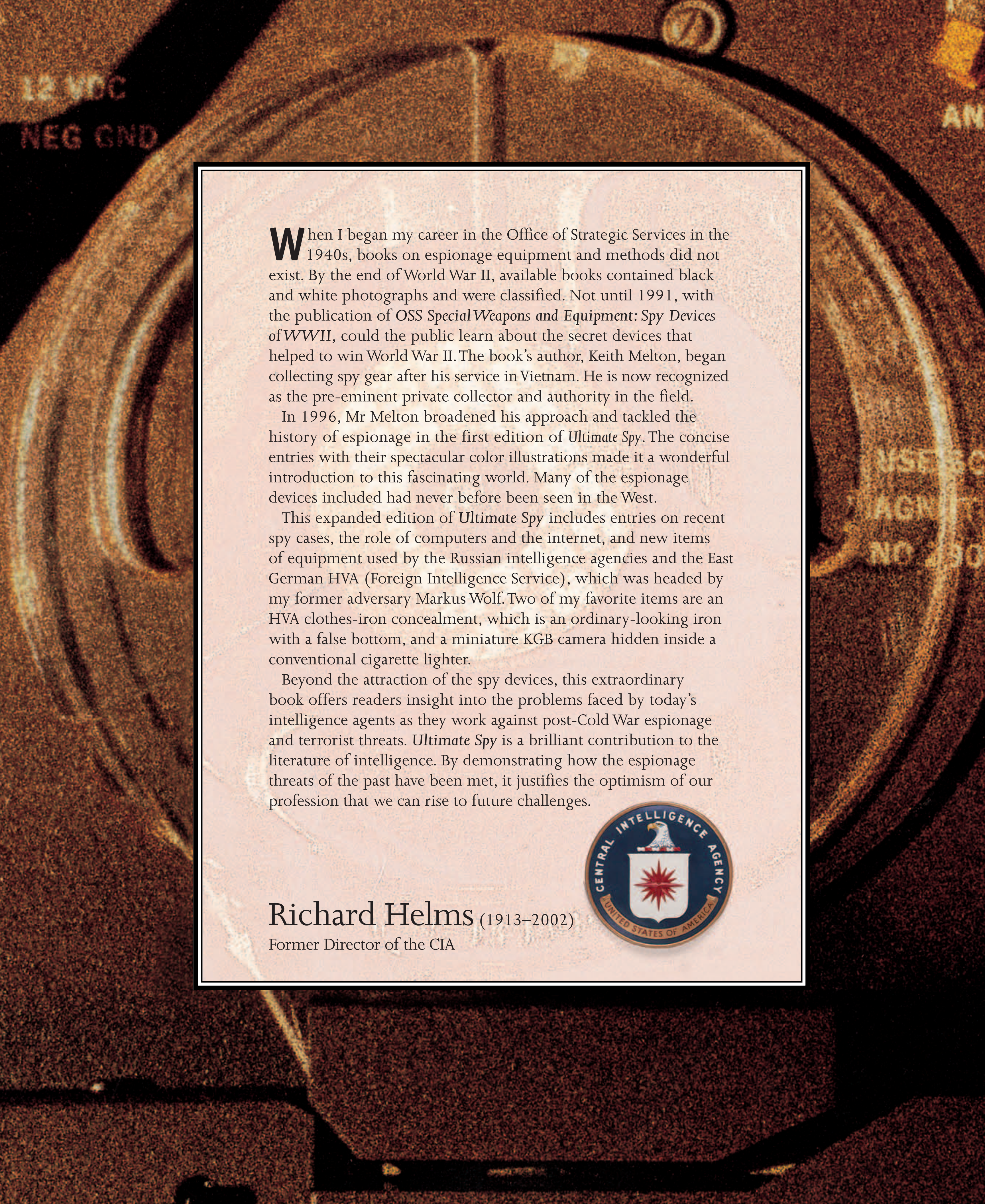
Contents



EQUIPMENT AND TECHNIQUES 76

HOW TO BE A SPY 200





When I began my career in the Office of Strategic Services in the 1940s, books on espionage equipment and methods did not exist. By the end of World War II, available books contained black and white photographs and were classified. Not until 1991, with the publication of *OSS Special Weapons and Equipment: Spy Devices of WWII*, could the public learn about the secret devices that helped to win World War II. The book's author, Keith Melton, began collecting spy gear after his service in Vietnam. He is now recognized as the pre-eminent private collector and authority in the field.

In 1996, Mr Melton broadened his approach and tackled the history of espionage in the first edition of *Ultimate Spy*. The concise entries with their spectacular color illustrations made it a wonderful introduction to this fascinating world. Many of the espionage devices included had never before been seen in the West.

This expanded edition of *Ultimate Spy* includes entries on recent spy cases, the role of computers and the internet, and new items of equipment used by the Russian intelligence agencies and the East German HVA (Foreign Intelligence Service), which was headed by my former adversary Markus Wolf. Two of my favorite items are an HVA clothes-iron concealment, which is an ordinary-looking iron with a false bottom, and a miniature KGB camera hidden inside a conventional cigarette lighter.

Beyond the attraction of the spy devices, this extraordinary book offers readers insight into the problems faced by today's intelligence agents as they work against post-Cold War espionage and terrorist threats. *Ultimate Spy* is a brilliant contribution to the literature of intelligence. By demonstrating how the espionage threats of the past have been met, it justifies the optimism of our profession that we can rise to future challenges.

Richard Helms (1913–2002)
Former Director of the CIA

In *The Art of War* (c. 400 BCE), Sun-Tzu advised his political and military masters that success follows sound decisions based on the foreknowledge that comes from well placed spies and not from oracles, psychics, or astrological calculations. Much has changed since those words were written, but their accuracy has been validated by over 2,000 years of experience. During the Cold War, despite technological advances, intelligence agencies relied heavily on human sources to achieve the advantage of foreknowledge.

Until the collapse of the Soviet Union and its allied governments in Europe, the question of how agents collected their secrets was largely a matter of conjecture left mainly to journalists, novelists, and film makers. But then the first edition of *Ultimate Spy* appeared. I and many members of the former East German Foreign Intelligence Service, the HVA, were surprised to discover a book that included elegant photographs of spy equipment, from Keith Melton's unique collection, and accurate descriptions of clandestine techniques that we had spent our careers keeping secret from Western intelligence agencies. This new edition shows many new items of equipment and brings us up to date with post-Cold War intelligence activities.

I am pleased to make this small contribution to a book that describes significant cases and illuminates the history of the equipment and methods used by spies. It is important for everyone to know how intelligence services and agents function and to understand that as the technology changes, the basic methods of espionage remain the same. Providing the foreknowledge to keep nations secure in this time of increased international terrorist threats is in large part the responsibility of intelligence and security services. This book helps make clear how they go about it.

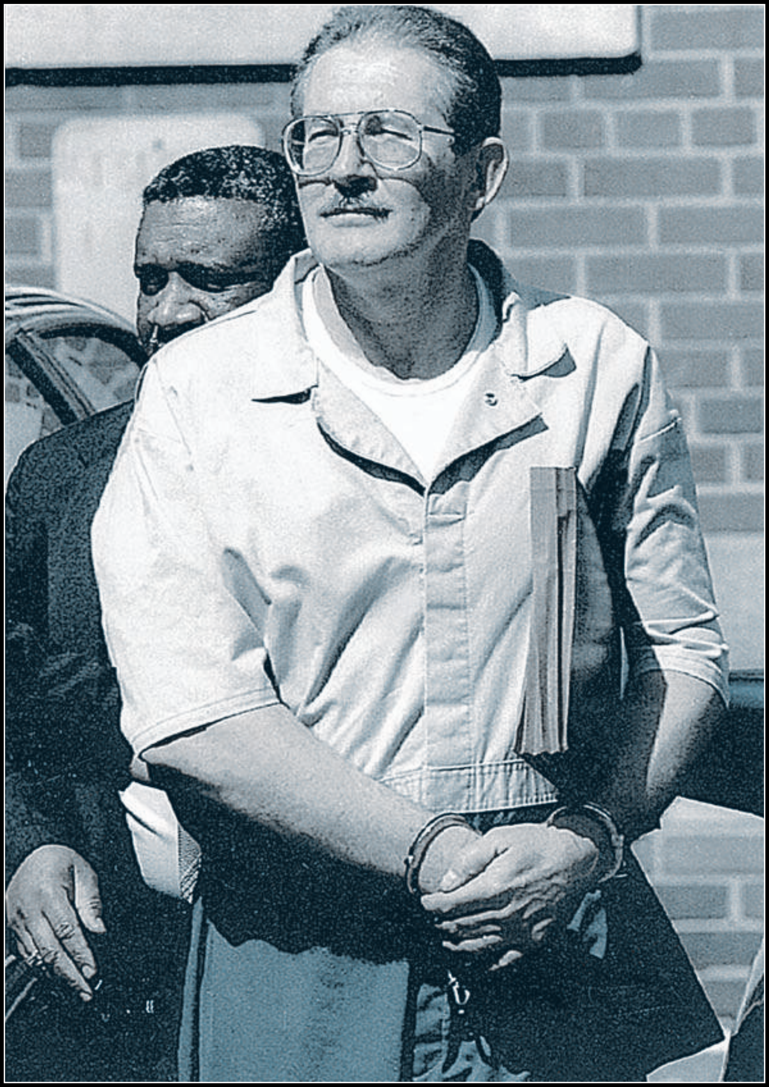
Markus Wolf (1923–2006)

Former Head of the East German Foreign Intelligence Service, the HVA

WHO SPIES?

THE SPECIFIC ACT of gathering information from an enemy is rarely carried out by an intelligence officer in person. To accomplish this task, intelligence officers recruit agents who, perhaps by virtue of their position, have access to the information required. Officers who recruit and handle agents are known as case officers. Most work from an embassy under some form of official cover (see p. 206) and are protected legally by diplomatic immunity. Others may operate without diplomatic immunity, perhaps living under an assumed identity. When recruiting agents, case officers are guided by the factors most likely to motivate people to become spies. These can be summed up by the acronym MICE—Money, Ideology, Compromise, and Ego.

CIA infrared receiver
This small device was plugged into an electrical socket and controlled remotely to trigger a hidden surveillance camera.

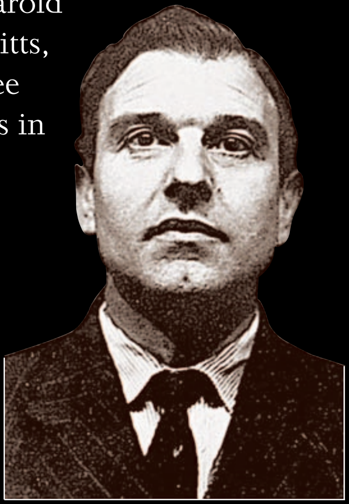


Aldrich Ames
Ames voluntarily became a KGB mole and revealed CIA secrets to the Soviets in exchange for $2.7 million. By his own account, he offered his services to pay off his debts and to finance his wife's spending habits.

M = MONEY

Financial problems, such as deep debt, are fertile ground for those who recruit agents. This has proved to be true in both capitalist and communist countries. Many Soviet intelligence officers were lured into spying for the West by the offer of a solution to money problems. The CIA (see p. 46) sometimes succeeded in targeting officers of the KGB's First Chief Directorate (see p. 50) who were unable to pay back operational funds that they had used personally.

The major KGB successes that have come to light in recent years were also achieved by exploiting greed. The most significant American agents in the history of the KGB and SVR (see p. 64), Aldrich Ames (see p. 202), John Walker, Jr. (see p. 54), Harold James Nicholson, Earl Edwin Pitts, and Robert Phillip Hanssen (see p. 66), all offered their services in return for financial reward.



George Blake
Inspired by communist ideology, Blake served the KGB as a mole within Britain's MI6 (see p. 203).

I = IDEOLOGY

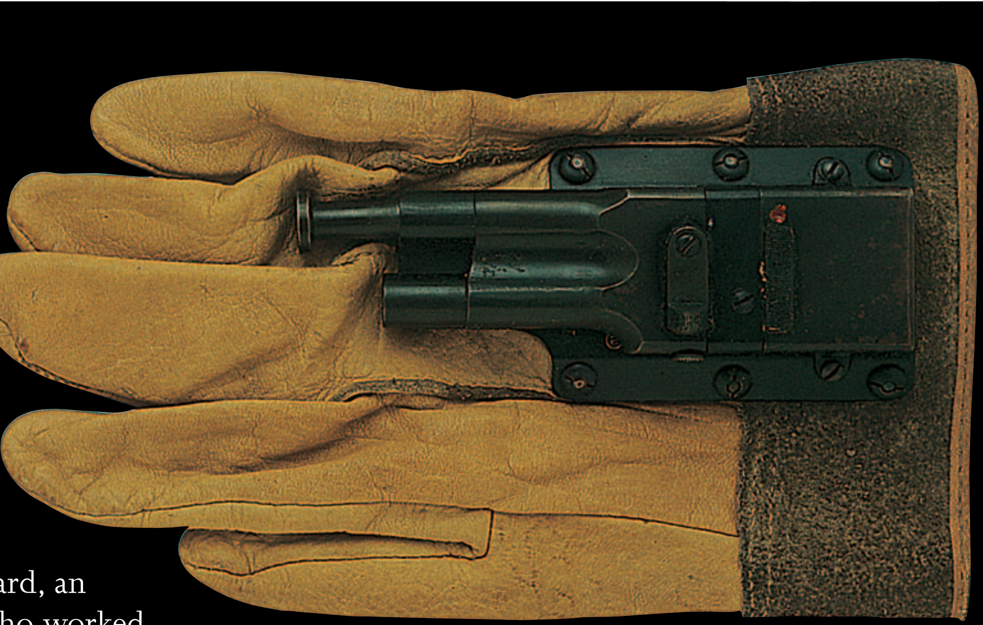
A person may alternatively be led into becoming an agent because of a belief in the ultimate superiority of the social and political institutions of a foreign country. During the 1930s in particular, the Soviet Union was able to recruit agents by exploiting the attraction that communism held for many in the West at that time. These included five idealistic students who were to become the Soviet Union's chief spies in Britain—Kim Philby, Anthony Blunt, Guy Burgess, Donald Maclean, and John Cairncross. Despite the decline of communism, ideology remains a factor in the recruitment of agents. Jonathan Pollard, an American citizen who worked at the US Naval Intelligence Support Center, initially agreed to spy for Israel out of an ideological commitment to the cause of Zionism. Like many others, however, his motivation was mixed—he was later to accept money for spying.

John Vassall
While working as a clerk at the UK embassy in Moscow, Vassall was compromised by his sexuality and recruited by the KGB.

C = COMPROMISE

A first step in recruitment by compromise is to identify an element in a potential agent's lifestyle that he or she would not wish others to know about. Homosexuals, for instance, at least in the immediate postwar decades, often risked ruin if their private lives were revealed. This made it possible for the KGB to recruit John Vassall when he was an embassy clerk in Moscow (see p. 204). In 1955 the Soviets carried out an intricate operation in which they set him up in an embarrassing situation, took photographs, and used these to blackmail and entrap him. Seven years later in London, Vassall was convicted of passing secrets to the Soviets between 1956 and 1962.

The KGB kept special hotel rooms in Moscow that were used for photographing visiting Westerners in compromising circumstances—with prostitutes, for instance. With pictures in hand, the KGB could usually blackmail its target individuals into becoming agents. Today, homosexuality and, of course, many heterosexual relationships, are no longer such effective means of coercion. On the other hand, financial and marital difficulties are still exploited with success.


Glove pistol
During World War II, the US Navy's Office of Naval Intelligence conceived this self-defense weapon for possible use by intelligence support and other administrative personnel who were stationed close to the front line.

E = EGO

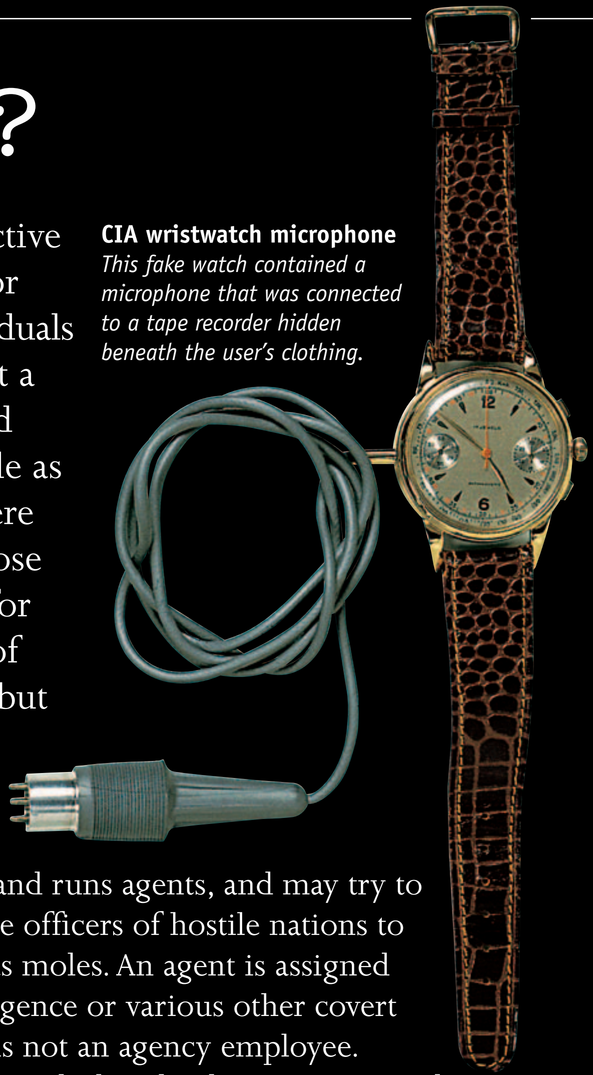
Case officers are often trained to appeal to the egos of candidates vulnerable to intellectual flattery in order to entrap them. Typically, a case officer might commission a candidate to write articles for publication. Initially they may be on safe, unclassified subjects. If asked, later, to write on subjects of a more sensitive nature, the writer may already be ensnared by the praise, money, and possibly the sense of adventure gained through previous efforts.

Hugh Hambleton was lured to the KGB by flattery and a sense of adventure (see p. 204). Despite an awareness of the risks involved, some subjects continue in the belief that they can outwit intelligence professionals.

Hugh Hambleton
The KGB used intellectual flattery to recruit Hambleton, an academic who later rose to the rank of professor.

WHAT DO SPIES DO?

THE PEOPLE WHO APPEAR IN THIS BOOK have all been active within the general field of intelligence, covert action, or special military operations. In a broad sense, these individuals can be brought together under the term "spies," but this is not a precise term. First, depending on one's point of view, the word may carry dishonorable overtones and be taken by some people as an insult. There are cases where this is appropriate. And yet there are other people working in this field—equally spies—on whose skills and strengths their country relies for its survival. Second, the fictional world of spying is one of action and excitement, but the reality is infinitely more discreet, professional, and subtle.



CIA wristwatch microphone
This fake watch contained a microphone that was connected to a tape recorder hidden beneath the user's clothing.

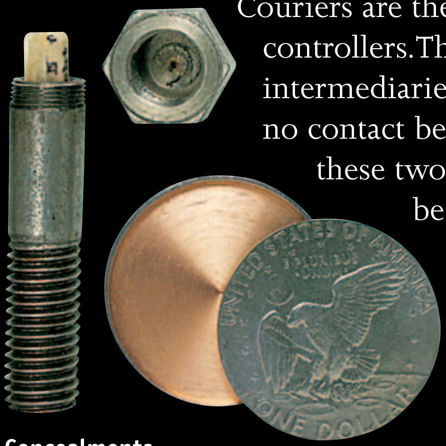
Maria Knuth
Knuth began her spy career in 1948 as a courier for Polish intelligence in West Berlin.

VARIETY OF ROLES

Those entering a career in special military operations must face the unglamorous aspects of military life, as in the other armed forces. The physical training is hard; so is the competition with others aiming to be selected for special duties. For those who are chosen, training will become much more diverse, since there are many different roles in today's special military forces, each requiring a course of specialized training.

There are many different roles, too, in the intelligence agencies. Similar roles, and similar structures, occur in each country. Typically, there is one agency for intelligence (the gathering of sensitive information), and one for counterintelligence (defense against enemy spies). An important distinction exists between officers, most of whom are career members of their agency, and agents, whose status varies with the country and the individual, and whether they are operating in war or in peacetime. A case officer is one who recruits and runs agents, and may try to encourage case officers of hostile nations to defect or act as moles. An agent is assigned tasks in intelligence or various other covert activities but is not an agency employee.

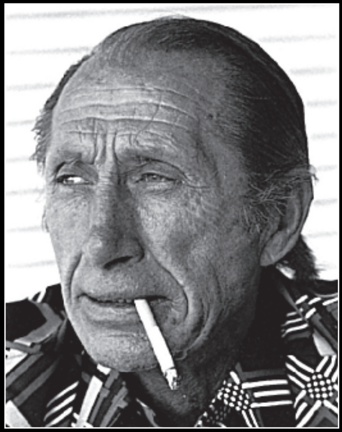
Some officers deal with administration and support, which generally accounts for about 25 percent of all agency staff. The other 75 percent are usually divided equally between analysis and operations, and what follows is a brief overview of some of their roles.



Concealments
Intelligence agencies often use ingenious adaptations of everyday objects as hiding places for secret information or equipment.

THE COURIER

Couriers are the links between the agents and their controllers. They sometimes also serve as cutouts: intermediaries who enable the system to work with no contact between sender and receiver. If neither of these two parties knows the other, they will be unable to betray one another. Some couriers work in embassies, collecting information from local agents. The Israeli agency Mossad makes use of couriers called *bodlim* to do this. Other couriers transport intelligence across international borders, sometimes in the guise of diplomatic couriers, as in the case of Alfred Frenzel (see p. 48).



Dusan Popov
German military intelligence (the Abwehr) approached Popov in 1940. He joined their organization but passed secrets to British intelligence. His double-agent codename was Tricycle.

A courier's task is often a dangerous one, as his or her fate is far less important than the information he or she carries. Some agencies have developed concealments that will self-destruct if anyone tampers with them. Although the destruction of the information will not save the courier from being incriminated, it may protect the identity of the agent who gathered it. Some agents begin their careers as couriers. An example is the Polish agent Maria Knuth (see p. 164), who started in 1948 as a courier in West Berlin, carrying secrets on microfilm.

THE DOUBLE AGENT

These are agents who turn against the intelligence service that originally recruited them and work for another agency, while at the same time making the original agency believe their loyalty has not changed. They may do this for ideological reasons, for personal gain, or to save their lives after being captured. Double agents are a dangerous threat to intelligence operations, as they can be used by their new controllers to feed misleading information to their original employers.

During World War II, Britain's MI5 (see p. 208) set up an organization known as the Twenty, the XX, or the Double Cross Committee. This body clandestinely controlled much of Germany's intelligence-gathering effort in Britain. It went so far as to set up a series of largely fraudulent "German" intelligence networks that reported to the Germans without arousing suspicion, but were in reality under the control of MI5.

Two of the most successful double agents actually volunteered their services to British intelligence during World War II. Dusan Popov (see p. 41) was a Yugoslav who ran a network of three double agents for MI5. He passed misleading intelligence to the German Abwehr. The other example was also a British agent in World War II—the Spaniard Juan Pujol, codenamed Garbo, who was so successful in deceiving the Germans on behalf of the Allies that he was decorated by both sides.

THE DEFECTOR

A defector is an intelligence officer who abandons his or her original agency and betrays it by giving information to a foreign intelligence service. Some defectors are motivated by ideology, while others act out of fear for their own safety. The latter was the case with Vladimir Petrov, a KGB officer in Australia. In 1954, facing allegations that he had been involved in a plot, he evaded recall to Moscow and turned himself over to the Australian authorities. As soon as they had

Fear of retribution
KGB officer Vladimir Petrov (1907–91, inset) defected from the Soviet embassy in Australia. Above, KGB men escort his wife Evdokia, a KGB code clerk, to a flight back to Moscow. Australian authorities freed the couple and granted them asylum.

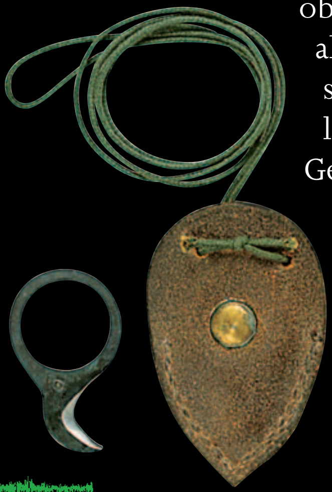
Supporting role
Odette Sansom served as a courier for an SOE circuit organizing sabotage in France.

abandoned the KGB, Vladimir Petrov and his wife were granted asylum in Australia, and in return gave valuable information on Soviet espionage activities in Australia. A more recent and dramatic defection was the escape from Moscow of Oleg Gordievsky, a KGB officer working for British intelligence (see p. 210). He realized that he was under suspicion, but evaded KGB surveillance. Gordievsky was smuggled out of the Soviet Union by MI6. But if not under suspicion, would-be defectors are often encouraged to remain in their intelligence service to work clandestinely as moles.

KGB defector Peter Deriaban was an example of a defector whose knowledge of his old agency proved useful long after he escaped. He served for years as an adviser to the CIA. In particular, he followed the organization and structure of the KGB and its officers, and lectured on the subject inside the agency.

THE SABOTEUR

The word "sabotage" is French in origin, and refers to the action of a disgruntled workman who destroys machinery by throwing a wooden clog (*sabot*) into it. The destruction of enemy equipment is a frequent objective of sabotage. But there are also more sophisticated forms of sabotage, such as the ingenious but largely ineffective attempt by the Germans in World War II to sabotage the British economy by flooding world markets with counterfeit English banknotes (see p. 34).



Tyre ripper and sheath
Saboteurs and special operations personnel used tire slashers to sabotage enemy vehicles.

It was in World War II that saboteurs were most regularly and effectively employed, especially by the British SOE (see p. 30) and American OSS (see p. 32). Both organizations sent teams of officers to assist local resistance groups in sabotage. Some of these personnel were trained in the various sabotage methods, others were needed for support roles. The latter was the case with Odette Sansom, who was sent to France by the SOE in 1942 as a courier. She was unwittingly revealed to the Gestapo by a captured member of the resistance and was arrested in 1943 (see p. 30).

THE MOLE

Moles are ostensibly employees of one intelligence service who are at the same time secretly working on behalf of a hostile agency. As such, they can be extremely valuable to the intelligence agency that runs them. Provided they have sufficiently high-level access,

Long-term undercover informer
CIA officer Larry Wu Tai Chin (b.1918) was a mole for Chinese intelligence, supplying secret information from the early 1950s until his suicide in 1986.

they will be able to supply information on many aspects of their employers' work. People have a variety of motives for becoming moles. Some may do so for ideological reasons, others because of the lure of money. Whatever the case, the double life that they lead is one of extreme stress, often causing such personal problems as alcoholism or irresponsibility with money.

The CIA has suffered at least two major penetrations by moles. In one instance, Larry Wu Tai Chin joined the CIA in 1952 and, from early in the 1950s until his death by suicide in 1986, he secretly worked for Chinese intelligence. A recent and well-publicized example of a mole was CIA officer Aldrich Ames (see p. 202), who offered his services to the KGB in return for money. From 1985 until he was arrested in 1994, he sold a vast number of secrets to the Soviet Union.

Ring concealment
This British World War II ring was used to conceal microdots and microfilm.

THE ANALYST

The information gathered by espionage and technical means forms only a small part of the material that needs to be evaluated by intelligence services. Much of the vast quantity of information that passes through their hands is acquired from publicly available sources. Analysts have the task of combining these diverse elements of intelligence into their written reports and digests. Their output is a potentially valuable aid for military and political decision-makers.

The role of the analyst is unglamorous compared with that of spies who take part in operations, and analysts seldom come to the notice of the public. Without them to provide a usable end product, however, espionage would be much less effective than it actually is. With the current rapid development of digital information technology (see p. 212), the analysts' role is becoming ever more important.

Walther PPK
Easy to conceal, this reliable weapon is commonly adopted for self-protection by personnel in a number of intelligence agencies.

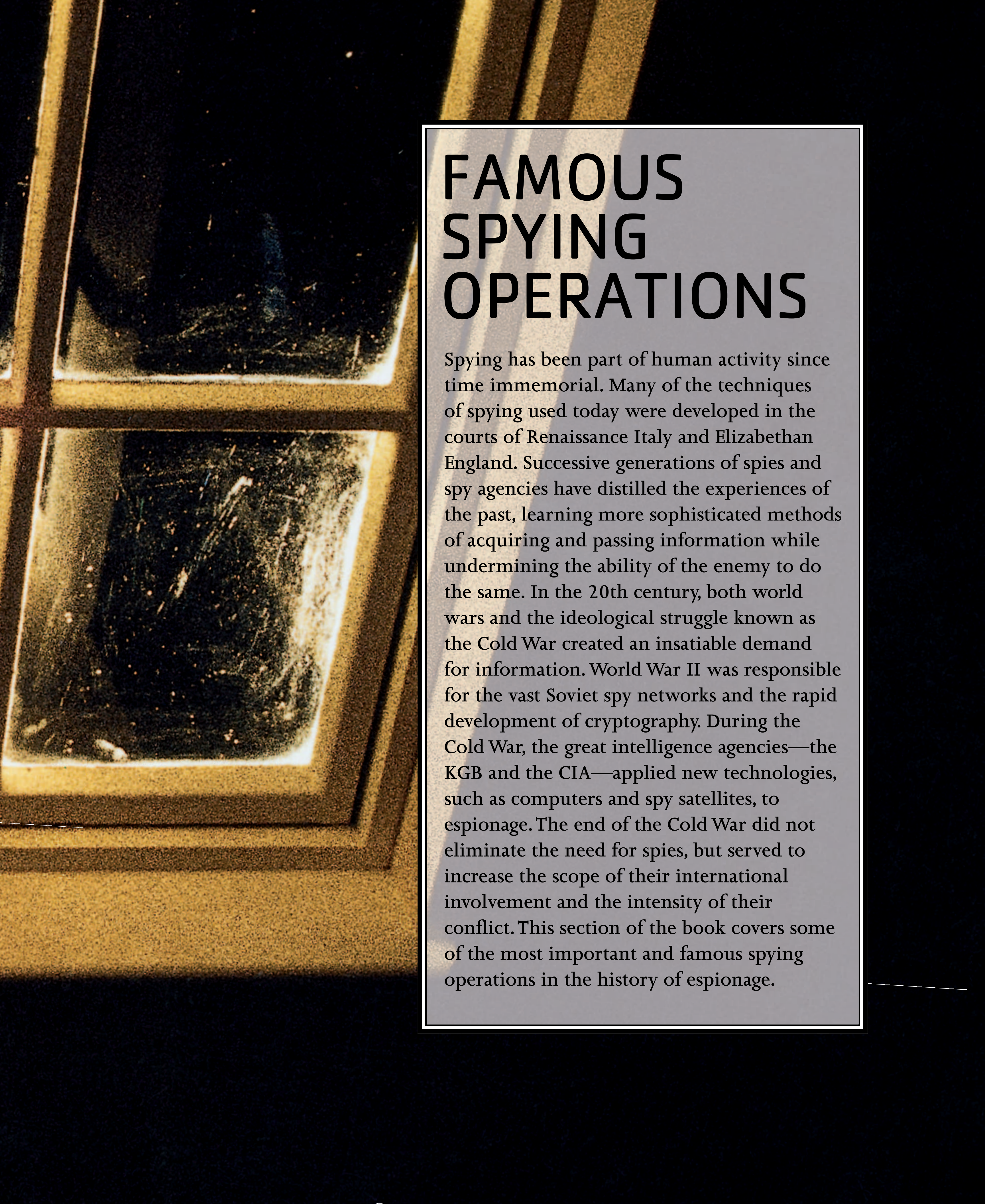
THE ASSASSIN

Assassins take their name from a medieval Muslim sect that exerted its power by murdering the leaders of those who opposed it. The role of the intelligence service assassin is essentially the same. Contrary to common belief, assassinations are not frequently carried out by spies. US Senate hearings in 1976 established that the CIA had never actually participated in the murder of a foreign leader, despite some abortive plans to that end. The CIA is now prohibited by executive order from taking part in assassinations.

By contrast, the intelligence services of the Soviet Union made effective use of assassination to liquidate political enemies. As early as the 1930s they created a special laboratory, the kamera, to develop poisons and other assassination tools. Their most prominent victim was Trotsky, one of the founders of the communist state, who was killed in 1940 on the orders of his rival, Stalin (see p. 26).

Later killings included those of two Ukrainian nationalist exiles in Munich by the KGB. These were carried out in 1957 and 1959 by a KGB officer named Bogdan Stashinsky. The device he used was hidden in a rolled-up newspaper and sprayed poison gas in the victim's face, causing death within seconds. At first, there was no suspicion of foul play: even after the autopsy had been performed. Stashinsky revealed all when he defected to West Germany in 1961 (see p. 194).

Assignment in Munich
While serving as a KGB officer, Bogdan Stashinsky assassinated two Ukrainian nationalists.



FAMOUS SPYING OPERATIONS

Spying has been part of human activity since time immemorial. Many of the techniques of spying used today were developed in the courts of Renaissance Italy and Elizabethan England. Successive generations of spies and spy agencies have distilled the experiences of the past, learning more sophisticated methods of acquiring and passing information while undermining the ability of the enemy to do the same. In the 20th century, both world wars and the ideological struggle known as the Cold War created an insatiable demand for information. World War II was responsible for the vast Soviet spy networks and the rapid development of cryptography. During the Cold War, the great intelligence agencies—the KGB and the CIA—applied new technologies, such as computers and spy satellites, to espionage. The end of the Cold War did not eliminate the need for spies, but served to increase the scope of their international involvement and the intensity of their conflict. This section of the book covers some of the most important and famous spying operations in the history of espionage.

EARLY ESPIONAGE

Pinkerton's National Detective Agency
"WE NEVER SLEEP."

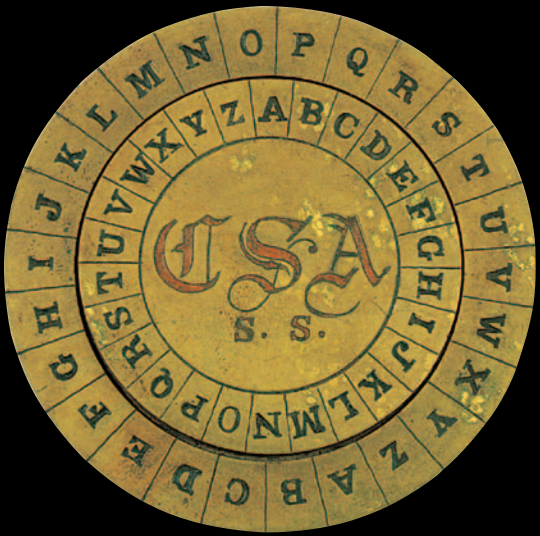
Emblem of the Pinkerton Agency
Allan Pinkerton, founder of Pinkerton's National Detective Agency, headed "Pinkerton's Secret Service," which was active in spying for the North during the Civil War (see p. 20).

RULERS AND MILITARY LEADERS have always needed to know the strengths, weaknesses, and intentions of their enemies. Consequently, the trade of spying is as old as civilization itself. Around 400 BCE, the ancient Chinese strategist Sun Tzu wrote about the importance of intelligence and espionage networks in his classic book, *The Art of War*. The Bible contains more than a hundred references to spies and intelligence-gathering. Most of the elements of modern espionage, however, originate in 15th- and 16th-century Europe.

Cardinal Richelieu
Richelieu, chief minister to King Louis XIII of France, created the Cabinet Noir intelligence service.

SPIES AT COURT

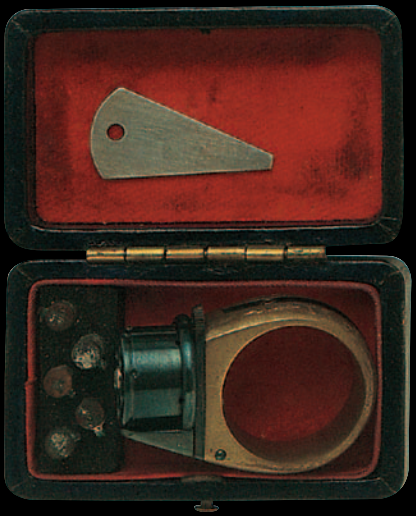
The political, philosophical, and cultural changes of this period fostered the development of intelligence-gathering. During the 15th century, the principles of polyalphabetic ciphers were laid down; these principles were still in use in the early 20th century (see p. 154). During the 16th and 17th centuries, the European courts became centers of intrigue as rulers strove to maintain their hold on and increase their power. The ambassadorial system of diplomacy was established, and ambassadors were expected to combine their official diplomatic duties with espionage and subversion. Intelligence services were created and used to great effect by such powerful men as Cardinal Richelieu in France (see p. 19) and Sir Francis Walsingham in England (see p. 18).



Confederate cipher disc
This substitution disk, which is made of brass, is a type of cipher wheel (see p. 154). It was used by the Signal Service of the Confederacy for secret communications during the Civil War.

THE CIVIL WAR

By the time of the Civil War (1861–65), a number of technological advances, such as the invention of photography, had occurred that changed the methods used to gather and communicate intelligence. The Confederacy may have even used an early form of microphotography. Telegraphy was used for the

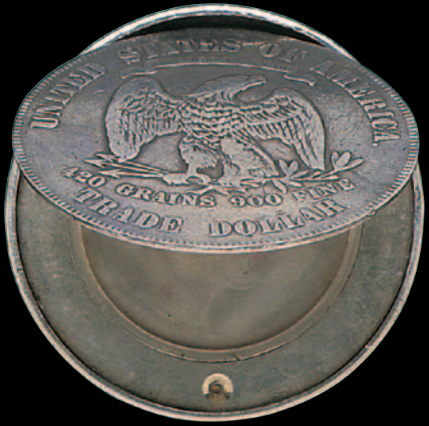


Ring revolver
This tiny five-shot weapon, shown with its case and ammunition, was sold under the brand name Le Petit Guardian. *It was made in late-19th-century France.*

first time in a major war for military communications, in spite of its vulnerability to interception. Aerial photography was also done, from hydrogen balloons (see p. 21).

WORLD WAR I

Early in World War I (1914–18), human spies were seen as the main threat by the public on both sides of the conflict. But it was signals intelligence that was to prove far more decisive, and indeed it attained a greater importance than in any previous war. For instance, British Admiralty cipher experts decoded a top-secret German government telegram offering Mexico an offensive alliance against the United States. By subtle use of this discovery, Britain helped to bring the US into the war on the Allied side (see p. 22). In the US, a cryptology section for military intelligence had been created under Herbert Yardley (see p. 22).

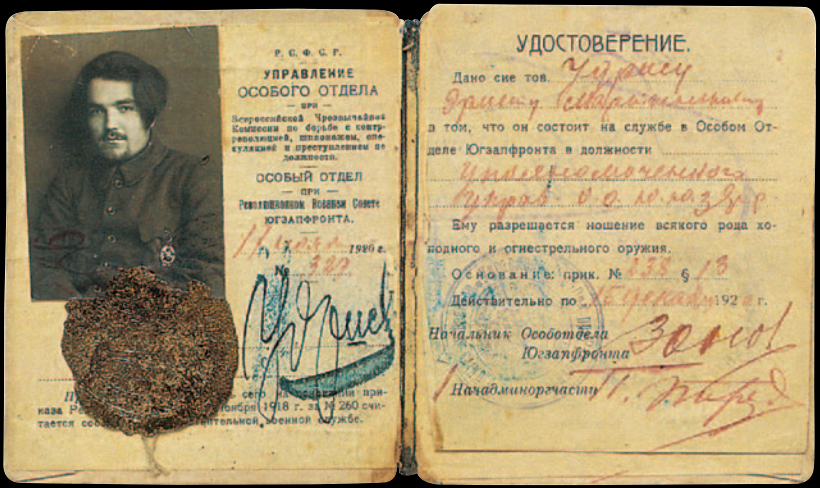


Silver dollar concealment
This 19th-century silver dollar could be used to conceal secret messages. The side with the eagle was hinged, and opened when pressed at a point near the rim.

Cheka badge
The Cheka replaced the Okhrana, the old security service of the Czarist regime.

CHANGES IN RUSSIA

Russia's participation in World War I led to the seizing of power by the Bolshevik Party after the 1917 revolution. The party created its own secret police, the Cheka (see p. 25), which conducted a ruthless offensive—the Red Terror—against opponents of Bolshevism. Once bolshevik power was established, the Cheka extended its activities to foreign countries. After the formation of the Soviet Union in 1923, the Cheka's responsibilities were taken on by various organizations, including the NKVD, which became the KGB in 1954.



Р. С. Ф. С. Р.

УПРАВЛЕНИЕ
ОСОБОГО ОТДЕЛА
— при —
Всероссийской Чрезвычайной Комиссии по борьбе с контрреволюцией, шпионажем, спекуляцией и преступлением по должности.

ОСОБЫЙ ОТДЕЛ
— при —
Революционном Военном Совете
ЮГЗАПФРОНТА.

17 [illegible] 1920 г.
№ 327

П[illegible] сего [illegible] при-каза Ре[illegible] ноября 1918 г. за № 260 считается со[illegible]ительной военной службе.

УДОСТОВЕРЕНИЕ.

Дано сие тов. [illegible]
[illegible]
в том, что он состоит на службе в Особом Отделе Югзапфронта в должности
Уполномоченного
[illegible]

Ему разрешается ношение всякого рода холодного и огнестрельного оружия.

Основание: прик. № 338 § 13

Действительно по 15 декабря 192 г.

Начальник Особотдела
Югзапфронта Зорин

Начадминоргчасти Г. [illegible]

Cheka credentials
The Cheka was founded in 1917. Its name is the Russian-language abbreviation for "Extraordinary Commission for the Struggle against Counter-revolution, Espionage, Speculation, and Sabotage."

Court intrigues

SEVERAL IMPORTANT FEATURES of modern espionage had their origins in the Renaissance, the cultural movement of rebirth and modernization that spread through Europe in the 15th and 16th centuries. In the arts and sciences a new, enlightened age began. But in public life dynamic changes were taking place, and bitter struggles for power and religious authority gave new scope for court intrigue and treachery. This was the world observed by writer Niccolò Machiavelli and dominated by a new class of politicians such as Cesare Borgia (1475–1507).

CESARE BORGIA

By a combination of deceit, charm, and aggression, Cesare Borgia carved out a kingdom for himself in central Italy. Other rulers of the period were just as much in tune with the new political spirit of the age. In the prevailing climate of mistrust, the growing craft of espionage could hardly fail to flourish.

The tools of the trade were already being developed. Impressively complex polyalphabetic ciphers were devised in the late 15th century by two scholars, Leon Battista Alberti and Johannes Trithemius. Others, such as Giovanni Soro in Venice, contributed significantly to the science of cryptography (the study of codes and ciphers).

The Renaissance also saw the emergence of the modern nation-state, and it was at the courts of such states that the most important developments in espionage took place. By the second half of the 16th century, states such as France, England, and Spain had set up official structures for the gathering of political and military intelligence at home and abroad. Ministers of state and diplomats were made responsible for gathering intelligence, and ambassadors abroad were expected to combine their official duties with espionage as a matter of course.

Elizabethan intrigues

An effective intelligence service was maintained in England during the reign of Queen Elizabeth I (1533–1603). As a Protestant nation with a weak army, England was constantly threatened by the Catholic powers, France and Spain. War with either could have proved a disaster for England, so intelligence about their intentions was vital.

Elizabeth herself was unmarried and childless, and there were several foreign princes who wanted to marry her and so gain the throne. Within England, too, she had Catholic opponents who wished to overthrow her and replace her with a Catholic monarch. The security of the Protestant state depended on protecting the queen from such dangers. In 1573, Sir Francis Walsingham (1537–90) was appointed secretary of state. By skillful use of espionage and counterespionage, he was able to defeat a number of plots aimed at the overthrow of Elizabeth and the restoration of Roman Catholicism.

One possible heir to the English throne was Elizabeth's cousin Mary, Queen of Scots. A Catholic, she featured in many political intrigues of the reign, such as the Babington Plot of 1586. This aimed to release Mary, who had been imprisoned in England after being forced to flee Scotland. The principal elements of the highly ambitious plot were an

MACHIAVELLIAN MIND

Niccolò Machiavelli (1469–1527) was a scholar and writer with a particular interest in political philosophy. While serving as a diplomat for the Republic of Florence, Machiavelli met Cesare Borgia, whose great political subtlety and extreme cunning he later wrote about as an example to other rulers. Machiavelli also wrote about the art of warfare, emphasizing the great usefulness of military intelligence.

CHRISTOPHER MARLOWE

SPY PROFILE

The English poet and playwright Christopher Marlowe (1564–93) was recruited into the secret service while studying at Cambridge University. In 1587, posing as a Catholic student, he entered a seminary at Rheims in France. Gaining the trust of the Jesuit students there, Marlowe learned details of various Jesuit plots in England. Marlowe's death in a brawl in London, England is believed by many to have been linked to his shadowy secret service work.

Queen Elizabeth I
The motifs decorating the Queen's dress in this portrait are emblematic of various aspects of her power. The eyes and ears (inset) symbolize the activities of her secret service.

uprising of the Catholics of England, invasion by an army financed by Spain and the Pope, and the assassination of Queen Elizabeth herself.

At the center of the conspiracy was John Ballard. A priest of the then-militant Catholic order the Jesuits, he was well known to Walsingham's staff. Ballard recruited Anthony Babington (b.1516), who had formerly acted as a messenger for Mary. Walsingham meanwhile used a double agent who gained the trust of the conspirators and soon learned how they communicated with Mary.

This correspondence was intercepted and deciphered by Thomas Phelippes (1556–1625), Walsingham's master cryptographer. It contained enough evidence to ensure the arrest and execution of the various plotters and even, on February 8, 1587, of Mary.

There were also threats from overseas to the security of the English state. King Philip II of Spain believed that it was his duty to restore England to the Catholic faith. Walsingham sent Anthony Standen to gather intelligence in Spain. Standen gained the assistance of the Florentine ambassador at Philip's court, and secured the help, too, of a Flemish courtier whose brother was a servant to the Grand Admiral of the Spanish fleet. In 1587 information from these sources alerted Walsingham to the great fleet, or Armada, being prepared for the invasion of England. Using his influence abroad, Walsingham secretly contrived to delay the loans Philip needed to finance his expedition. This gave the English time to prepare for the arrival of the Armada, which was duly defeated in 1588.

Richelieu and the Cabinet Noir

During the 17th century, the French court became a center of espionage activity. In the early years of the century, France suffered from an overly powerful nobility and from internal religious divisions. It was threatened externally as well, by the power of the Hapsburg family—the rulers of Spain, Austria, parts of Italy, and the Low Countries.

These difficulties were overcome by Cardinal Richelieu, chief minister to Louis XIII. Louis himself was an ineffective ruler, with the result that from 1624 to 1642 France was virtually run by Cardinal Richelieu. One of Richelieu's first acts after being appointed was to set up an intelligence service, known as the Cabinet Noir. This service monitored the activities of the French nobility by intercepting their correspondence.

Using the information gained in this way, Richelieu thwarted plots against the king and strove to establish the absolute power of the monarchy. His greatest successes were in frustrating plots devised by the king's brother, Gaston of Orleans, and the Marquis de Cinq Mars.

Cardinal Richelieu
Cardinal Armand Duplessis, Duke of Richelieu (1585–1642), used a national intelligence service to establish royal absolutism in France.

Richelieu also used agents abroad in support of his policy of weakening the Hapsburgs without involving France in costly wars. They subverted Spain, for example, by encouraging Portugal and Catalonia to rebel against Spanish rule.

The cardinal's machinations helped to bring Sweden into the Thirty Years' War (1618–48) against the Holy Roman Empire. With Germany paralyzed by this conflict, Richelieu was able to seize Alsace for France. By means such as this, his secret service helped to make France a powerful, absolutist nation-state.

American Civil War

DURING THE CIVIL WAR (1861–65), both the Union and the Confederacy were faced with the need for intelligence organizations. Some early attempts were of limited efficiency; but during the course of the war, intelligence-gathering methods improved. The ability of both sides to obtain information from each other was enhanced by the new technologies of the time. Photography, for instance, was exploited for espionage purposes, and an early form of microphotography may have been used.

Allan Pinkerton
Allan Pinkerton (left), head of the Union secret service, with President Abraham Lincoln (center) and General John McClernand (right).

Secret services

At the outbreak of the war, neither side had an established intelligence organization. Both the Union and the Confederate forces initially relied upon patriotic volunteers such as Rose O'Neal Greenhow for intelligence.

Union army commander General George McClellan set up a secret service early in the war, selecting a detective, Allan Pinkerton (1819–84), to be its head. Before the war Pinkerton had owned a detective agency, providing security for railroads. Pinkerton's detectives had limited success as spies, but they established a process of debriefing escaped slaves.

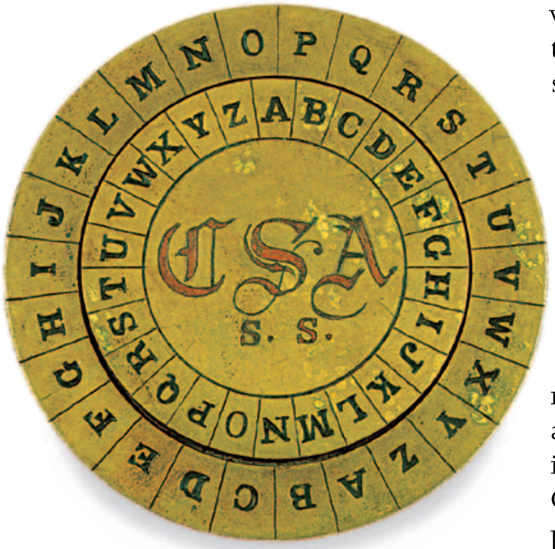
Conflict arose when another Union commander, General Winfield Scott, started his own security organization, led by Lafayette Baker (1826–68). Baker was less effective than Pinkerton, despite personally spying in the South, disguised as a photographer. Both Baker's and Pinkerton's men sought out Confederate spies operating in the Union capital of Washington, sometimes even arresting each other by mistake. Much more efficient and effective regional military intelligence operations were set up by Union commanders in the field, notably

Belle Boyd, "The Rebel Joan of Arc"
A flamboyant Southern patriot, Belle Boyd (1844–1900) achieved limited success as a spy and courier. After the war she romanticized her activities in a book and enjoyed a long career enacting her espionage work on the stage.

ROSE GREENHOW

SPY PROFILE

Rose O'Neal Greenhow (1817–64) was an accomplished Confederate agent. A society hostess in Washington, she set up a spy network just before the war began; using her charms, she obtained information from Union politicians and the military. The first battle of the Civil War—at Bull Run—was won by the Confederates aided by information supplied by Greenhow. Even when under house arrest, she continued to gather and pass on information.



Confederate cipher disk
Used to provide a substitution cipher for secret communications, this disk was adopted by the Confederate Signal Service Bureau in 1862.

that run for General Ulysses S. Grant by Colonel George H. Sharpe. In the South, Colonel Thomas Jordan and later Major William Norris ran an intelligence-gathering operation that obtained daily information by courier from the North. It was only toward the very end of the war—in 1865, when it was far too late to alter the outcome of the conflic—that an official Confederate secret service was set up.

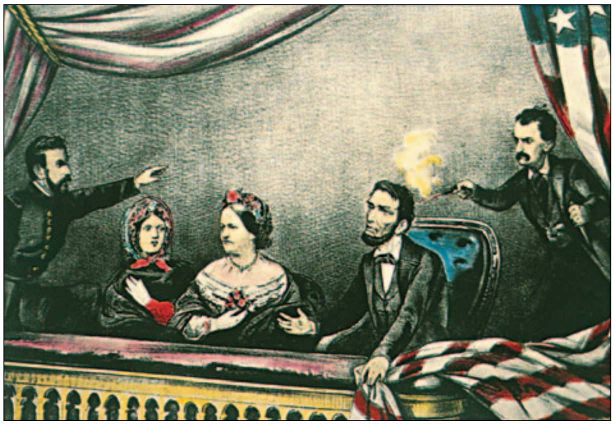
New technology

Several new methods of gathering intelligence were used in the war. Photography was so new that few commanders saw it as a threat. Photographers were allowed to take pictures of military defenses and camps, and both sides obtained information in this way. Confederate couriers photographically reduced messages so they could be hidden in metal buttons. Telegraphy was used for quick communication and both sides devised ciphers for secrecy. Aerial reconnaissance from tethered hydrogen balloons was developed during the war, but it was of limited use because the balloons could be shot down easily.

Doll with secret compartment
There was a great shortage of medicine in the South. Women and children carried medicine in the body of this doll through enemy lines.

THE PLOT TO ASSASSINATE PRESIDENT LINCOLN

In 1865, as the Civil War neared its end, the Confederate secret service devised several plots against Union leaders. Although these plots failed, some key conspirators continued to plot after the official Confederate surrender on April 9, 1865. The most ambitious of these plots was one to assassinate the Union president, Abraham Lincoln, the vice president, and the secretary of war. John Wilkes Booth, a famous actor, was selected to kill Lincoln, and he shot him in the head as he watched a play at Ford's Theater in Washington on April 14, 1865; the president died later. Booth escaped from the theater, but was later found and shot. A search of his possessions revealed a Confederate cipher device. In popular history Booth is generally considered to have acted alone in his assassination of Lincoln. But he definitely had connections with the Confederate secret service, and questions remain to this day about the group's role in the assassination.

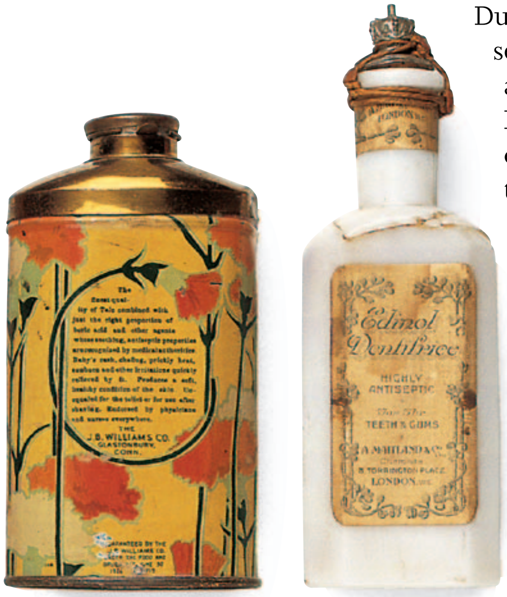


Abraham Lincoln
This picture shows President Lincoln being shot by Booth, as he sits in a box at Ford's Theater.

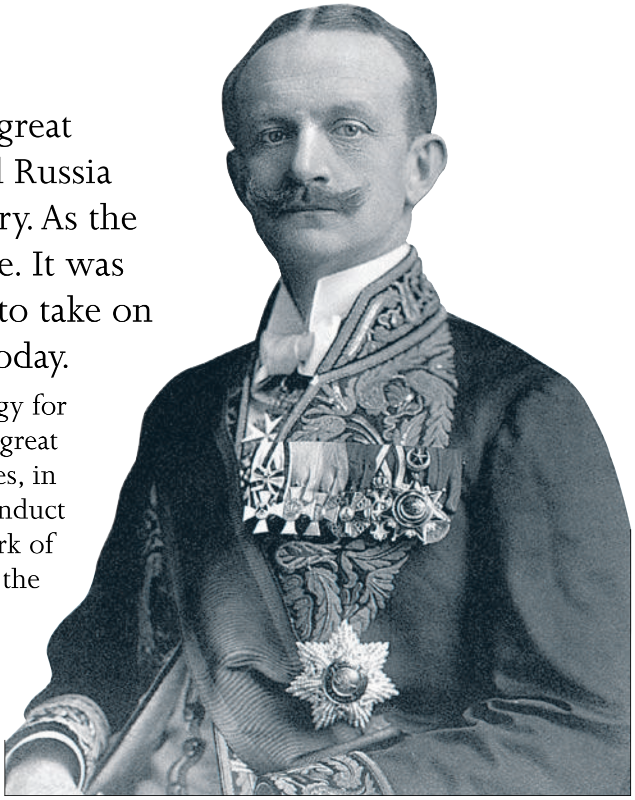
John Wilkes Booth
President Lincoln's assassin, actor John Wilkes Booth (1838–65), had also been involved in an earlier attempt to kidnap the president.

World War I

WORLD WAR I (1914–18) began as a struggle between the great European powers: the Triple Entente of France, Britain, and Russia against the Central Powers of Germany and Austria–Hungary. As the war progressed, more nations were drawn into the struggle. It was during this war that code-breaking (cryptography) began to take on the great importance that it has in intelligence-gathering today.



Concealments for invisible ink
This talcum powder can and dentifrice bottle, full of invisible ink, were seized from German spies captured by the British security service.



Count Johann Heinrich von Bernstorff
Germany's ambassador in Washington, DC during World War I, von Bernstorff (1862–1939) relayed the famous Zimmermann telegram to Mexico.

During the early 20th century, technology for sending long-distance messages made great advances. Telegraph and radio messages, in Morse code, were soon vital to the conduct of war. The intelligence-gathering work of the "agent on the ground," known in the trade as human intelligence, or HUMINT, was joined by a new craft, signals intelligence—later known as SIGINT. In addition to sending and receiving messages, it was now necessary to break the ciphers of enemy nations. Early in World War I, Russia had not learned the importance of this: the first German victory against Russia was the result of German signals intelligence intercepting Russian army signals that had been transmitted in unenciphered Morse code. Some other countries did establish special centers for deciphering messages. For example, the British set up Room 40 of naval intelligence, which was renowned for its deciphering skills.

The Zimmermann telegram

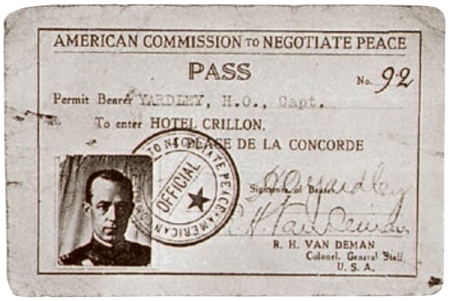
In 1917, German Foreign Minister Arthur Zimmermann (1864–1940) sent an encrypted telegram to Count von Bernstorff, Germany's ambassador in Washington, DC, saying Mexico was to be offered a war alliance with Germany against the United States. The count sent a modified version of the telegram to Mexico City, using the same cipher.

The telegram to Washington was intercepted and deciphered by British code-breakers. The British wanted to tell the Americans about the telegram, but did not want the Germans to know that their cipher had been broken. Admiral Hall, head of the Royal Navy's code-breaking organization, informed the US embassy in London about the telegram, and the embassy told Washington. The British suggested that Washington obtain a copy of the telegram sent to Mexico

HERBERT OSBORNE YARDLEY

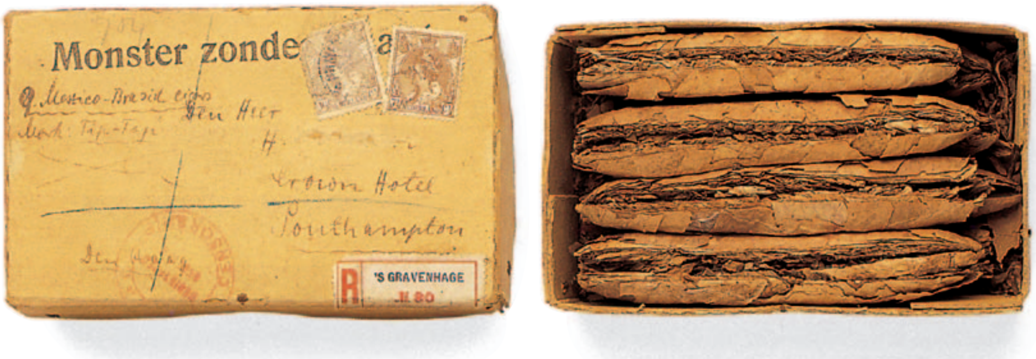
As a young man, the American Herbert Yardley (1889–1958) gained a reputation for his ability to break codes used by the US State Department, where he worked as an ordinary clerk. After the outbreak of World War I he was commissioned into the US Army and put in charge of the newly formed cryptography section of Military Intelligence (MI8). He devised new codes for use by the US Army and helped to convict a German spy whose secret message had been decoded by MI8.

After the war, Yardley established a permanent department, the American Black Chamber, to assist both the State Department and Military Intelligence with all code and cipher work. (For the difference between a code and a cipher, see the Glossary, p. 216.) Yardley's greatest success came when his cryptography group broke secret Japanese codes, which enabled the United States to gain significant advantages at the international naval disarmament conference of 1921.



AMERICAN COMMISSION TO NEGOTIATE PEACE
PASS
No. 92
Permit Bearer YARDLEY, H.O., Capt.
To enter HOTEL CRILLON.
PLACE DE LA CONCORDE
OFFICIAL ★ AMERICAN COMMISSION TO NEGOTIATE PEACE
Signature of Bearer
R. H. VAN DEMAN
Colonel, General Staff
U. S. A.

Peace conference credentials
Herbert Yardley led the cryptographic bureau of the US delegation at the 1919 Paris Peace Conference, after the end of World War I.



Suspect cigars

These cigars, sent to two Dutch spies who posed as cigar importers in Portsmouth, were slit open by the British in search of hidden messages.

from the Western Union Telegraph Company in Washington. That still encrypted copy was relayed to London where it was decoded, with the help of the British, at the US embassy.

The resulting translation was sent to Washington and leaked to *The New York Times*. The Germans believed that the Americans had obtained an already deciphered version of the telegram sent to Mexico City. This gave the Germans the impression that their cipher was still secure. They had no reason to suspect British involvement. Public indignation over the telegram quickly led to the entry of the United States into the war.

German spies

A fear of German spies spread through Britain and France at the outbreak of World War I. Although some spies were present in both countries, there were actually far fewer than imagined, and most were captured at the beginning of hostilities. One spy who succeeded in evading capture was Jules Silber. He operated in Britain, taking a job in the Office of Postal Censorship and passing censored information to the Germans.

Two Dutch agents who were sent to Portsmouth to spy for the Germans were not so successful. They pretended to be cigar importers and used their orders for cigars as codes for the ships they saw in Portsmouth harbor. These bogus orders were intercepted by the British postal censors, who became suspicious about the quantity of cigars ordered. The spies were captured and executed in 1915.

MATA HARI

Dutch-born Margaretha Zelle (1876–1917) became famous throughout Europe as a dancer under the stage name Mata Hari. She performed a dance which was, by her account, an authentic Hindu temple ritual. Her fame brought her many influential lovers.

Mata Hari briefly took up spying in 1916 when the German consul in Amsterdam persuaded her to use her lovers to acquire information for Germany. He gave her inks with which to send secret messages. It was not long before Mata Hari's amateurish attempts at espionage aroused the suspicions of both French and British intelligence. In spite of this, the French accepted her offer to spy for them. She seduced the German military attaché in Madrid, hoping he would give her information that she could pass on to France.

Mata Hari's end came when she was mentioned in a German secret service telegram from Madrid to Germany. Although referred to as "agent H-21," she was identifiable, and the message was intercepted by the French—it was in a code that they had already broken.

Mata Hari was arrested as a German spy on her return to Paris. She was tried in a French military court, found guilty, and executed by firing squad in 1917.

MATA HARI IN PRISON IN FRANCE

MATA HARI AS A DANCER BEFORE WORLD WAR I

Revolutionary Russia

THE RUSSIAN REVOLUTION of 1917 replaced the feudal government of the Czars with the communist government of the Bolsheviks (the Communist Party). The revolution took place as a result of hardships during World War I and of political pressures for a change in government. The Czarist government had an intelligence and security service called the Okhrana. One of the key tasks of the Okhrana had been to spy on revolutionaries such as the Bolsheviks. After they came to power, the Bolsheviks copied the Okhrana's techniques for gathering information.

EARLY CHEKA BADGE

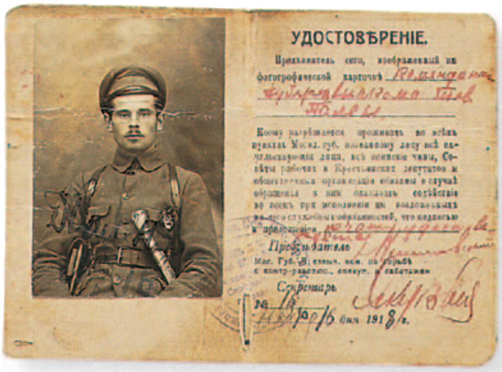
Felix Dzershinsky
The Russian secret police was founded by Felix Dzershinsky (seated in center). The huge and powerful organization that he established was to survive for longer than the Soviet Union itself.

The Czarist intelligence services had a mixed history. In 1913, military intelligence achieved a major success against the Austro-Hungarian Empire. Important secrets were acquired from an Austrian army officer, Colonel Alfred Redl (1864–1913). The colonel was secretly homosexual, and the Russians were able to blackmail him into passing Austro-Hungarian war plans to them.

In 1914, on the other hand, it was an intelligence failure that caused the first great Russian disaster of World War I, the defeat at the battle of Tannenberg. Radio signals relating to the deployment of the Russian forces were broadcast in plain Morse code (without the use of a cipher to ensure secrecy). This gave a crucial advantage to the Germans, who were monitoring the broadcasts.

The Okhrana

The Okhrana was more aware of the possibilities of signals intelligence than the military, and it employed spies to assist in code-breaking activities. The organization also had some success in bribing foreign journalists to present a favorable picture of Russia. This helped the Czar to secure war loans from countries allied to Russia. The most effective work of the Okhrana took place in Europe. A system of informers and agents was developed to penetrate revolutionary groups. The information from these networks was so good that Okhrana files are a major source of information on the early history of the Bolsheviks. When the Bolsheviks gained power, they were quick to see the value of the Okhrana's spying techniques and records.



УДОСТОВѢРЕНІЕ.

Предъявитель сего, изображенный на фотографической карточкѣ [illegible]

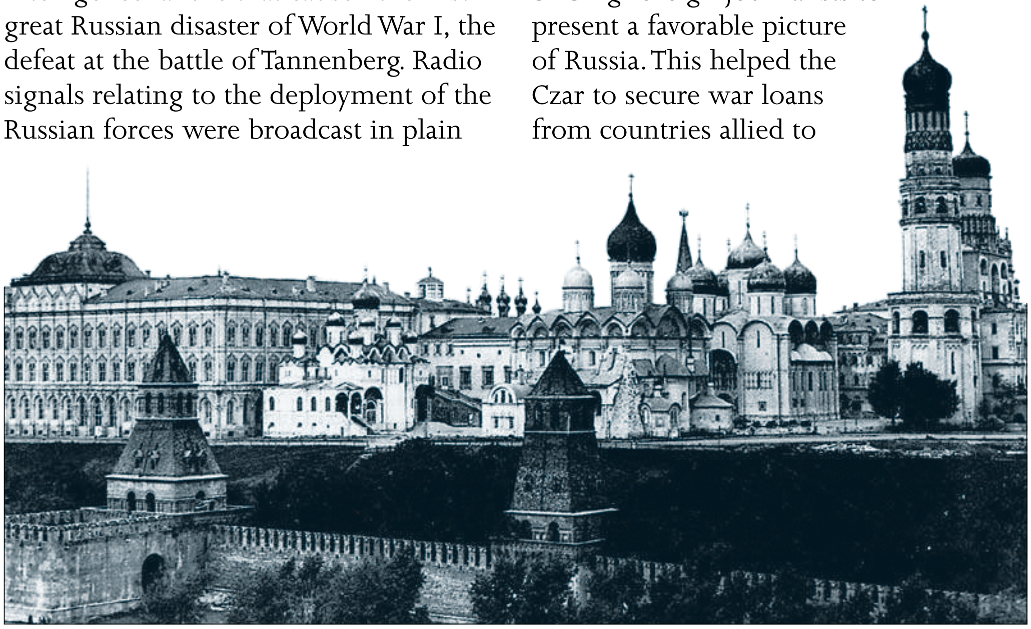
Коему разрѣшается проживать во всѣхъ пунктахъ Моск. губ. вышеназванному лицу всѣ начальствующія лица, всѣ воинскія чины, Совѣты рабочих и Крестьянских депутатов и общественныя организаціи обязаны в случаѣ обращенія к ним оказывать содѣйствіе во всѣхъ при исполненіи им возложенныхъ на него служебныхъ обязанностей, что подписью и приложеніем [illegible]

Председатель
Мос. Губ. Чрезвыч. ком. по борьбѣ с контр-революц., спекул. и саботажем

Секретарь

№ 16 [illegible] 1918 г.

Cheka credentials
This is the earliest known example of a Russian secret police identification credential. It belonged to a member of the Cheka.



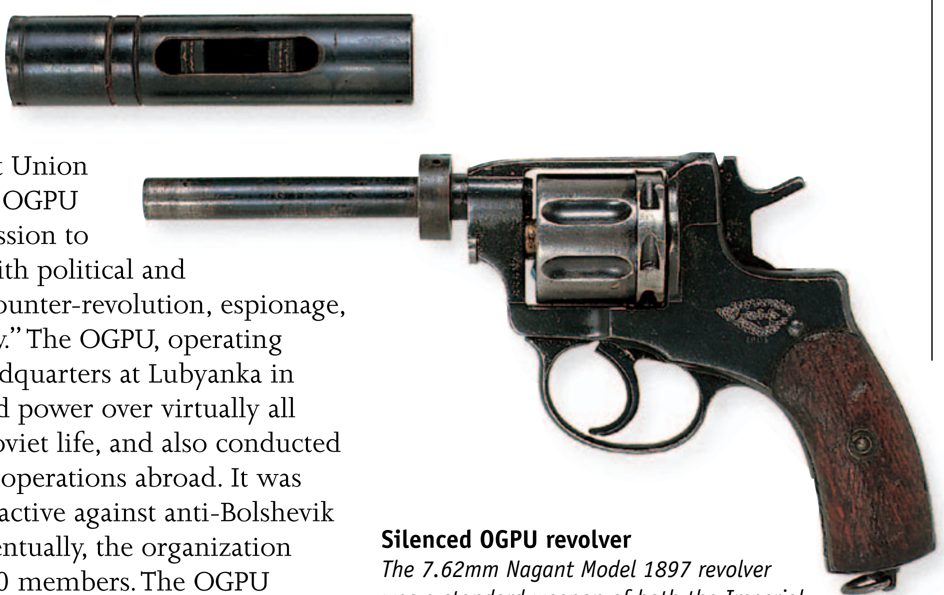
Moscow: the Kremlin
The Kremlin, a walled fortress in the center of Moscow, became the seat of Bolshevik power in 1918; today, it houses Russia's government.

The Cheka

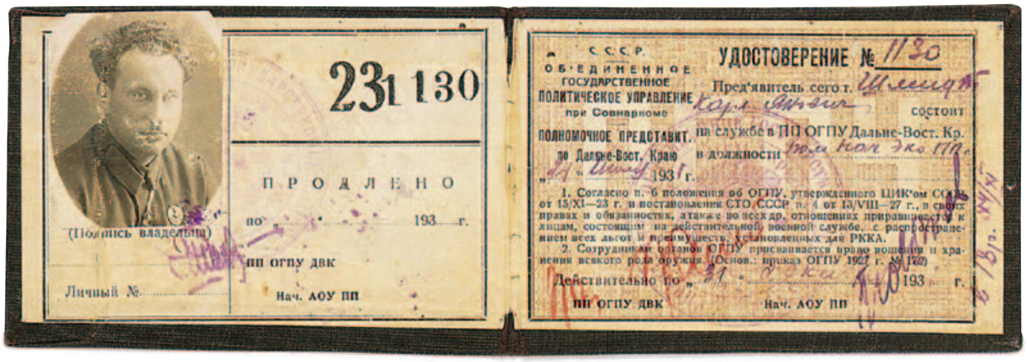
After gaining power in late 1917, the Bolsheviks created their own secret police, the Cheka. Under the command of Felix Dzershinsky (1877–1926), the Cheka immediately set about securing the Bolshevik hold on power. Political opponents of the regime were arrested, imprisoned, or executed. In the face of growing threats to the regime, these actions reached their peak in late 1918. Hostages were taken, concentration camps set up, and torture by Cheka interrogaters officially approved as a tool for extracting information. Combining this extreme ruthlessness with the interrogation techniques of the Okhrana and the prerevolutionary Bolshevik Party's expertise in clandestine activities, the Cheka was able to establish itself as the primary agency for espionage abroad and for counterintelligence at home.

The OGPU

In 1922, with the Bolsheviks firmly in power, the Cheka was converted into the GPU (State Political Directorate), still under Dzershinsky. When the Soviet Union was created in the following year, the GPU became the OGPU (United State Political Administration). The constitution of the Soviet Union charged the OGPU with the mission to "struggle with political and economic counter-revolution, espionage, and banditry." The OGPU, operating from its headquarters at Lubyanka in Moscow, had power over virtually all aspects of Soviet life, and also conducted intelligence operations abroad. It was particularly active against anti-Bolshevik émigrés. Eventually, the organization had 800,000 members. The OGPU remained, under a number of names, a central part of the government of the Soviet Union until 1991.



Silenced OGPU revolver
The 7.62mm Nagant Model 1897 revolver was a standard weapon of both the Imperial Russian and Soviet armies. This special example was used by the OGPU. It had a silencer, here shown removed.



(Подпись владельца)

Личный №

231 130

ПРОДЛЕНО

по .... 193 .... г.

ПП ОГПУ ДВК

Нач. АОУ ПП

С.С.С.Р.
ОБ'ЕДИНЕННОЕ
ГОСУДАРСТВЕННОЕ
ПОЛИТИЧЕСКОЕ УПРАВЛЕНИЕ
при Совнаркоме

ПОЛНОМОЧНОЕ ПРЕДСТАВИТ.
по Дальне-Вост. Краю
„24" Июня 1931 г.

УДОСТОВЕРЕНИЕ № 1130

Пред'явитель сего т. Шмидт Карл Янович состоит на службе в ПП ОГПУ Дальне-Вост. Кр. в должности пом нач Эко ПП

1. Согласно п. 6 положения об ОГПУ, утвержденного ЦИК'ом СССР от 15/XI—23 г. и постановления СТО СССР п. 4 от 13/VIII—27 г., в своих правах и обязанностях, а также во всех др. отношениях приравнивается к лицам, состоящим на действительной военной службе, с распространением всех льгот и преимуществ, установленных для РККА.

2. Сотрудникам органов ОГПУ присваивается право ношения и хранения всякого рода оружия. (Основ.: приказ ОГПУ 1927 г. № 172)

Действительно по „31" декабря 193 г.

ПП ОГПУ ДВК   Нач. АОУ ПП

OGPU credentials
In 1923, Felix Dzershinsky's intelligence and secret police organization became known as the OGPU. This organization was the direct forerunner of the later NKVD, MGB, and KGB. After the demise of the communist state in 1991, the KGB was dissolved and its directorates were renamed.

THE TRUST AND SIDNEY REILLY

The Trust was a deception operation, devised by the secret police chief Felix Dzershinsky (see above). Its purpose was to entice counterrevolutionary émigrés back to the Soviet Union so that they could be killed or imprisoned by the secret police.

Officially called the Moscow Municipal Credit Association, the organization was established in Moscow and had an office in Paris. Its ostensible purpose was to offer support to anti-Bolshevik groups. To gain the trust of the émigré community, Dzershinsky allowed the Trust to engineer the escape of a famous anti-Bolshevik general from Russia. Then, in 1924, the Trust was involved in persuading an émigré leader, Boris Savinkov, to return to Moscow, supposedly to lead a counterrevolution. Once in Moscow, Savinkov was arrested and tortured. In 1925 he was killed by being pushed out a window in the OGPU headquarters at Lubyanka in Moscow.

The same year, a British intelligence operative named Sidney Reilly was lured to a meeting with Trust members in Moscow, where he was arrested and forced to write a confession revealing all his Moscow contacts. He was then executed. His body was photographed in the Lubyanka morgue, as proof for OGPU records that he had been captured and killed.

Sidney Reilly, "Ace of Spies"
Reilly's exploits were sensationalized in the 1920s by a journalist, and writer Ian Flemin later used him as a model for James Bond.

Assassination of Trotsky

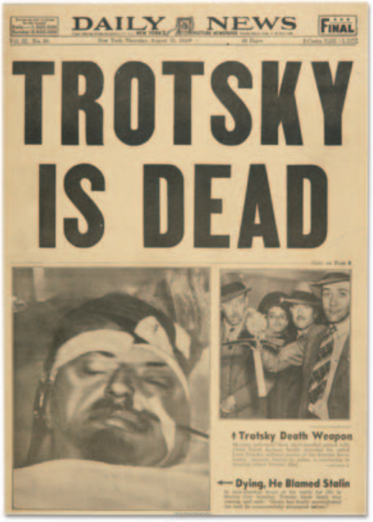
RAMON MERCADER'S ASSASSINATION of Leon Trotsky with an ice-climbing ax in Mexico in 1940 became known as the crime of the century. A leader of the Russian Revolution, and the founder of the Red Army, Trotsky (b.1879) was second only to Vladimir Lenin in the Russian Civil War of 1917–23. As Lenin's health failed in 1921, Trotsky was heralded as his heir apparent. But after Lenin's death in 1924 he was eclipsed by Josef Stalin—General Secretary of the Communist Party—expelled from the Communist Party in 1927, and exiled in 1929.

Ramon Mercader
Born in Barcelona in 1914, keen communist Ramon Mercader (seen here as "Frank Jacson") spent part of his youth in France. Back in Spain, Russian agents taught him the arts of sabotage, guerilla warfare, and assassination. In 1937 he was sent to Moscow for further training.

Leon Trotsky, international revolutionary
Trotsky differed fundamentally from Stalin in that he advocated a worldwide workers' revolution, and not just a strong communist Russia.

Continuing his outspoken criticism of Stalin, Trotsky fled to Turkey for four years, then on to France in 1933 and Norway two years later. In each country the Soviet Union mounted political pressure for him to be expelled. There seemed no safe place for him, especially not after August 1936, when he was sentenced to death in his absence at a Moscow show trial. But then the world-renowned Mexican painters Diego Rivera and his wife Frida Kahlo, who were both committed communists, arranged with Mexican President Lazaro Cardenas for Trotsky to have refuge in their country. In January 1937, Trotsky and his wife, Natalia Sedova, arrived in the Mexico City suburb of Coyoacan as house guests of Diego and Frida.

How the murder weapon was lost—and found
After Mercader's trial, his ax remained in a police property room, then in 1949 was put in a museum. The museum closed in the 1960s and its director was given the ax. The ax was next seen in 2005, having spent 40 years under his daughter's bed.



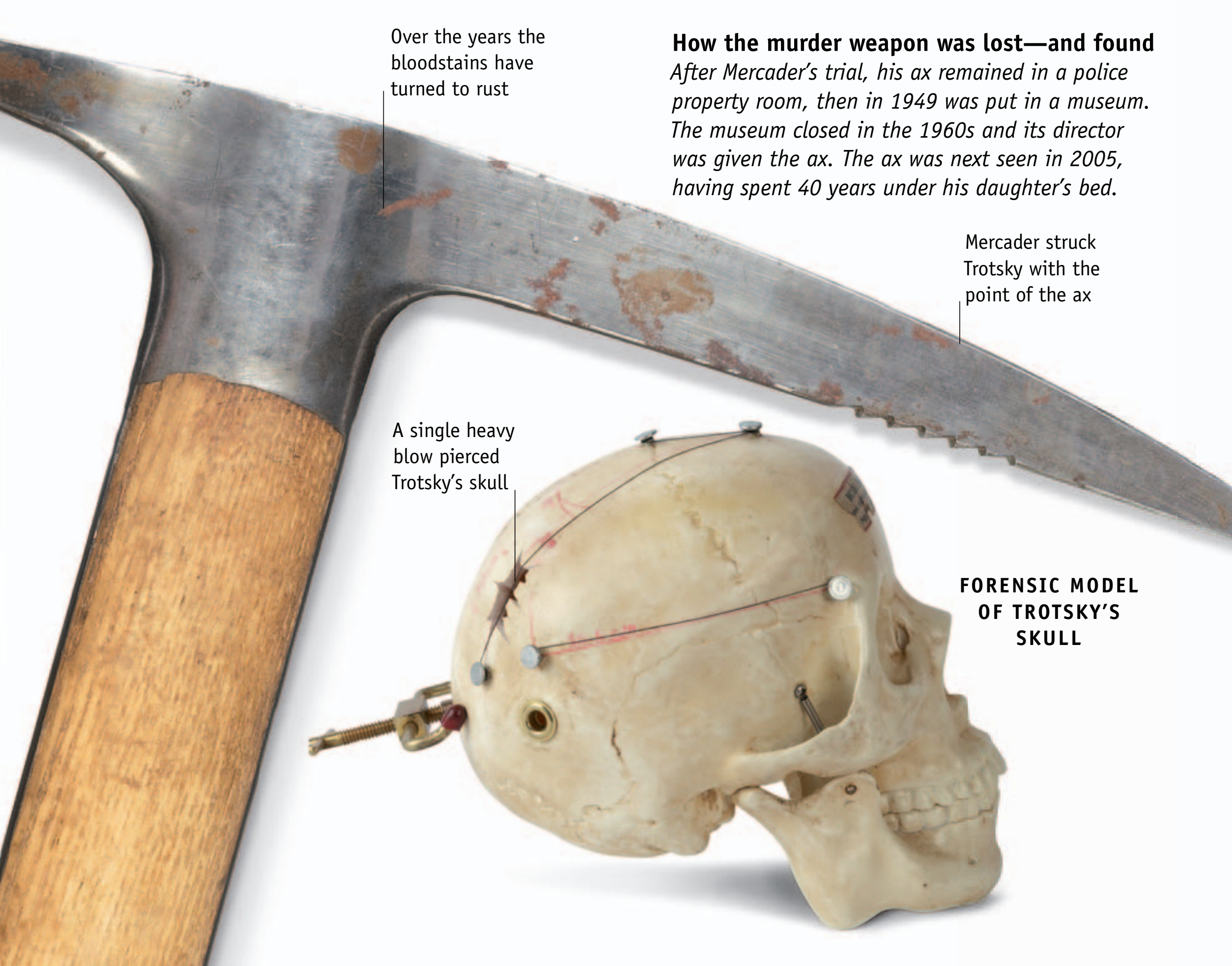
DAILY NEWS FINAL

TROTSKY IS DEAD

↑Trotsky Death Weapon

←Dying, He Blamed Stalin

FRONT PAGE OF A NEW YORK NEWSPAPER, AUGUST 22, 1940


Over the years the bloodstains have turned to rust
Mercader struck Trotsky with the point of the ax
A single heavy blow pierced Trotsky's skull

FORENSIC MODEL OF TROTSKY'S SKULL

CARIDAD MERCADER

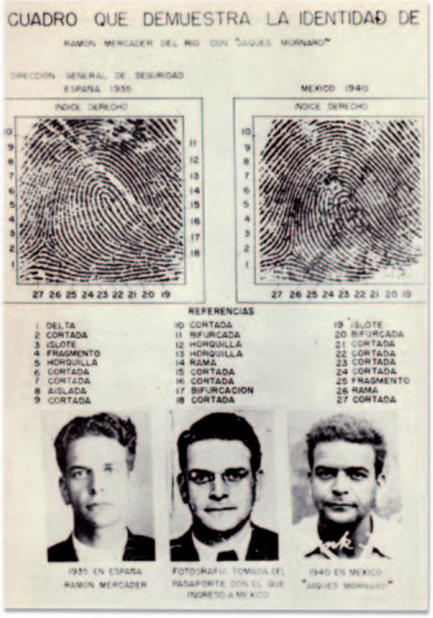
SPY PROFILE

Cuban-born Caridad Mercader (1892–1975) left Spain for France with Ramon after separating from his father in the 1920s. Both fought the Fascists in Spain, where she was NKVD officer Eitingon's lover. In 1937 she trained with Ramon in Moscow. Following Ramon's arrest, she and Eitingon fled Mexico. Stalin received her as a hero. After a failed operation (codename Gnome) to spring Ramon, she worked for the KGB in Paris. She saw Ramon often after his release.

The assassination of Trotsky (codename Starik) was personally authorized by Stalin, but after one failed attempt the year before, in 1939 Stalin entrusted the operation (codename Utka—Duck) to the head of "Special Tasks" Pavel Sudoplatov. Field command in Mexico went to Leonid Eitingon (codename Tom), an NKVD officer (see p. 217).

Sudoplatov set up two assassination teams. The first was led by the Mexican artist and Stalinist David Siqueiros (codename Kone). The second was made up of two NKVD agents, Caridad Mercader (codename Mother) and her son Ramon (codename Raymond). The two teams knew nothing of each other's existence.

By then, Trotsky had moved into a fortified residence in Coyoacan. On the night of May 24, 1940, Siqueiros and 20 veterans of the Spanish Civil War (1936–39), disguised as policemen, entered the compound with the help of a guard and riddled Trotsky's bedroom with submachine-gun bullets. Miraculously, their target was completely unharmed. Siqueiros fled and Eitingon ordered the second team into action.



CUADRO QUE DEMUESTRA LA IDENTIDAD DE

RAMON MERCADER DEL RIO CON "JAQUES MORNARD"

DIRECCION GENERAL DE SEGURIDAD
ESPAÑA 1935

MEXICO 1940

INDICE DERECHO

INDICE DERECHO

REFERENCIAS

1	DELTA	10	CORTADA	19	ISLOTE
2	CORTADA	11	BIFURCADA	20	BIFURCADA
3	ISLOTE	12	HORQUILLA	21	CORTADA
4	FRAGMENTO	13	HORQUILLA	22	CORTADA
5	HORQUILLA	14	RAMA	23	CORTADA
6	CORTADA	15	CORTADA	24	CORTADA
7	CORTADA	16	CORTADA	25	FRAGMENTO
8	AISLADA	17	BIFURCACION	26	RAMA
9	CORTADA	18	CORTADA	27	CORTADA

1935 EN ESPAÑA
RAMON MERCADER

FOTOGRAFIA TOMADA DEL PASAPORTE CON EL QUE INGRESO A MEXICO

1940 EN MEXICO
"JAQUES MORNARD"

The document that identified the assassin
Mercader never revealed his true identity, which was only determined by fingerprinting in the late 1940s. The mugshots here are all of him, at different ages.

Mercader makes history

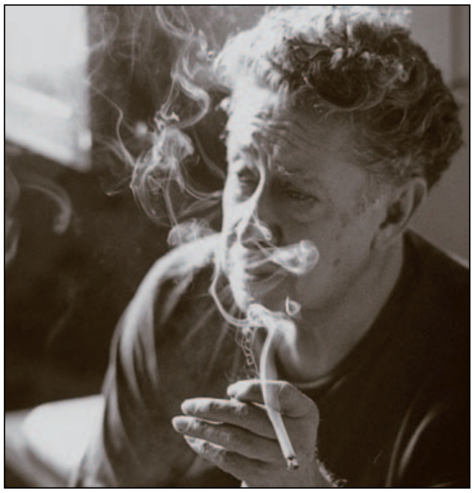
Under the alias Jacques Mornard, Ramon Mercader had been introduced in Paris in 1938 to a young American Trotskyite, Sylvia Ageloff—sister of one of Trotsky's former secretaries. He initially feigned disinterest in politics and they began a relationship. In 1939 he followed her to New York, posing as a Canadian called Frank Jacson—to avoid military service, he told her. ("Jacson" was a misspelling of "Jackson" by NKVD passport forgers.) In October 1939 Mercader moved to Mexico City as Jacques Mornard under the pretense of running a business, and asked Sylvia to join him. With Sylvia's unwitting help, he began to meet with Trotsky privately and gain his trust.

On the afternoon of August 20, 1940, "Mornard" visited Trotsky with a dagger, a pistol, and an ice-climbing ax hidden in his raincoat, while his mother waited outside in a getaway car. He was let into Trotsky's office without being searched and there struck him from behind with the ax, toward the back of the head, as Trotsky sat unsuspectingly at his desk. Trotsky cried out and his bodyguards overpowered his attacker. Trotsky died the next day. "Mornard" was sentenced to 20 years in a Mexican prison.

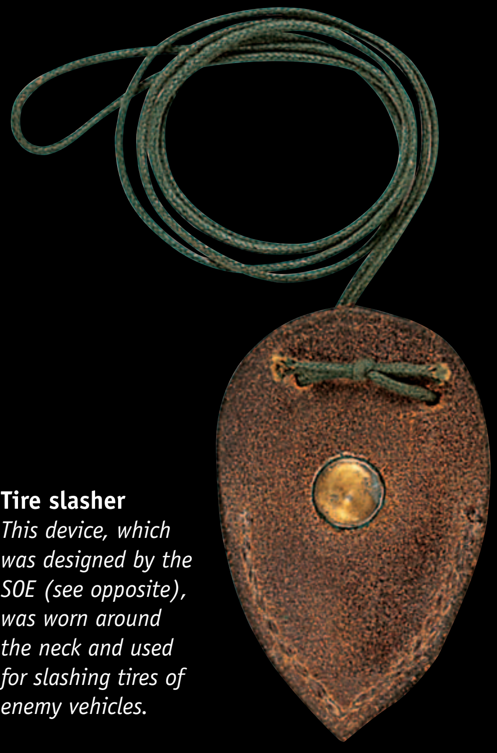
The reward for murder
Freed in 1960, Mercader lived in the Soviet Union and Cuba until his death in 1978. The Soviets made Comrade Ramon Ivanovich Lopez—his operational name—a Hero of the Soviet Union, their highest honor, and in 1965 gave him this gold watch.

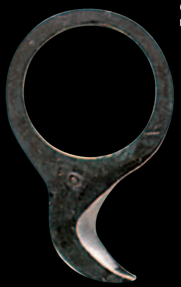
THE FAILED ASSASSIN

David Alfaro Siqueiros (1896–1974) was Mexico's second most famous muralist, after Rivera. Noted for his realistic depictions of the Mexican Revolution of 1910 and the Spanish Civil War, he was radicalized when he was a student. In the early 1920s he traveled in Europe, before returning to Mexico to work as a muralist for the revolutionary government until he was briefly jailed then exiled in the early 1930s. In the Spanish Civil War he fought for the Soviets. Back in Mexico, he was jailed for his May 1940 attempt to assassinate Trotsky, and in the early 1960s for allegedly inciting a riot. In 1961 the Soviets awarded him the Lenin Peace Prize.



WORLD WAR II





Tire slasher
This device, which was designed by the SOE (see opposite), was worn around the neck and used for slashing tires of enemy vehicles.

THE MAJOR COMBATANTS OF WORLD WAR II deployed their intelligence services with varying degrees of success. At the start of war in Europe in 1939, the Soviet Union, Germany, Japan, and Britain had well-established foreign intelligence networks, although the United States did not.

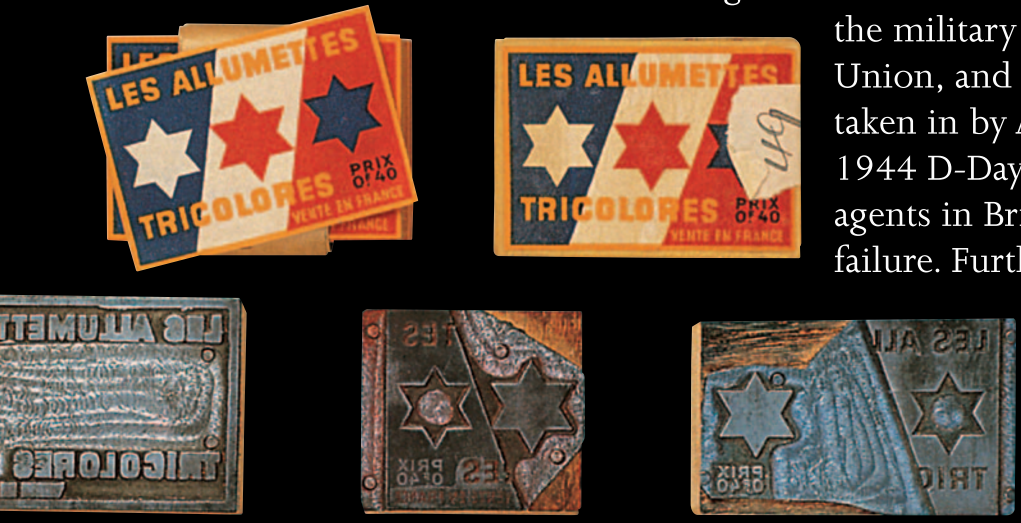
The most extensive networks operated were the Soviet ones, including the west European network under Leopold Trepper. Among other things, Trepper warned of the German invasion of the Soviet Union in 1941. Warnings were sent, too, by Richard Sorge, a Soviet spy in Japan (see p. 39). Unfortunately, Premier Stalin did not trust his own intelligence sources. But there was one message from Sorge that did help significantly, prompting Stalin to move Soviet troops from the east to halt the German advance in the west and prevent the fall of Moscow.

AXIS INTELLIGENCE

Lapel badge
In 1945 the OSS (see opposite) issued this pin to its veterans.

German espionage efforts were less successful. The intelligence community was split into two rival camps, the Army-controlled Abwehr and the Nazi Party SD. Toward the end of the war, the Abwehr was put under SD control. Germany's intelligence services seriously underestimated the military power of the Soviet Union, and they were completely taken in by Allied deception plans that masked the 1944 D-Day landings. German attempts to establish agents in Britain and the United States, too, were a failure. Furthermore, when good information was acquired by the German intelligence agencies—for example, through the agent called Cicero (see p. 34)—it was badly mishandled.

In contrast to Germany, Japan used its intelligence sources well, having gathered intelligence to good effect prior to its successful attacks on Pearl Harbor and on a number



Counterfeit matchboxes
Special operations personnel operating in occupied countries had to have belongings that seemed to be locally made. These matchbox labels and color printing blocks were made for the SOE (see opposite).

Walter Schellenberg
Following the assassination in 1942 of SD head Reinhard Heydrich (see p. 35), Schellenberg (1910–52) took over SD foreign intelligence operations.

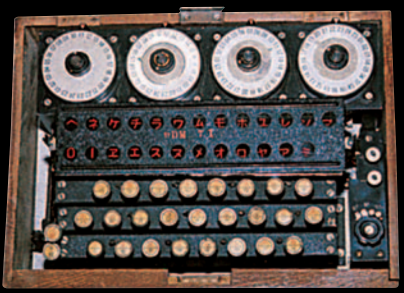
of countries in Southeast Asia that were dependencies of European powers (see p. 41). The Japanese also maintained a spy ring in America.

THE WESTERN ALLIES

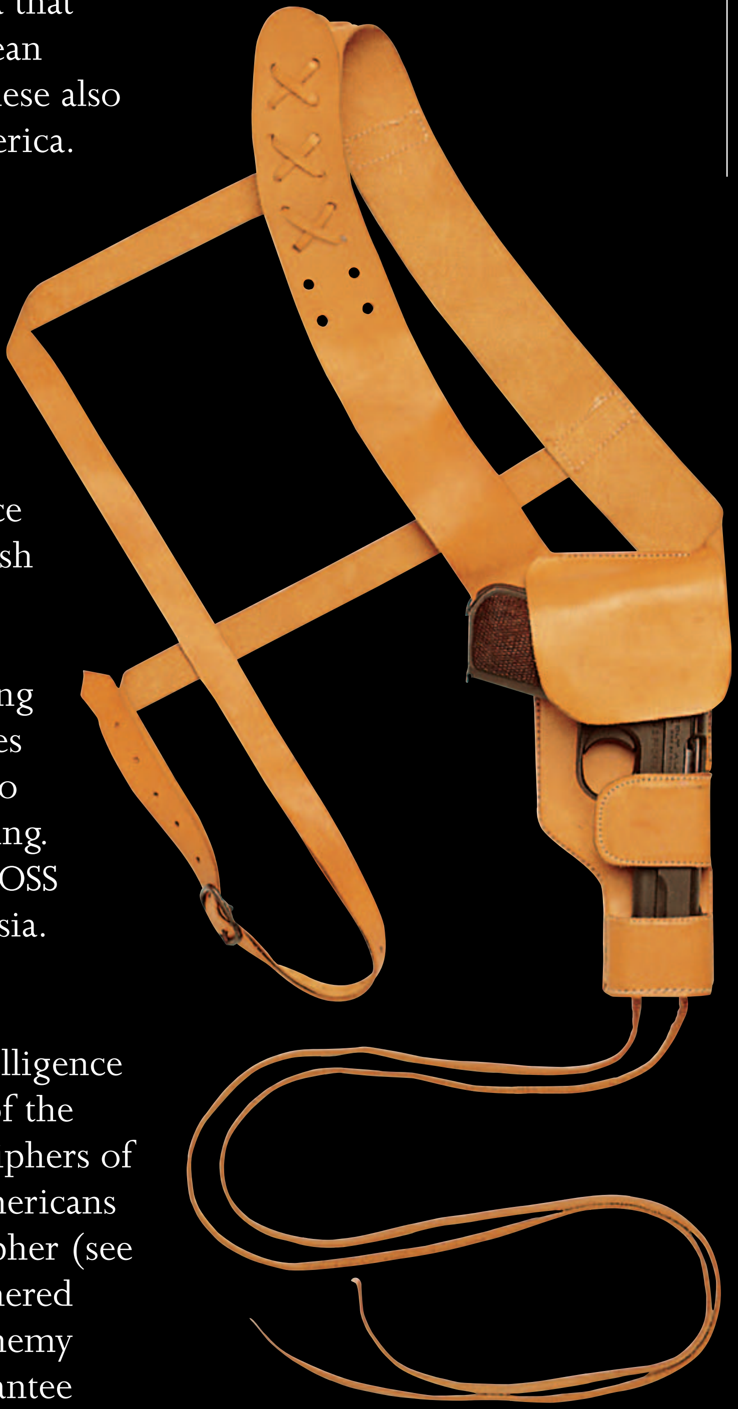
The British and Americans had to invent intelligence strategies to cope with war against an enemy who seized vast areas of territory. In 1940, European stations of Britain's senior intelligence service, MI6, were all overrun by the Germans. The British created a new service, the Special Operations Executive (SOE, see p. 30). This was the first service that combined intelligence-gathering with clandestine warfare (including support for resistance groups). In 1942, the United States created the Office of Strategic Services (OSS, see p. 32) to play a similar role but with stronger intelligence-gathering. Together, and with local resistance groups, the SOE and OSS caused chaos behind enemy lines, in both Europe and Asia.

NEW SKILLS

In terms of influencing the outcome of the war, the intelligence operations that proved to be most effective were those of the Allied code-breakers. British cryptographers broke the ciphers of the German Enigma and Geheimschreiber, while the Americans broke the Japanese Purple cipher (see p. 36). Information thus gathered gave the Allies insight into enemy intentions. This did not guarantee them victory, but it had far-reaching effects on their conduct of the war. In 1943 it helped to defeat the German submarine fleet, which otherwise would have blocked essential Allied shipping lanes in the North Atlantic.



Cipher machine
Japan produced its own innovations in intelligence codes and ciphers. This is a Japanese rotor-type cipher machine.



Shoulder holster
Holsters of this type were used by SOE officers who chose to carry a pistol for personal protection. This example contains a Colt .32 pistol.

Special Operations Executive

THE BRITISH SPECIAL OPERATIONS EXECUTIVE (SOE) was founded during World War II in the summer of 1940, after Germany had invaded much of continental Europe. Its task was to equip, train, and help lead resistance groups in areas occupied by the German forces, as well as to take part in aggressive sabotage operations. SOE officers and operatives worked with local resistance groups, coordinating their activities with one another and with the campaigns of the anti-German Allied armies for the liberation of occupied Europe.

SPECIAL FORCES' WINGS

All the SOE's recruits were volunteers, and were often dismissed by the more established intelligence services as amateurs, meddling in "cloak-and-dagger" warfare.

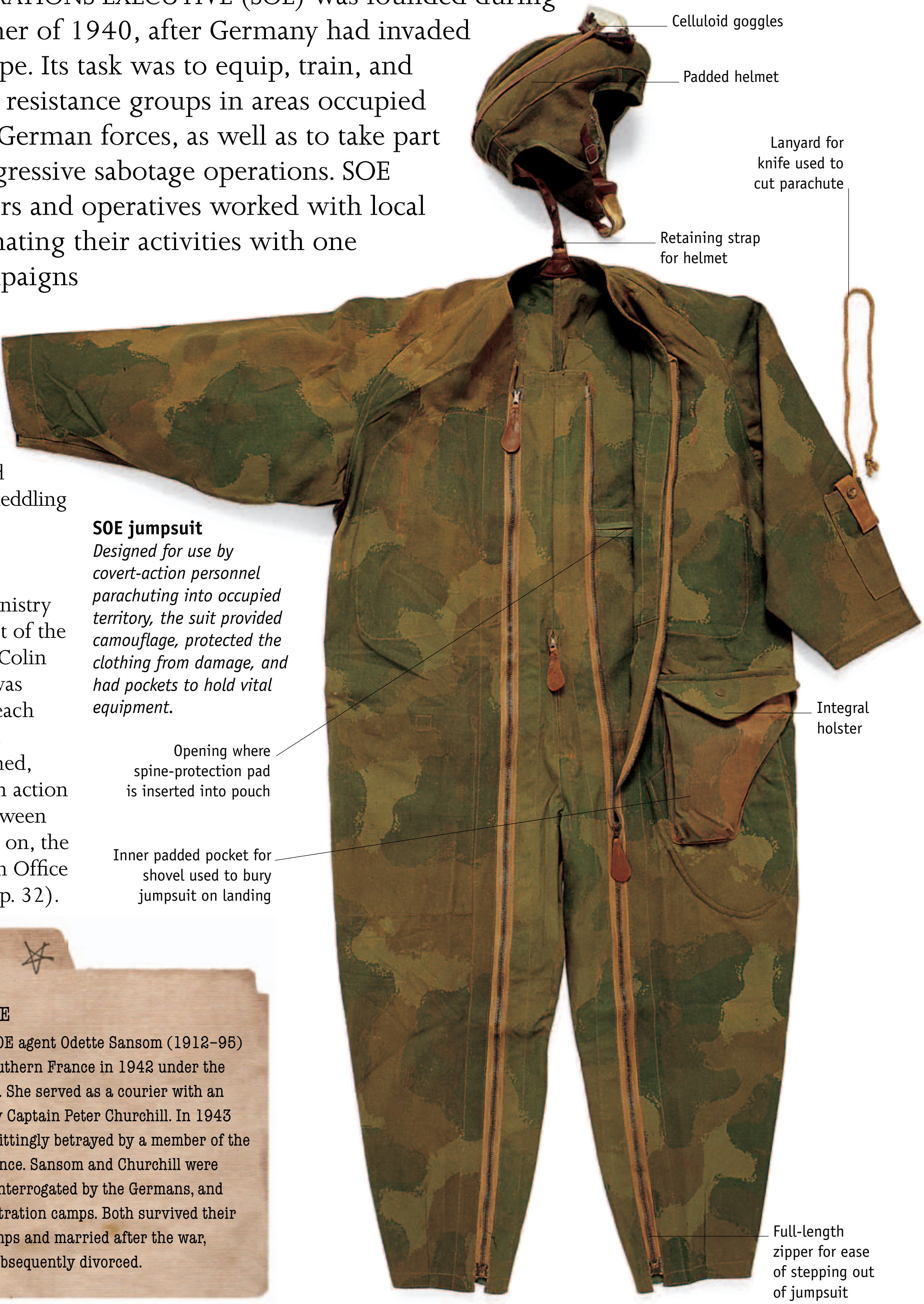
Organization

The SOE was controlled by the Ministry of Economic Warfare, and for most of the war was led by Major General Sir Colin Gubbins (1896–1976).The SOE was divided into separate "desks" for each country in which operations were planned. Each desk recruited, trained, and operated its own personnel. In action the SOE operated in groups of between two and 30 members. From 1943 on, the SOE cooperated with the American Office of Strategic Services, the OSS (see p. 32).

ODETTE SANSOM

SPY PROFILE

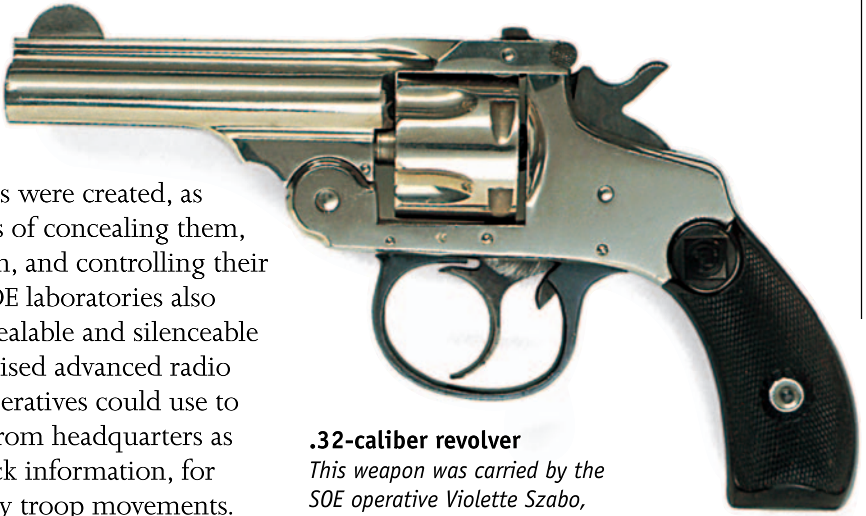
French-born SOE agent Odette Sansom (1912–95) was sent to southern France in 1942 under the codename Lise. She served as a courier with an SOE unit led by Captain Peter Churchill. In 1943 they were unwittingly betrayed by a member of the French resistance. Sansom and Churchill were captured and interrogated by the Germans, and sent to concentration camps. Both survived their time in the camps and married after the war, though they subsequently divorced.


Celluloid goggles
Padded helmet
Lanyard for knife used to cut parachute
Retaining strap for helmet
Integral holster
Opening where spine-protection pad is inserted into pouch
Inner padded pocket for shovel used to bury jumpsuit on landing
Full-length zipper for ease of stepping out of jumpsuit

SOE jumpsuit
Designed for use by covert-action personnel parachuting into occupied territory, the suit provided camouflage, protected the clothing from damage, and had pockets to hold vital equipment.

Operations

SOE operatives and officers were sent into enemy territory clandestinely, some landing in aircraft in fields or dropping by parachute, others using submarines and small boats. The SOE's approach was always to cooperate closely with local resistance groups. Together they made sabotage attacks on communications, factories, and power lines to disrupt the enemy. Back in Britain, the SOE set up laboratories to develop equipment for its operatives and officers. Special forms of explosives were created, as were original ways of concealing them, camouflaging them, and controlling their detonation. The SOE laboratories also made special concealable and silenceable weapons. They devised advanced radio equipment that operatives could use to receive messages from headquarters as well as passing back information, for example, on enemy troop movements.



.32-caliber revolver
This weapon was carried by the SOE operative Violette Szabo, who was an excellent shot.

VIOLETTE SZABO

SPY PROFILE

British-born Violette Szabo (1921–45) joined the SOE after her husband, who was an officer in the Free French army, was killed fighting the Germans. Szabo's last mission to France was on June 6, 1944 (D-Day), when she was sent to assist a resistance group. Within days she was captured by the Gestapo (see p. 34) but she refused to talk, despite being raped and tortured. Szabo was sent to Ravensbruck concentration camp and executed on January 26, 1945.

The risks

Since their work involved resistance and sabotage, SOE operatives were relentlessly hunted by enemy forces. If captured, the operatives risked torture and death. From 1940 until 1944, 393 SOE operatives were sent to work in France—17 were captured and survived, 104 were killed. Despite such sacrifices, the SOE was never fully accepted by the established intelligence services. Officers of its British rival, the Secret Intelligence Service (MI6), disliked the SOE's policy of combining guerrilla warfare, sabotage, and subversion with more conventional forms of intelligence-gathering.

The SOE nonetheless played a vitally important role in organizing resistance forces and coordinating their operations in support of the Allied invasion of Europe, which finally came in 1944.

THE FRENCH RESISTANCE

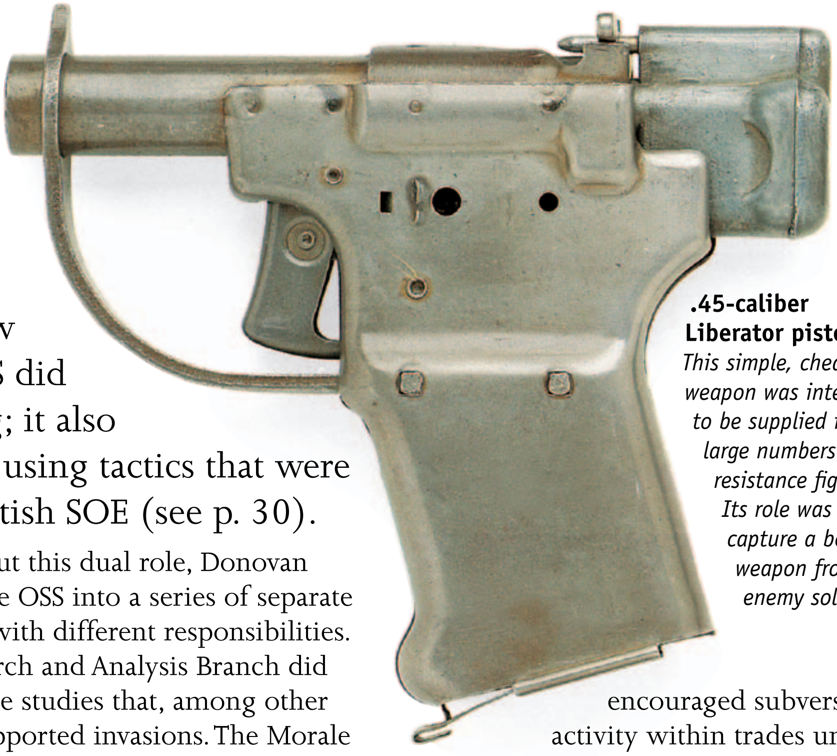
The Maquis preparing their weapons
The first Maquis units were made up of people evading a German forced labor program. Later, the whole French resistance was called the Maquis.

The French resistance was made up of groups within France that actively opposed the German occupation. The resistance provided a ready-made network of spies and saboteurs for the nations allied against Germany. Particularly valuable intelligence was provided by resistance members and sympathizers who were employed in German military bases and other establishments. The resistance often supported the escape lines set up by the British and American intelligence services, through which many airmen and escaped prisoners of war were helped to reach safety. A sabotage campaign was mounted, in which the resistance was aided by the SOE and OSS. This gave rise, in June 1944, to widespread attacks on German transportation and communications in support of the Allied invasion of Europe, the D-Day landings. On August 10, 1944, a series of work stoppages began in Paris that led to a full-scale public revolt against the German occupiers. On August 24, the Allied forces, including elements of Free French armored units, entered Paris. The German garrison surrendered the following day.

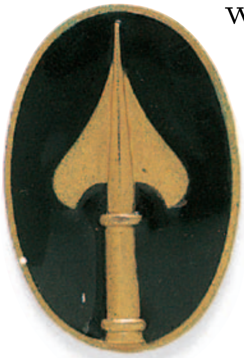
Lapel blade, sheath, and armband
The sheath shows the Cross of Lorraine, symbol of the Free French army, which fought against the Germans from outside France.

Office of Strategic Services

THE OFFICE OF STRATEGIC SERVICES (OSS) was created in June 1942, six months after the United States entered World War II. Its director, William J. "Wild Bill" Donovan (1883–1959), had previously held the key intelligence post of coordinator of information, reporting directly to the president. He formed a new service truly worldwide in scope. The OSS did not restrict itself to intelligence-gathering; it also waged clandestine warfare, using tactics that were similar to those of the British SOE (see p. 30).



.45-caliber Liberator pistol
This simple, cheap weapon was intended to be supplied in large numbers to resistance fighters. Its role was to capture a better weapon from an enemy soldier.



OSS COLLAR INSIGNIA

OSS LAPEL PIN

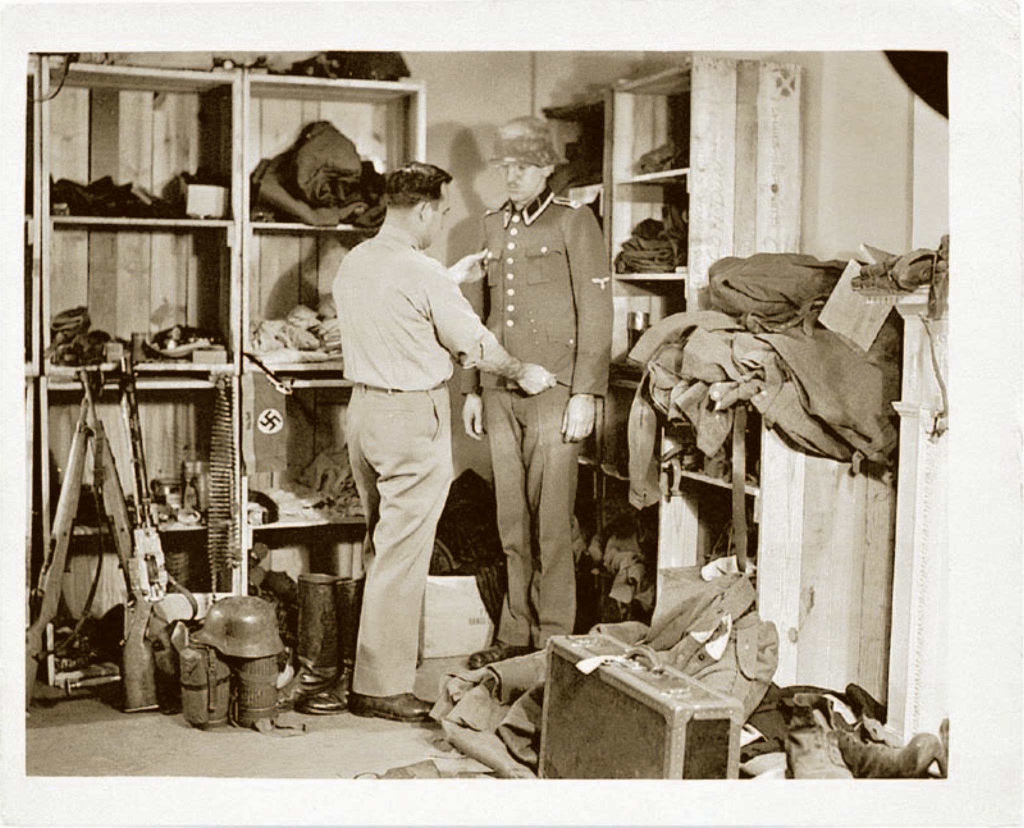
To carry out this dual role, Donovan divided the OSS into a series of separate branches with different responsibilities. The Research and Analysis Branch did intelligence studies that, among other things, supported invasions. The Morale Operations Branch produced propaganda, using the skills of advertising copywriters and screenwriters. The Labor Division encouraged subversive activity within trades unions in enemy-occupied Europe, in order to disrupt production and communications systems. Three of the main functional branches of the OSS were: Special Operations (SO), Secret Intelligence (SI), and Counterintelligence (X-2).

Clandestine warfare

The SO branch, modeled on Britain's SOE, supported resistance movements in parts of Europe and Asia. Usually working in groups of between two and 30 people, members of the SO branch operated behind enemy lines. Lines of communications and supply, factories, and airfields were sabotaged.

Secret Intelligence

The SI branch of the OSS established a comprehensive system for the gathering of intelligence. To ensure worldwide coverage, the SI branch was divided into four geographical "desks" dealing with parts of Europe, Africa, the Middle East,



OSS clothing warehouse in London
Clothing such as this German army uniform was taken from prisoners and used by OSS operatives on secret missions in German-occupied territory.

OSS DETACHMENT 101

The first OSS unit created to carry out secret operations was called Detachment 101. Its personnel were trained at an SOE base, Camp X, in Canada. Captain (later Colonel) Carl Eiffler (1906–2002) was the commander of Detachment 101 from April 1942 until December 1943. The detachment's mission was to conduct a campaign of sabotage and guerrilla warfare in Burma (now Myanmar) behind Japanese lines. In the fall of 1942, the detachment entered the Burmese jungle and made contact with local Kachin people, who, having suffered badly at the hands of the Japanese, were willing to help the United States. The Kachins were provided with equipment and training by the Americans, and also possessed tribal ambush techniques of their own. Detachment 101 eventually reached a strength of 500, assisted by more than 10,000 Kachins. This combined force caused over 15,000 Japanese casualties.

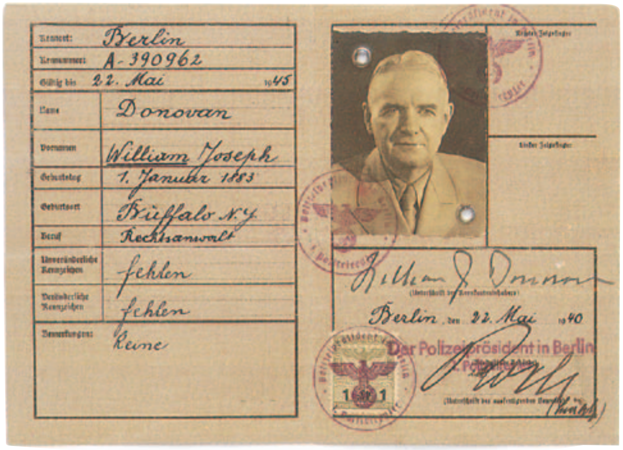
101 DETACHMENT CAMPAIGN BAR

COLONEL CARL EIFFLER

and Asia. A number of other sections assisted the SI branch in its operations. A Reporting Board analyzed the agents' reports and distributed them. The Ship Observer Unit gathered information on the enemy from seamen's organizations and shipping operators. The Technical Section reviewed technical reports and provided information for Britain, as well as the United States, about matters such as the development of V1 and V2 rockets.

Special equipment

The OSS was supplied with a range of specialized equipment by the Research and Development Division, which was led by Stanley Lovell (see p. 189). Many innovative weapons and devices were produced specially for the OSS. The Liberator pistol was a cheaply made weapon intended for distribution to resistance groups in occupied countries. Special explosives were invented, along with devices for camouflaging them and delaying their detonation. Advanced radio equipment was made for contact between OSS headquarters and operatives in the field. Secret cameras were developed for taking clandestine photographs.



Kennort:	Berlin
Kennnummer:	A-390962
Gültig bis	22. Mai 1945
Name	Donovan
Vornamen	William Joseph
Geburtstag	1. Januar 1883
Geburtsort	Buffalo N.Y.
Beruf	Rechtsanwalt
Unveränderliche Kennzeichen	fehlen
Veränderliche Kennzeichen	fehlen
Bemerkungen:	Keine

William J. Donovan
(Unterschrift des Kennkarteninhabers)

Berlin, den 22. Mai 1940

Der Polizeipräsident in Berlin

(Unterschrift des ausfertigenden Beamten)

False German identification card

Produced for OSS chief William Donovan, these credentials demonstrate the ability of OSS forgers to create realistic German documents.

Donovan's achievement

During World War II, the OSS achieved notable successes in both clandestine warfare and intelligence-gathering, and demonstrated the benefits of combining these two major roles in one central organization. Nevertheless, its mode of operations was new to the United States and had not yet been wholly accepted. Also, Harry S. Truman, who became US President in 1945, saw Donovan as a political rival and had no reason to keep him on in a top government post. The OSS was abolished in 1945 and its intelligence-gathering role was then taken over by the US War Department, while the analysis role went to the State Department. Donovan had hoped that he would be able to set up a postwar intelligence service, but the plan he put forward was overshadowed by Truman's dislike for him.

Although Donovan never attained his goal of creating a single, centralized US intelligence service, a variation of his plan did come into being two years after the OSS had been disbanded. This was the Central Intelligence Agency (CIA) (see p. 46). Donovan also left another legacy to US intelligence in the form of several highly experienced OSS veterans who joined the CIA, including William Colby and Richard Helms.

WILLIAM COLBY

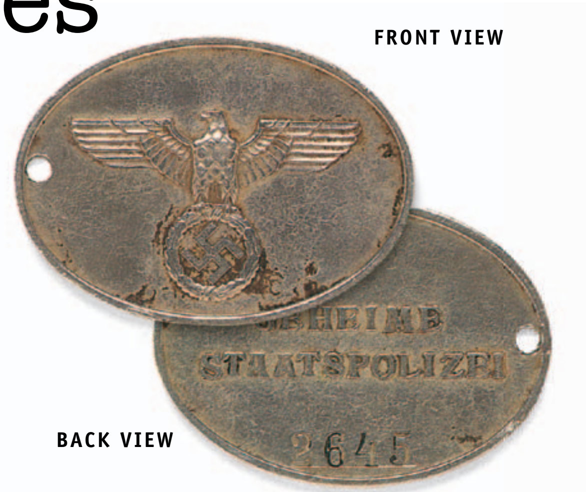
SPY PROFILE

During World War II, William Egan Colby (1920–96) served with the OSS in both France and Norway, where he carried out sabotage with local resistance groups (see p. 181). After the war, Colby held posts around the world with the Central Intelligence Agency (CIA). Later, in Vietnam, on leave from the CIA, he headed a key military-intelligence program with the rank of ambassador. Colby was Director of the CIA from 1973 until 1976.

German secret services

DURING WORLD WAR II (1939–45), there were two German intelligence agencies—the Abwehr and the Sicherheitsdienst, or SD. The Abwehr was the intelligence and clandestine warfare section of the armed forces. The SD was controlled by the Schutzstaffel (the notorious SS), an arm of the National Socialist Party (the Nazi Party), which ruled Germany from 1933 until the defeat of Germany at the end of the war. The role of the SD was to spy on the other Nazi Party members for the SS.

ADMIRAL WILHELM FRANZ CANARIS (1887–1945)



Gestapo warrant disk
Numbered warrant discs were carried by members of the Gestapo as proof of authority for use only when carrying out arrests and house searches.

From 1935, the head of the Abwehr was Admiral Wilhelm Canaris. As a naval officer, Canaris had been involved in undercover work during World War I. When appointed head of the Abwehr, his first task was to establish a working relationship with the SD, as previously there had been very little cooperation between the two agencies. Reinhard Heydrich was the chief of the SD. In 1938, the Geheime Staatspolizei (the Gestapo, the secret state police) and the Kripo (criminal police) came under control of the SD. Heydrich had served as a cadet under Canaris in the navy, and they agreed on a compromise that made the Abwehr responsible for military espionage and all counterespionage, while the SD took responsibility for political intelligence and police work.

Cooperation between the Abwehr and the SD did not last, and Canaris soon expanded the Abwehr in an attempt to become more important than the SD and free himself from Nazi Party control. But he failed to gain the authority he wanted for the Abwehr and, despite some successes, the Abwehr's foreign intelligence operations produced few significant results.

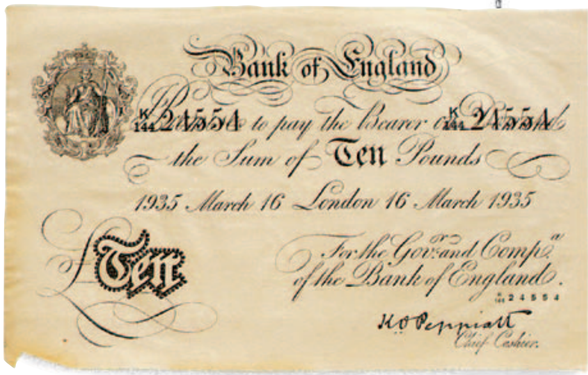
The SD

From 1935 onward, the SD expanded greatly in size and power. Reinhard Heydrich enjoyed the support and patronage of the chief of all German police, Reichsführer SS Heinrich Himmler. Under Heydrich the SD gradually

CICERO AND OPERATION BERNHARD

Cicero was the codename for Elyesa Bazna (1904–70), the Albanian valet of the British ambassador to Turkey, Sir Hugh Knatchbull-Hugessen. Bazna worked as an agent for the SD between 1943 and 1944. Having stolen the keys to the ambassador's safe, Bazna photographed documents about conferences in Moscow, Cairo, and Teheran and information relating to the impending D-Day invasion of German-occupied Europe. The Germans did not gain much advantage from this information, however, because it was mishandled by the German intelligence services. The SD paid Bazna £300,000 ($1,200,000) in counterfeit notes. These notes had been made as part of a plan—Operation Bernhard—to destabilize the British economy by distributing large amounts of forged currency. The SD used Jewish master forgers from concentration camps to forge the currency, which they did to such a high standard that the forgeries were not discovered until after the war. Bazna's postwar retirement plans collapsed when the forgeries were detected; he sued the German government, without success.

Elyesa Bazna
Years after the discovery of his spying activities, Bazna demonstrated how he had photographed secret documents with a Leica camera.


Bank of England
to pay the Bearer
the Sum of Ten Pounds
1935 March 16 London 16 March 1935
Ten
For the Gov. and Comp. of the Bank of England
Chief Cashier

Counterfeit British 10-pound note
Jewish master forgers in concentration camps were coerced into forging British banknotes, causing the recall of an entire series of currency.

“*This page left intentionally blank.*”

Code-breaking

SPIES, DIPLOMATS, military personnel, and others often relied on cipher machines to protect the secrecy of their messages during World War II. Messages enciphered by means of the German Enigma cipher machine (see p. 156) and the Japanese Alphabetic Typewriter 97 were deciphered by code-breakers working in special establishments in both Britain and the United States.

Baron Hiroshi Oshima

Oshima (1886–1975) was Japan's ambassador to Germany during World War II. He sent messages on the broken Purple cipher.

The Purple code

In 1939, the Japanese began using a new cipher machine for sending diplomatic messages. They called it the Alphabetic Typewriter 97, but in the United States it was known by the codename Purple. The Purple machine was a development of an earlier one codenamed Red. The US Army Signals Intelligence Service, led by William Friedman, had already cracked the Red system, and now a team led by Frank Rowlett (1908–98) began work on the new cipher. They were aided by the interception of a message that had been enciphered on both the Red and Purple machines.

This and other intercepted messages were the only information the code-breakers had to help them build their own Purple machine. A breakthrough came when they used stepping switches, part of the telephone technology of the time. By a lucky coincidence, these worked in exactly the same way as the switches in the Purple machine.

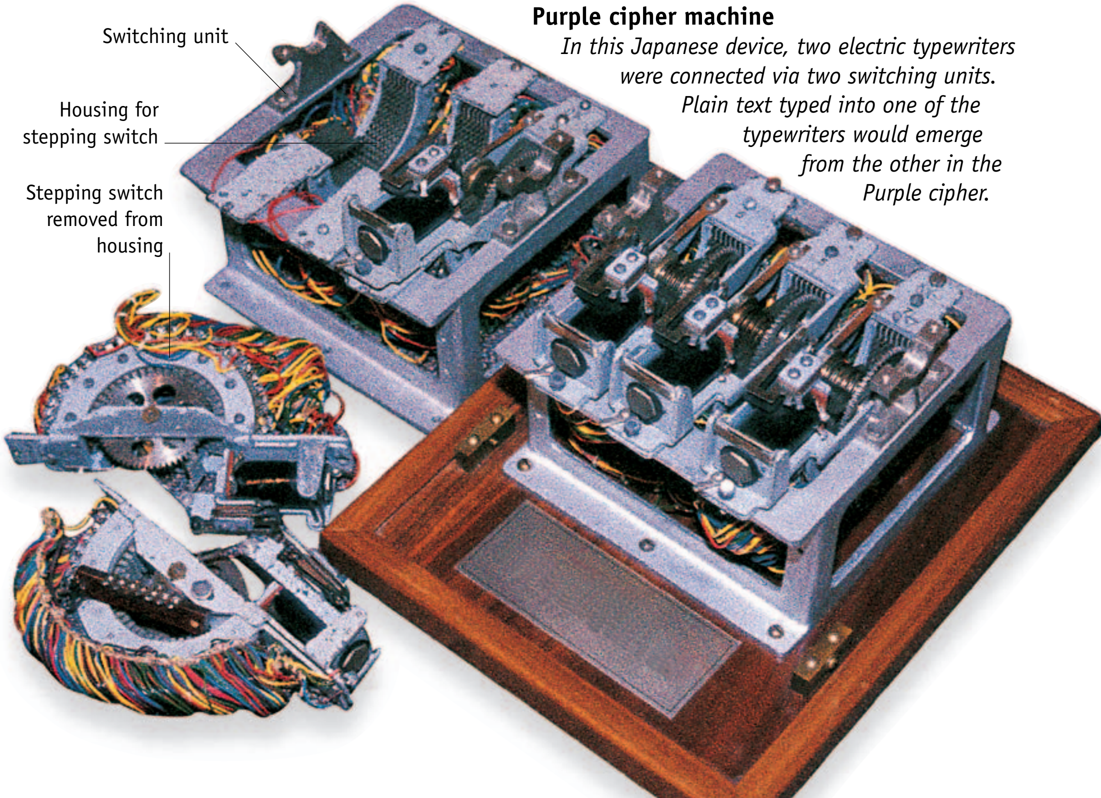
By late 1940, Rowlett and his team of US Navy code-breakers were able to construct a Purple machine. Intelligence deciphered using the machine was called Magic. It was so efficient that Japan's declaration of war—sent to the embassy in Washington a day ahead of the attack on Pearl Harbor to allow time for decipherment—was read by American intelligence before it was presented to the US Secretary of War.

WILLIAM FRIEDMAN

A Russian émigré to the US, William Friedman (1891–1969) was the author of a series of pioneering papers that set out the main principles of modern cryptography. Friedman's wife, Elizabeth, was also an expert cryptographer, and sometimes they collaborated. In 1929, Friedman was appointed the civilian head of the US Army Signal Intelligence Service. In the 1930s, he was a pioneer in the use of machines for code-breaking. After World War II, his work culminated in the formation of the US National Security Agency (see p. 46), an organization that specializes in signals intelligence and cryptography.

How the Enigma was cracked

In 1939, the British, with Polish help, began investigating the German Enigma cipher machine. The Government had set up a Code and Cipher School, which in



Switching unit
Housing for stepping switch
Stepping switch removed from housing

Purple cipher machine

In this Japanese device, two electric typewriters were connected via two switching units. Plain text typed into one of the typewriters would emerge from the other in the Purple cipher.

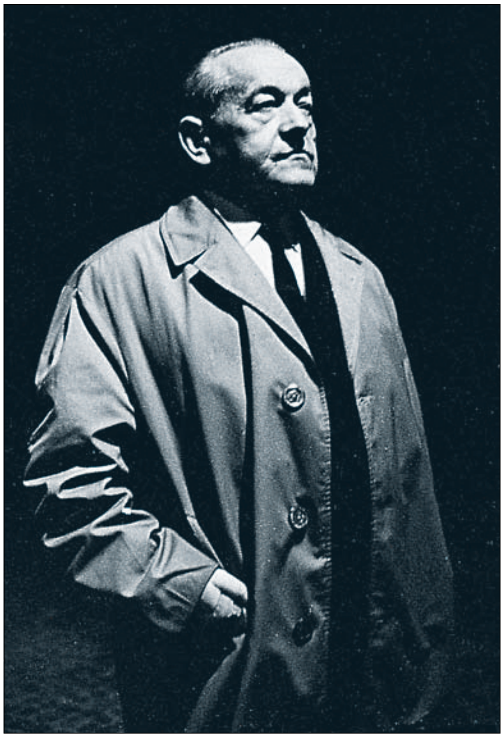
"*This page left intentionally blank.*"

Soviet spy networks

THE TOP PRIORITY for Soviet espionage during World War II was to help defend the Soviet Union against its enemies, Japan and Germany. From the 1930s, Soviet Military Intelligence's Fourth Department (formerly and again later called the GRU) set up spy networks in Japan and Europe. The largest of these was in Western Europe, run from Brussels and later Paris. It was nicknamed the Red Orchestra (Rote Kappelle) by German counterintelligence.

Schulze-Boysen
Soviet agent Harro Schulze-Boysen (1909–42, left) was an officer in the German air force. This picture was taken at the German air ministry.

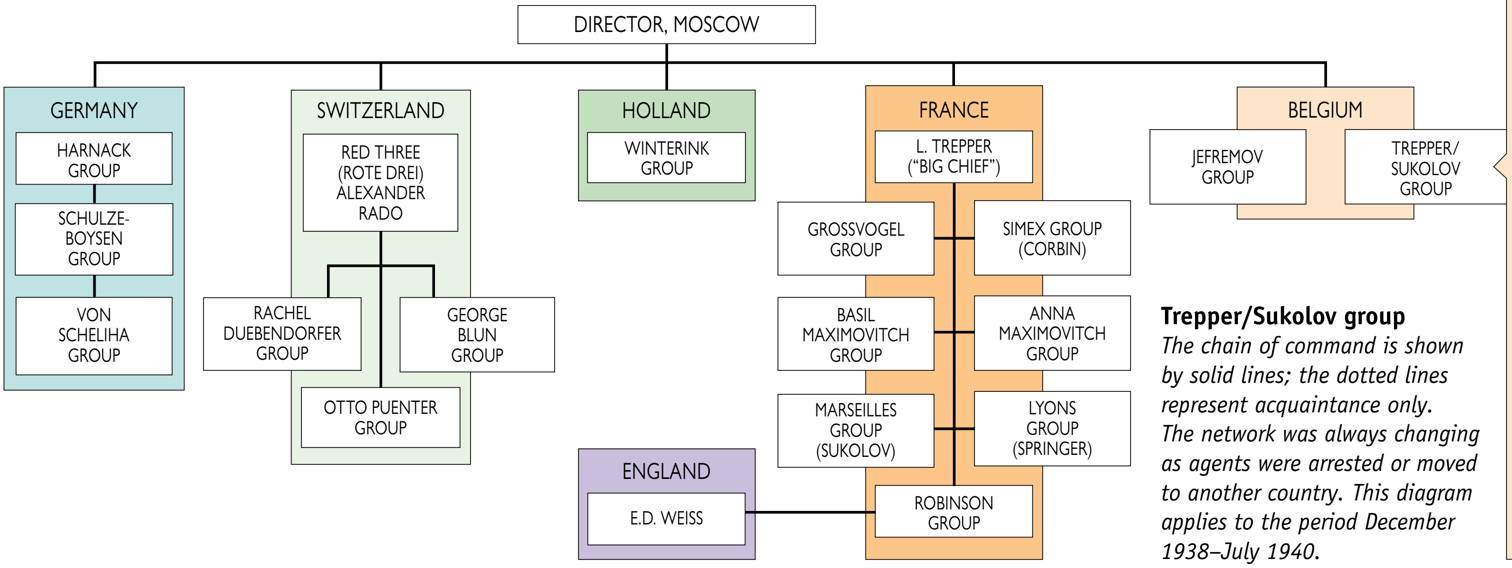
The Red Orchestra was headed by Leopold Trepper and had agents at high levels throughout enemy civil and military structures. It was, however, often frustrated by the poor quality of its clandestine radios, which meant that sometimes the network had to depend on vulnerable human couriers. The network suffered badly from German counterintelligence: the Germans captured important messages from Moscow that led them to identify key members of the network; they



Leopold Trepper
Nicknamed "Big Chief," Trepper (1904–82) went to Brussels in 1938 to launch and operate the Red Orchestra. He later moved to Paris.

THE RED ORCHESTRA

The Red Orchestra was the part of the Soviet spy network that covered Western Europe. It was led by Leopold Trepper and conducted its business under the cover of the Foreign Excellent Raincoat Company. All units reported to Moscow, but not all were in contact with one another. After Trepper's arrest by the Gestapo in 1942, the Red Three unit was the most productive element of the Red Orchestra. This unit was run by Alexander Rado (1899–1981) and operated from Switzerland. Its most important agent was Rudolf Rössler (1897–1958), codenamed Lucy. Today, the Red Orchestra is studied as a classic example of a Soviet intelligence network.



Trepper/Sukolov group
The chain of command is shown by solid lines; the dotted lines represent acquaintance only. The network was always changing as agents were arrested or moved to another country. This diagram applies to the period December 1938–July 1940.

Richard Sorge
This Soviet stamp shows Richard Sorge with a star denoting him to be a Hero of the Soviet Union.

also captured the cipher used for messages from Brussels. Another difficulty was that the Soviet leader Stalin distrusted some of the sources used by the Red Orchestra. For this reason, not all of the information that the Red Orchestra sent to Moscow from Western Europe was believed by the Soviet authorities.

Unheeded warnings

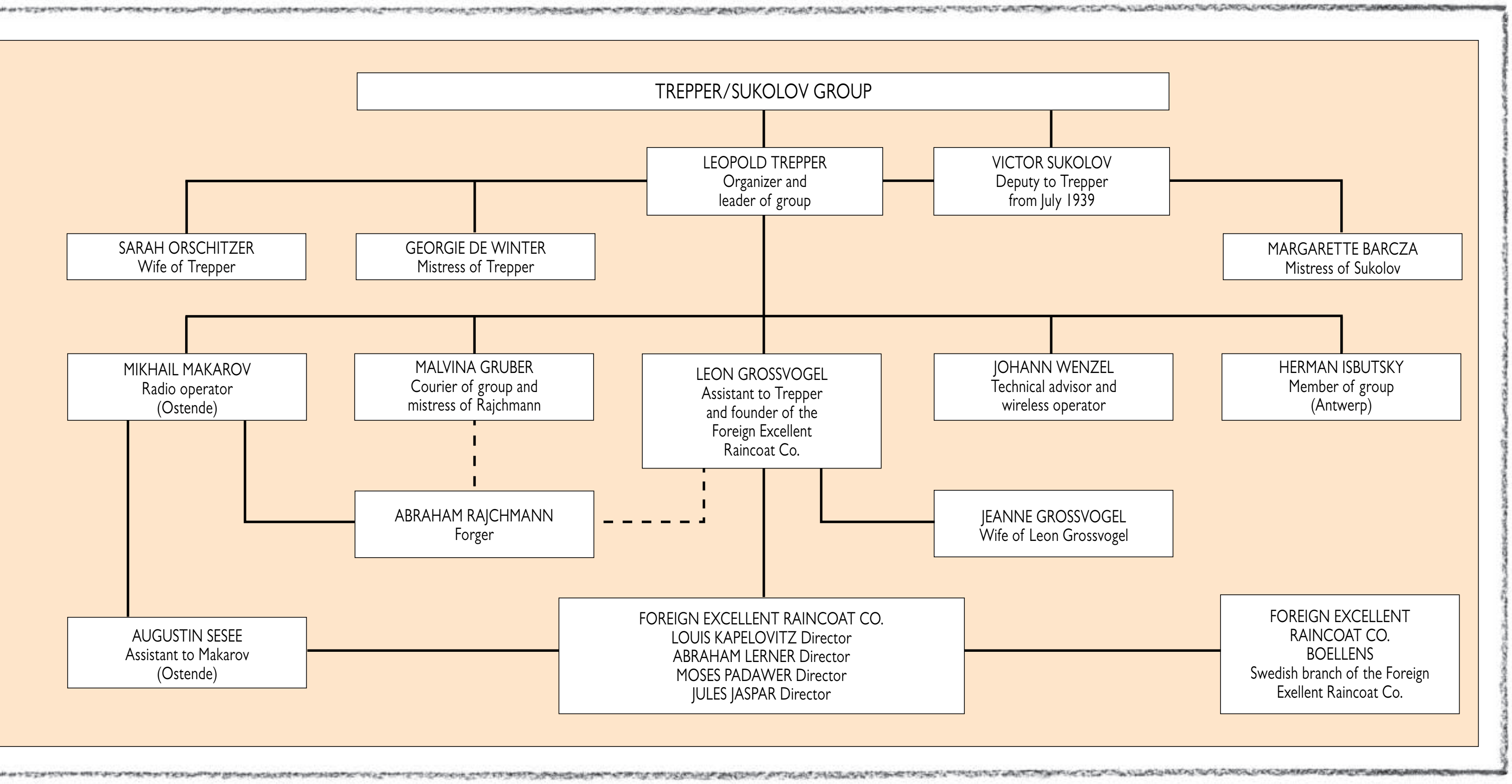
When the Germans invaded France in 1940, Trepper moved to Paris. He went into business as a contractor for the German army. Intelligence that he gathered from sources in the German army enabled Trepper to forewarn Stalin of Hitler's plan to invade the Soviet Union in June 1941 but, like other warnings, this was ignored. Warning of the attack also came from two other Soviet agents in Germany, Arvid Harnack (1901–42)and Harro Schulze-Boysen. They sent German secrets to Moscow by radio, until their arrest and execution in 1942. Trepper was arrested soon afterward. He managed to trick the Germans into believing that he was a double agent. He escaped in 1943, and lived out the war in hiding.

Richard Sorge

Long before Japan entered the war in 1941, Moscow feared a Japanese invasion. The Fourth Department sent Richard Sorge (b.1895), a spy who was half German, to Tokyo in 1933. Posing as a German journalist, Sorge befriended the German military attaché in Tokyo, Eugene Ott, and a Japanese journalist, Hotsumi Ozaki (1901–44). In July 1941, Sorge learned from them that Japan was more likely to begin its military campaign in Southeast Asia than to attack the Soviet Union.

Hotsumi Ozaki
Recruited by Sorge in 1930, Ozaki gathered intelligence from Japanese political circles.

If it were true, this information would enable some Soviet armies to be moved from defensive duties on the Soviet Union's eastern borders and used to fight the Germans attacking Moscow. Stalin did not believe it, however, just as he had not believed Sorge's warning of Germany's attack in May 1941. Only later in 1941 was Stalin ready to believe Sorge's information about Japan, when signals intelligence confirmed it. Stalin was then able to move more troops from the east to halt the German invasion. Sorge was arrested and executed in Japan in 1944.


TREPPER/SUKOLOV GROUP
LEOPOLD TREPPER
Organizer and leader of group
VICTOR SUKOLOV
Deputy to Trepper from July 1939
SARAH ORSCHITZER
Wife of Trepper
GEORGIE DE WINTER
Mistress of Trepper
MARGARETTE BARCZA
Mistress of Sukolov
MIKHAIL MAKAROV
Radio operator (Ostende)
MALVINA GRUBER
Courier of group and mistress of Rajchmann
LEON GROSSVOGEL
Assistant to Trepper and founder of the Foreign Excellent Raincoat Co.
JOHANN WENZEL
Technical advisor and wireless operator
HERMAN ISBUTSKY
Member of group (Antwerp)
ABRAHAM RAJCHMANN
Forger
JEANNE GROSSVOGEL
Wife of Leon Grossvogel
AUGUSTIN SESEE
Assistant to Makarov (Ostende)
FOREIGN EXCELLENT RAINCOAT CO.
LOUIS KAPELOVITZ Director
ABRAHAM LERNER Director
MOSES PADAWER Director
JULES JASPAR Director
FOREIGN EXCELLENT RAINCOAT CO.
BOELLENS
Swedish branch of the Foreign Exellent Raincoat Co.

Japanese intelligence

JAPAN'S INTELLIGENCE organization in World War II had several elements. Abroad, embassies played a key role coordinating the gathering of intelligence. Within Japan, the Tokko—a special bureau of the Tokyo police force—was responsible for domestic counterintelligence. The armed services also had their own intelligence sections, with the military police (Kempei Tai) covering counterintelligence activities in territories occupied by the Japanese.

The Tokko was formed in 1911 with the purpose of suppressing "subversive thoughts" and defending Japan's strictly regulated political system. It did much to prevent the rise of communism in Japan in the years after World War I.

Counterintelligence

By 1932, the Tokko had become Japan's chief internal counterintelligence organization. It was divided into four sections: the first monitored left-wing political activists; the second maintained files on the right wing; the third section watched foreign residents and embassies; and the fourth monitored friendly embassies, like that of Germany.

The domestic responsibilities of the Kempei Tai were officially limited to matters concerning members of the armed services. However, the right-wing military movement that dominated Japanese politics used the Kempei Tai to intimidate opposition politicians, arresting those who campaigned against the political order of the time as "terrorists." During the war, the power of the Kempei Tai was enhanced by the patronage of the prime minister, Hideki Tojo, who had been one of its officers early in his career. In territories occupied by Japan during the war, such as parts of China and much of Southeast Asia, the Kempei Tai operated with extreme ruthlessness, gaining a brutal reputation similar to that of the Gestapo in Germany (see p. 34).

Admiral Yamamoto

Isoroku Yamamoto (1884–1943) planned the attack on the Pearl Harbor base of the US Pacific Fleet, making use of intelligence obtained from a Japanese spy.

Achievements and failures

Immediately after the Japanese capture of Singapore in February 1942, the Kempei Tai arrested hundreds of Chinese Singaporeans, whom it considered to be security risks, and executed them at night on beaches near the city center. Later, in 1944, naval Kempei Tai units were responsible for hunting down and executing a team of saboteurs from Allied countries, who had attempted to raid Singapore Harbor (see p. 131). Despite the zeal of Japanese counterintelligence efforts, a major spy ring working for the Soviet Union managed to flourish in Tokyo in the late 1930s and early 1940s. This spy network, created by Richard

The attack on Pearl Harbor

A Japanese naval officer in Hawaii provided intelligence on American ship movements until hours before the attack on December 7, 1941.

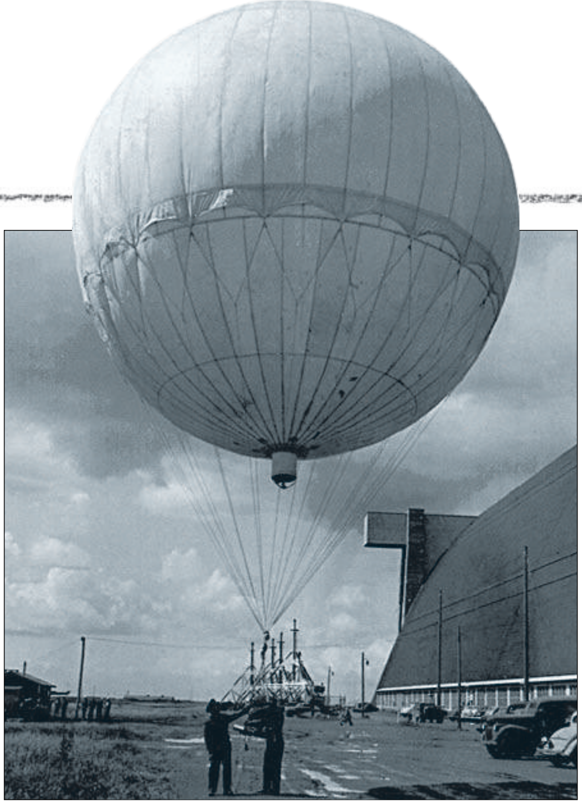
Consul-General Nagao Kita
As Japanese consul-general in Honolulu, Hawaii, Kita provided the enciphering facilities for the naval spy Takeo Yoshikawa.

Sorge (see p. 39), passed a great deal of highly important information to Moscow before it was discovered in 1941. One reason for Sorge's great success may have been that the Tokko was overburdened by the enormous volume of meaningless reports that it received from overeager informants.

SABOTAGE BALLOONS

Throughout World War II the continental United States lay outside the range of bombers from either Germany or Japan. Nevertheless, the Japanese brought the United States under an unusual kind of aerial bombardment. Between 1944 and 1945, some 6,000 balloons bearing incendiary charges were launched from Japan.

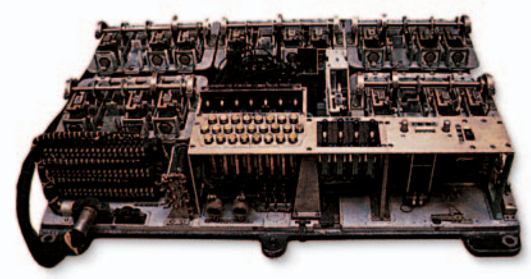
The balloons were carried by the prevailing winds, and dropped their charges over the heavily forested northwest of America. At least 369 balloons completed the 6,000-mile (9,700-km) journey. The only fatalities, however, were a family of seven, who were killed by a single balloon.



Japanese sabotage balloon
The Japanese used balloons carrying incendiary devices to bombard the United States. They were wind-borne, and were primarily intended to cause forest fires.

Intelligence in the Pacific

In the months before Japan's entry into World War II, Japanese army intelligence established its secret agents throughout Southeast Asia, as part of what was known as Organization F. Meanwhile, Japanese naval intelligence scored a major success in securing information on the US Navy base at Pearl Harbor in Hawaii, which Japan intended to attack. In March 1941, Japanese naval ensign Takeo Yoshikawa (1914–93) traveled to the Hawaiian islands under an assumed name. From then until Japan's surprise attack on the base on December 7, 1941, he sent weekly reports on the dispositions of American warships. Yoshikawa was familiar with the organization and structure of the American Navy. He possessed no code of his own but sent his messages through diplomatic channels, under the signature of Japanese Consul-General Nagao Kita. American code-breakers could read the coded Japanese diplomatic mail, sent by cable (see p. 36), but the cable authorities in Hawaii, for reasons never explained, did not pass on the relevant cable traffic to the American authorities. Yoshikawa's last message was transmitted just 12 hours before the Japanese began their attack on Pearl Harbor.

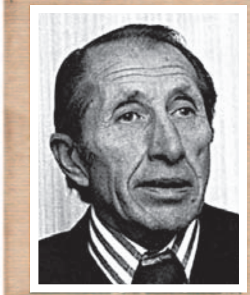


Purple cipher machine
The Japanese diplomatic service used the Purple machine to encode correspondence (see p. 36).

Intelligence in Europe

Another Japanese intelligence operation was run from Spain, a neutral country. This group was the TO network, which gathered intelligence on Allied shipping from agents in the United States and elsewhere. The coordinator of TO was Yakichiro Suma, who held the rank of a minister in the Japanese embassy in Madrid. Intelligence from TO was used by the Germans as well as the Japanese.

DUSAN POPOV



SPY PROFILE

Dusan "Dusko" Popov (1912–81) was a Yugoslav double agent, ostensibly working for the Abwehr (see p. 34) but actually controlled by the British. In 1941, the Abwehr sent him to the US with a list of questions, including some about Pearl Harbor. Popov gave the list to the director of the FBI, J. Edgar Hoover, but the Americans took no action regarding Pearl Harbor. As a result, the significance of this interest in the US Navy base was overlooked.

COLD WAR

U-2 spy plane
Introduced in 1956, the U-2 operated at such a high altitude that it was out of range of the Soviet aircraft and missiles of the time.

THE PERIOD OF CONFRONTATION between East and West that ran from 1945 until the fall of communism in the early 1990s is known as the Cold War. At the very beginning of this period, the Soviet Union's former wartime allies in the West were shocked to discover the extent of Soviet espionage activity that was directed against them. The United States responded (see p. 46) by creating its own foreign intelligence organization, the Central Intelligence Agency (CIA). Later, the National Security Agency (NSA) was set up as a central body for signals intelligence and cryptography. Counterintelligence within the United States remained the responsibility of the Federal Bureau of Investigation (FBI).

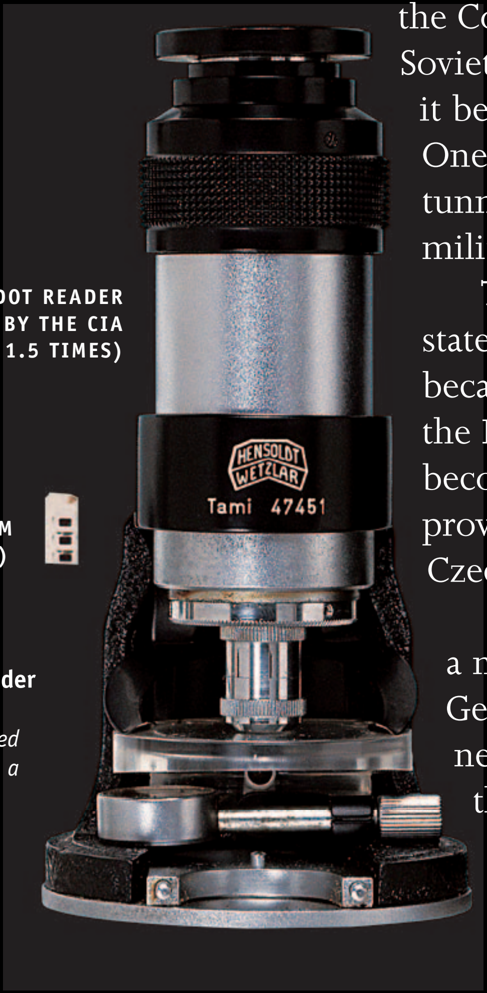
National Security Agency emblem
America's NSA is responsible for information security, foreign signals intelligence, and cryptography.

HUMAN INTELLIGENCE

The divided city of Berlin was in the forefront of espionage operations in the Cold War. Surrounded by the Soviet sector (later East Germany), it became an international center of intelligence activity. One of the most notable incidents was the digging of a tunnel by the CIA and MI6 to intercept a cable carrying military communications to Moscow (see p. 44).

The capture of Berlin in 1945 had given the Soviet state intelligence organization, the NKGB (which later became the KGB), control of Nazi records. This enabled the NKGB to blackmail many West German citizens into becoming spies. The secret police files of other states also provided blackmail material, as in the example of the Czech spy known as Anna (see p. 48).

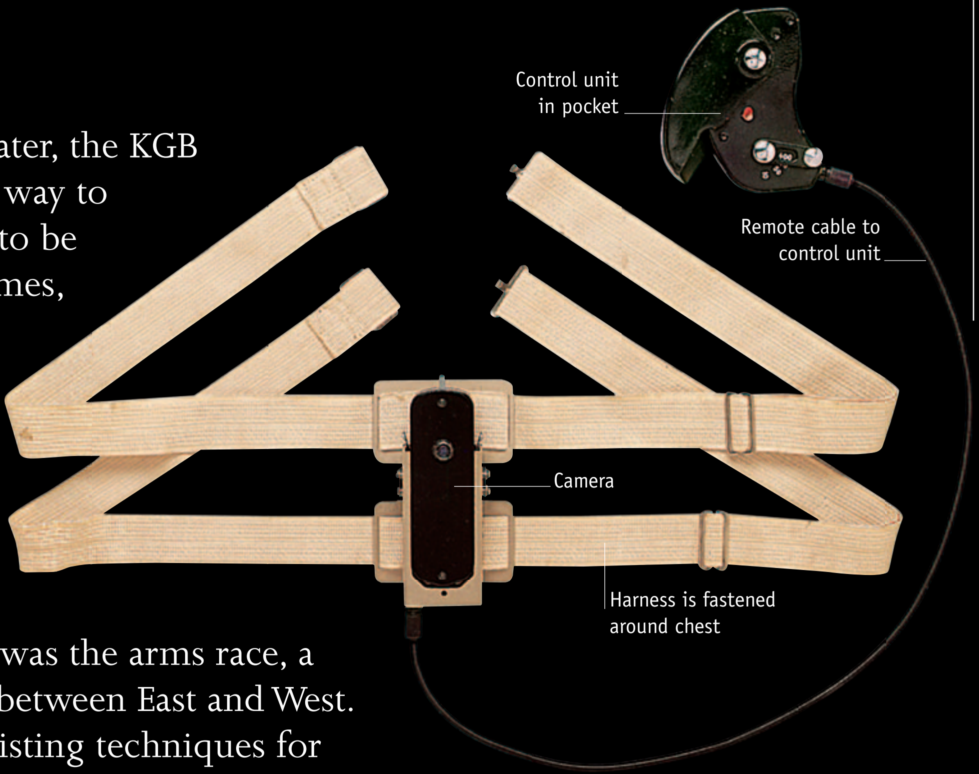
The Soviet Union was also successful in operating a number of spies in Britain. Notable among these were George Blake (see p. 203), Gordon Lonsdale and his network of agents (see p. 50), and, most damagingly, the five members of the Cambridge ring (see p. 209). Most of these early Soviet spies were motivated by



MICRODOT READER USED BY THE CIA (ENLARGED 1.5 TIMES)
MICRODOT FILM (ACTUAL SIZE)
HENSOLDT WETZLAR
Tami 47451

Microdot film and reader
During the Cold War, microdots were much used to convey intelligence in a miniaturized form. They can be read only under powerful magnification.

ideology or the threat of compromise. Later, the KGB found the lure of money was the easiest way to recruit. The most important KGB agents to be exposed in the United States in recent times, John Walker (see p. 54) and Aldrich Ames (see p. 202), both offered their services for money. Ames operated as a mole inside the CIA, while Walker sold secrets from within the US Navy.


Control unit in pocket
Remote cable to control unit
Camera
Harness is fastened around chest

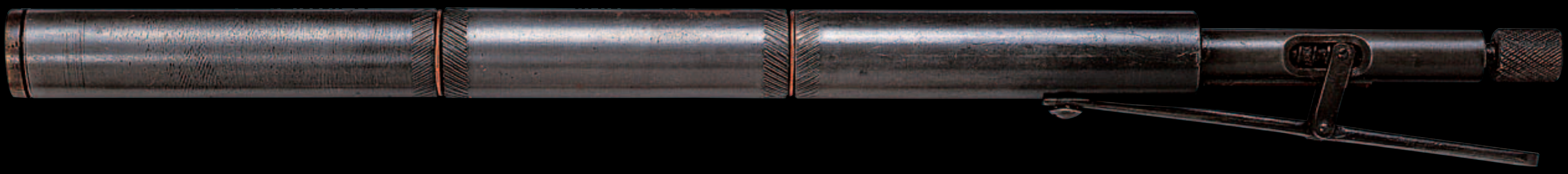
Necktie camera
Worn inside an intelligence officer's clothing, this KGB camera took photographs through a fake tiepin. It was operated by a remote shutter release that was concealed in the pocket.

SPIES IN THE SKY

Another major element of the Cold War was the arms race, a contest for nuclear weapons supremacy between East and West. In this struggle the CIA found that its existing techniques for intelligence-gathering were inadequate for assessing the nuclear strength of the Soviet Union. This led to the development of the U-2 spy plane, which was able to conduct high-altitude photographic reconnaissance (see p. 52). Besides flying over the Soviet Union, the U-2 monitored developments on Cuba in 1962, revealing the presence of Soviet medium-range nuclear missiles. This precipitated the Cuban Missile Crisis, the most dangerous event of the Cold War, resolved only when America's civilian leaders overruled the military. Another technological race arose from the Soviet Union's launch of the first satellite in 1957 (see p. 58). By 1961, satellites were being used for photographic reconnaissance, though the early technology necessitated jettisoning the film for recovery and development on Earth. In 1976 the Americans began using digital technology, enabling satellites to beam back high-definition images as soon as they were taken. Such developments have become a prime target for espionage.

Soviet stamp
This postage stamp commemorates 50 years of Soviet security services.

KGB gas gun
Developed during the Cold War for assassinating political opponents of the Soviet regime, this weapon emitted cyanide gas, capable of causing almost instant death.

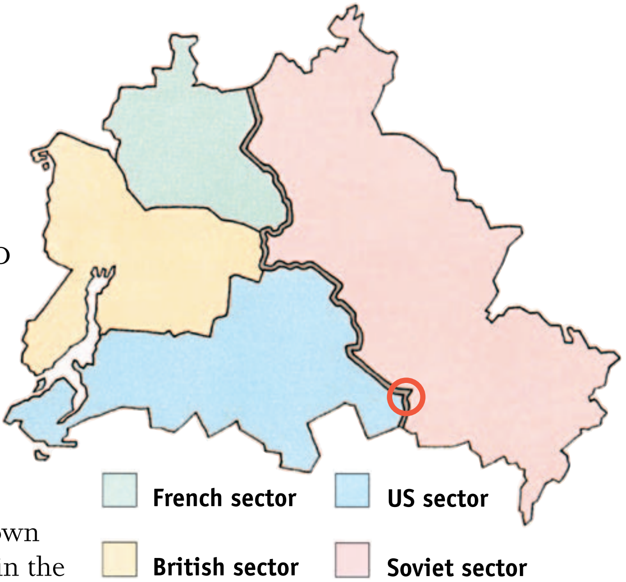


Berlin: spy city

THE GERMAN CITY OF BERLIN occupied a unique position during the Cold War years that followed World War II. After the end of the war, the victorious Allies—the United States, Britain, France, and the Soviet Union—divided Germany into zones of occupation. The old capital, Berlin, was similarly divided into four zones, even though it was surrounded by the Soviet zone of occupation, which became the German Democratic Republic, or East Germany.

Reinhard Gehlen
A German intelligence officer during World War II, Gehlen (1902–79) worked for the Americans after the war. He became head of the West German intelligence service.

The Soviet Union soon sealed off its own zone from Western interference. Within the Soviet sector, the MGB (state security) and GRU (military intelligence) operated without restriction, confiscating German industrial machinery, even whole factories, to be sent back to provide jobs in Soviet towns. German scientists were rounded up and made to work for Soviet industry.

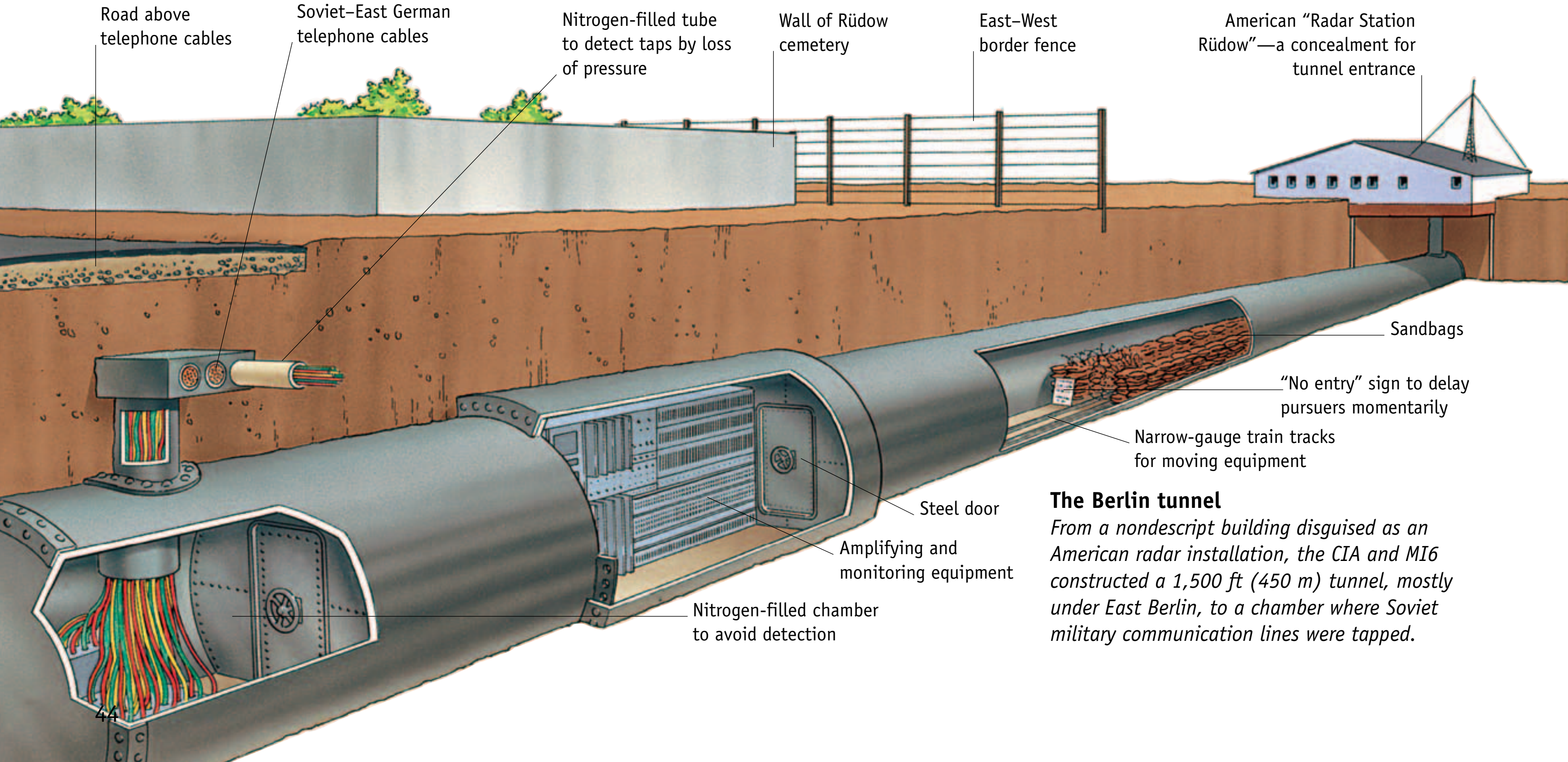


A divided city
Isolated within Soviet-occupied territory, later to become East Germany, Berlin was divided by the wartime Allies into four zones of occupation. The red circle shows the position of the Berlin tunnel, used to tap into Soviet military communications.

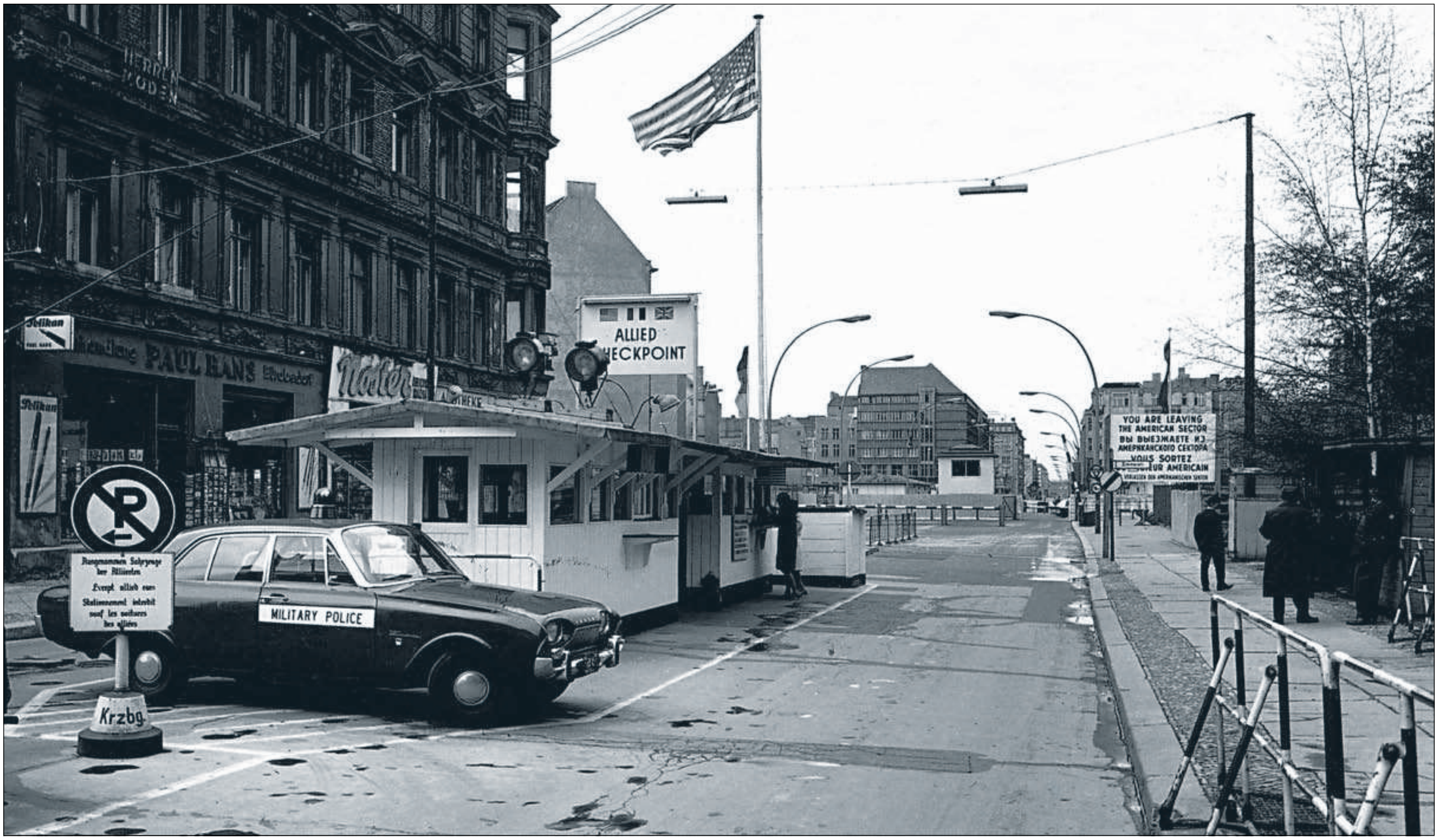
Intelligence activity

Meanwhile, agents were recruited to begin spying in the West. Captured Nazi records provided plenty of material with which to blackmail potential agents. West Germans with relatives in the East could also be coerced, by threats to their families, into assisting the Soviet Union. As a result, between 1950 and 1969 a total of 2,186 agents were convicted of espionage in West Germany, and 19,000 admitted espionage but were not prosecuted.

The head of the West German Foreign Intelligence Service (BND) for most of this period was Reinhard Gehlen. During the war, he had headed the section of


Road above telephone cables
Soviet–East German telephone cables
Nitrogen-filled tube to detect taps by loss of pressure
Wall of Rüdow cemetery
East–West border fence
American "Radar Station Rüdow"—a concealment for tunnel entrance
Sandbags
"No entry" sign to delay pursuers momentarily
Narrow-gauge train tracks for moving equipment
Steel door
Amplifying and monitoring equipment
Nitrogen-filled chamber to avoid detection

The Berlin tunnel
From a nondescript building disguised as an American radar installation, the CIA and MI6 constructed a 1,500 ft (450 m) tunnel, mostly under East Berlin, to a chamber where Soviet military communication lines were tapped.



Checkpoint Charlie
This famous crossing place in the Berlin Wall was the site of several successful escapes from the East, some failures, and a dangerous confrontation between American and Soviet tanks in 1961.

German military intelligence responsible for the Soviet Union. He surrendered to the Americans in 1945 but persuaded them to employ him and his staff as spies in return for files and names gathered by his wartime espionage network.

In 1949, Gehlen's organization continued its work with the newly formed CIA and in 1956 it became the BND. Gehlen remained in his position until 1968, when his reputation was tarnished by the discovery of double agent Heinz Felfe (see p. 139) among his headquarters' staff.

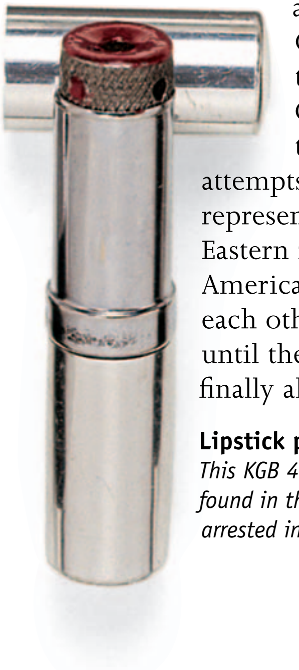
Underground interception

One of the Cold War's most ambitious intelligence operations was mounted in Berlin in 1954 by the CIA and Britain's MI6. From just inside West Berlin, the CIA dug a tunnel 1,500 ft (450 m) long to reach a point directly beneath the underground telephone lines by which the Soviet military HQ in East Berlin communicated with Moscow. MI6 then tapped into these lines. The tunnel functioned for a year before it was found by East German repair men. The intelligence gathered was mainly about the disposition of Soviet army units. Had the Soviets planned an invasion of the West, the tap might have provided a warning.

In later years, it emerged that the KGB spy George Blake (see p. 203) had warned his controllers about the tunneling operation. However, the controllers did not inform the GRU or the Red Army in order to protect Blake from being exposed as a mole.

The Berlin Wall

On August 13, 1961, the East German police began building a fence between East and West Berlin. This grew into a 96 mile (155 km) concrete structure with watchtowers and minefields, encircling all of West Berlin. Roads controlled by army checkpoints were allowed through the wall. On October 27, 1961, at the American Checkpoint Charlie, a confrontation took place over Soviet attempts to deny American representatives access to the Eastern zone. For 16 hours American and Soviet tanks faced each other across no-man's-land, until the representatives were finally allowed through.



Lipstick pistol
This KGB 4.5mm single-shot firing device was found in the purse of an East German spy arrested in West Berlin.

US security agencies

AFTER WORLD WAR II, the United States established a number of new organizations to meet the Cold War intelligence threat. The main three, the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Defense Intelligence Agency (DIA) collected and analyzed foreign intelligence. A fourth key organization, the Federal Bureau of Investigation (FBI), was already in charge of counterintelligence within the United States. Only one other country had a larger security system than America—the Soviet Union (see p. 38). But in the field of technical intelligence-collection systems the United States had the edge.

CIA CREST

J. Edgar Hoover
Hoover (1895–1972) directed counterintelligence during World War II, and tried in vain to bring foreign intelligence-gathering under FBI control.

Apart from these major American security organizations, there are also many other agencies of the United States government that are responsible for aspects of security. While some are often in the public eye, others operate in the closest possible secrecy.

Federal Bureau of Investigation

Established in 1909 as part of the US Department of Justice, the FBI became a national agency in 1934. Since 1939, it has been the primary organization responsible for the various aspects of domestic counterintelligence: it is charged with detecting and neutralizing all espionage, sabotage, and other clandestine activities carried out within the United States by hostile foreign intelligence services. The Washington Metropolitan Field Office of the Bureau has been involved in resolving a number of major spy cases, including the very damaging Walker case (see p. 54). The FBI works closely with the CIA, which is responsible for counterintelligence overseas. The CIA has no powers of arrest, and cooperates with the FBI to deal with traitors and spies within CIA ranks. Since the arrest in 1994 of SVR mole Aldrich Ames (see p. 202) in the CIA, the FBI and CIA have cooperated even more closely with each other.

Central Intelligence Agency

Created under the National Security Act of 1947, and based on a concept formulated in 1944, the CIA is made up of several directorates. The National Clandestine Service is responsible for the clandestine collection of all foreign intelligence, and for counterintelligence gathered from outside the United States. The Directorate of Intelligence is responsible for both the analysis of intelligence and the production of

FBI emblem
This is an emblem from the FBI headquarters in Washington, DC. The FBI is part of the US Department of Justice.

Allen Welsh Dulles
An OSS veteran and Director of the CIA from 1953–61, Dulles (1893–1969) ran covert operations in Iran and Central America, as well as the disastrous Bay of Pigs operation in Cuba.

finished reports. The CIA also has a Directorate for Science and Technology, which is comprised of various offices. The Office of Technical Service (OTS)—often likened to Ian Fleming's "Q Branch"—is described on p. 96. Several offices provide administrative services. The Office of SIGINT Operations assists the NSA in gathering foreign signals intelligence. The Foreign Broadcast Information Service (FBIS) monitors radio and television broadcasts around the world and produces transcripts of broadcasts, some of which are available to the media and the public. In the past, the National Photographic Interpretation Center provided the United States intelligence community with analysis of overhead reconnaissance photographs, taken either from satellites or aircraft. The analysis of photographs is now carried out by the National Imagery and Mapping Agency (NIMA), which is not part of the CIA.

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSA CREST

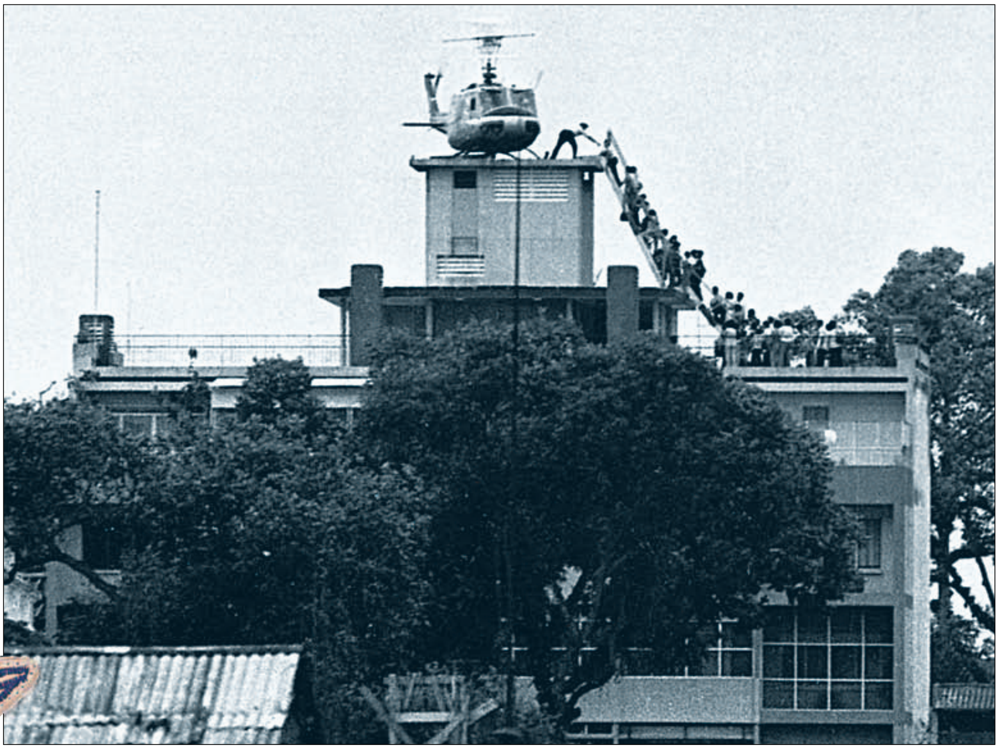
National Security Agency

The NSA was established in 1952 and has three main areas of activity. The first is information security, which means the protection of all national security systems and information, including computer systems. The second is the collection of foreign signals intelligence (SIGINT). The NSA's third area of activity is the creation of codes and ciphers for use by US national intelligence agencies and the US military. The NSA also attempts to break the codes and ciphers of foreign powers.

AIR AMERICA

On the surface, Air America was a normal American commercial airline; but it was in fact covertly operated by the CIA to support its operations throughout Southeast Asia. It evolved from a little-known organization, Civil Air Transport (CAT), which had been formed in China in 1946 to support American covert operations. At its peak during the Vietnam War (1959–75), Air America ran the world's largest commercial fleet of aircraft. Its pilots were often ex-military personnel, attracted by generous wages. They flew a variety of aircraft in support of CIA operations, sometimes (in great secrecy) carrying agents across national borders. One group, using U-2 and SR-71 jets, flew secret reconnaissance missions from Thailand. Air America was sold after the war and operates simply as a small-scale air charter company.

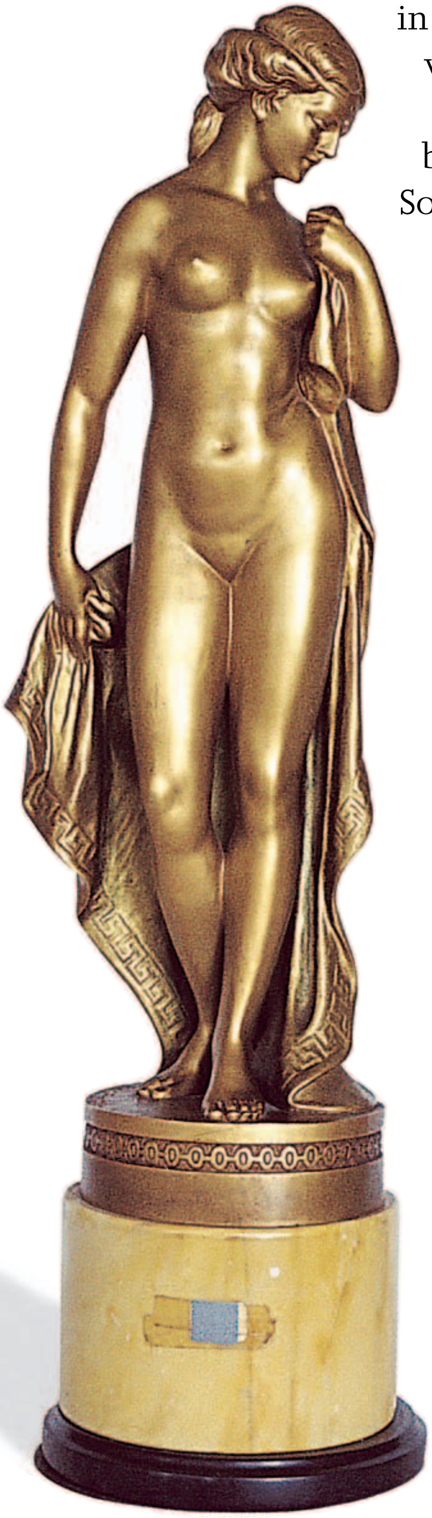
EMBLEM WORN BY AIR AMERICA PILOTS



Air America in action
At the end of the Vietnam War in 1975, the Southern capital, Saigon, finally fell to North Vietnamese forces. Here, some South Vietnamese intelligence officers are being evacuated by an Air America helicopter from the residence of the CIA Deputy Chief of Station in Saigon.

Codename Anna

ANNA WAS THE CODENAME given to the Czech spy Alfred Frenzel. A member of the Czech Communist Party in the 1930s, Frenzel went to England as an agent of the Czech government in exile when Germany invaded Czechoslovakia in World War II. At the end of the war, Europe was divided into a "democratic" West and an eastern bloc of countries dominated by the Soviet Union. Frenzel emigrated to the newly created state of West Germany, where he eventually became a member of parliament.



BRONZE STATUE

Intelligence coup
Alfred Frenzel (1899–1968) became Czechoslovakia's most important spy in West Germany during the late 1950s, operating under the codename Anna.

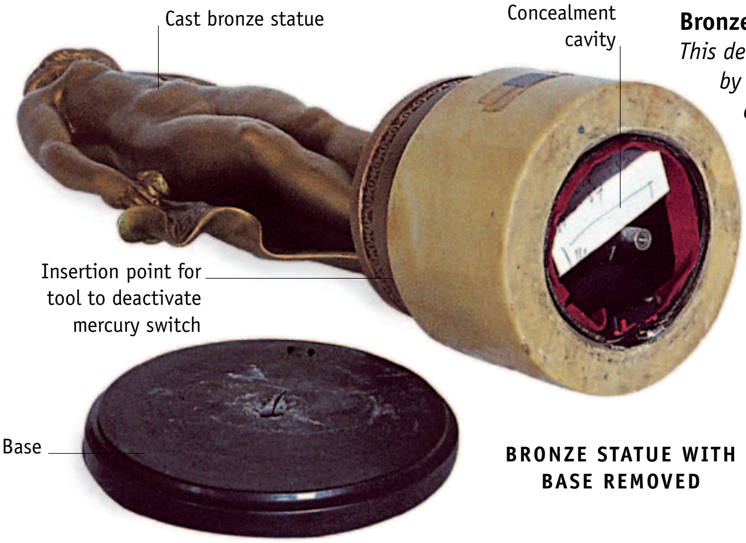
Czechoslovakia, in the meantime, became a communist state. The new state intelligence service (Statni tajna Bezpecnost or StB), examined the files of the prewar military intelligence and political police, and found information on Frenzel's past activities.

In West Germany, Frenzel had now been appointed to the parliamentary defense committee, which was responsible for the reestablishment of the West German armed forces, and for their future role in NATO.

Recruiting the spy

The StB investigators saw that Frenzel's position could be exploited and sent his file to the head of StB's First Directorate, known as I Sprava. This body was in charge (under the control of the Soviet KGB) of foreign intelligence gathering. I Sprava decided to recruit Frenzel as a spy and assigned the task to StB Major Bohumil Molnar in Vienna. In April 1956, Frenzel was visited by an old friend who had become an employee of the Czech government. He offered Frenzel a job and threatened to expose Frenzel's past political and criminal record if he refused. In addition, he made certain threats regarding the safety of Frenzel's wife, who was visiting Prague at the time. Forced to agree, Frenzel traveled to Vienna for a meeting at which he received 1,500 West German marks and was

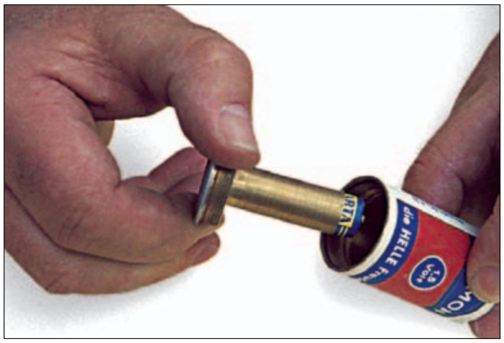
Bronze statue container
This device was made in Czechoslovakia by the StB's Technical Directorate. To open it, a mercury switch must be deactivated; otherwise an explosive charge will destroy the contents.



BRONZE STATUE WITH BASE REMOVED

MERCURY SWITCH

FILM CONTAINER



Battery film container
This battery could power a torch, but could also be used to hide film. If the battery container was not opened correctly, the film was destroyed by acid.

given the codename Anna. In July he put his signature on a document that showed that he had links with the StB. Having signed this, Frenzel was now trapped: the Czechs would be able to blackmail him if he did not spy for them.

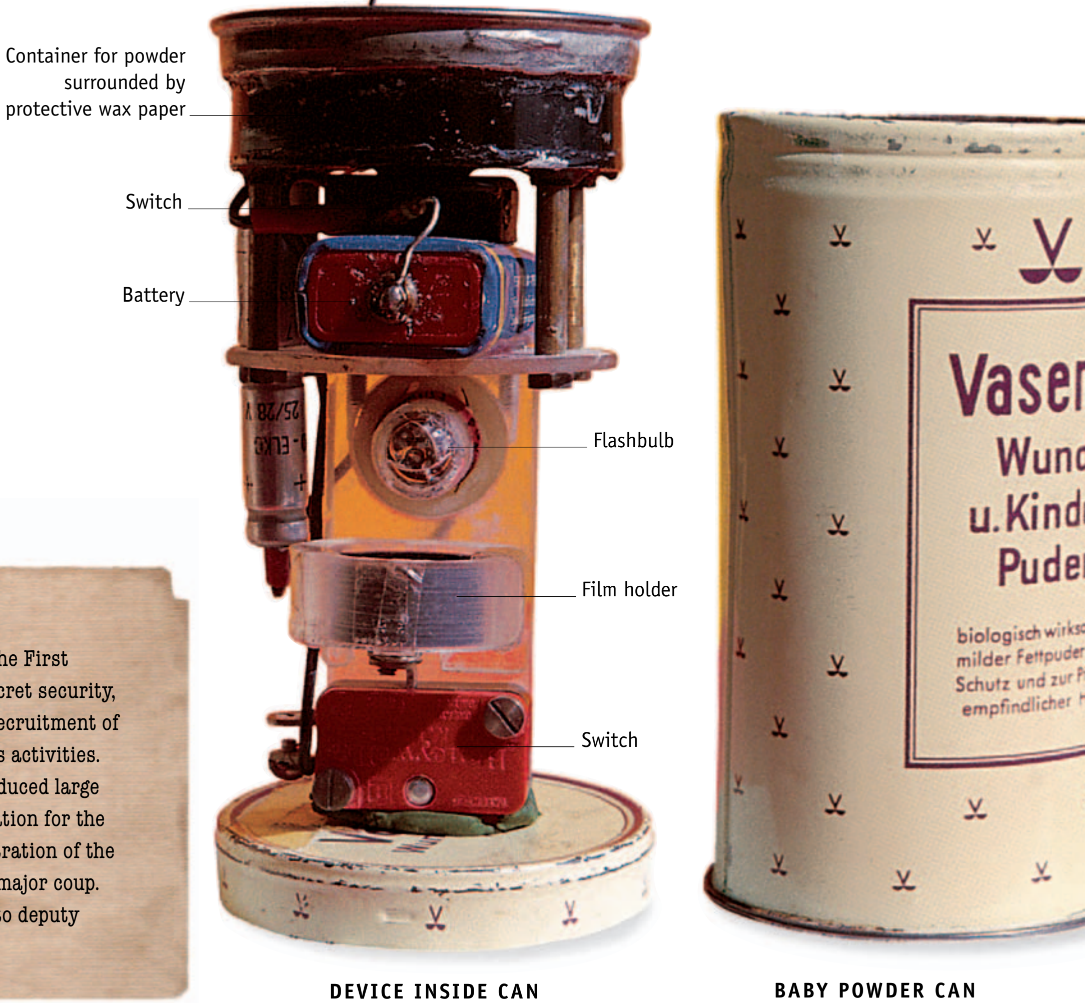
Frenzel began to pass information to his handlers, including a copy of the entire West German defense budget. In return, he was promised a large salary, to be paid into a Czech bank account, and a villa and car in Czechoslovakia should he eventually choose to defect. Frenzel also received money for each batch of information he provided. Subsequent batches included West German Air Force plans, and details of new American and German aircraft and missiles. In September 1959, control of Anna was passed to a new StB officer operating as an illegal (see p. 217) under the assumed name of Franz Altman. For transporting secret information, Altman used a range of containers that had been disguised as everyday objects by the StB's Technical Directorate, known as IX Sprava. The containers were designed in such a way that their contents would be destroyed if tampered with.

The unmasking of Anna

Altman's method was to pass his disguised containers to Czech diplomatic couriers, who would carry them, with all Frenzel's information, out of West Germany. In October 1960, the West German counterintelligence service, the BfV, started to watch Altman after the tax authorities became suspicious of him. This led to the discovery of his role as a spy. Altman was arrested while trying to leave the country with six rolls of film in a fake baby powder can. The can had to be disarmed before opening (see below).

When developed, the film revealed photographs of secret documents that were traced back to Frenzel: he had failed to cover the reference numbers when photographing them. He was arrested and given a 15-year sentence, but was exchanged for four West German spies in a swap five years later. He died in Czechoslovakia in 1968.

Film container in a baby powder tin
An internal electrical circuit had to be turned off before this container could be opened, otherwise it fired a flashbulb, which would ruin the film.



DEVICE INSIDE CAN

BABY POWDER CAN

BOHUMIL MOLNAR

SPY PROFILE

Bohumil Molnar was a major in the First Directorate of the Czech state secret security, StB. He was entrusted with the recruitment of "Anna" and the supervision of his activities. For five years, this operation produced large quantities of intelligence information for the StB and the KGB. The StB's penetration of the West German government was a major coup. Molnar's reward was promotion to deputy director of the StB.

House of spies

NUMBER 45 CRANLEY DRIVE, a small bungalow in the west London suburb of Ruislip, provided the technical support for a Soviet spy network. The head of the network was Konon Trifimovich Molody, alias Gordon Lonsdale. As a KGB "illegal" officer without embassy protection, Lonsdale reported directly to Moscow and operated under a legend (see p. 206). He arrived in London in 1955 and, using KGB funds, set up a slot-machine leasing company which, as he later claimed, was so successful that it generated a profit for the KGB. For six years, Lonsdale lived the life of a well-to-do businessman and surrounded himself with beautiful women.

45 Cranley Drive, Ruislip
This unremarkable bungalow, in a residential London suburb, was the Krogers' home and base for Lonsdale's communications with Moscow.

At the same time, Lonsdale ran a network of agents in Britain. He did not recruit agents himself but used those who had already been recruited. The Cohens, for example, had been active as Soviet agents in New York. Houghton had been recruited by Polish intelligence.

The Krogers

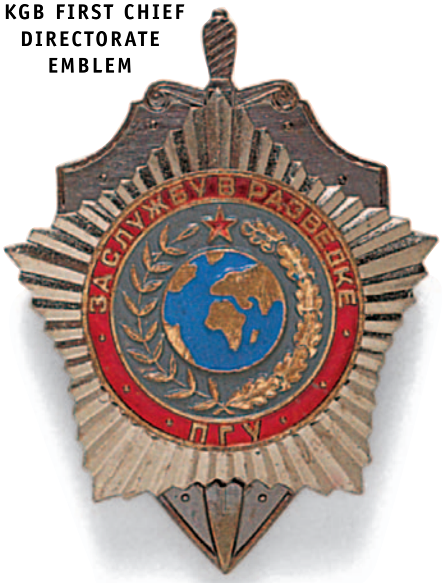
The couple who lived apparently normal lives at 45 Cranley Drive were Lona Cohen (1913–92) and Morris Cohen (1910–95), operating under the aliases of Helen and Peter Kroger. They provided Lonsdale with the technical support that he needed to pass on his intelligence information to the KGB headquarters in Moscow. The "Krogers" ran a small business as antiquarian book dealers, and this provided them with opportunities to smuggle microdots hidden in the books they bought and sold internationally. They sent these books to various addresses abroad, from which they were then forwarded to the Soviet Union. The Krogers' radio and burst transmitter (see p. 152) were reserved for urgent communications with Moscow.

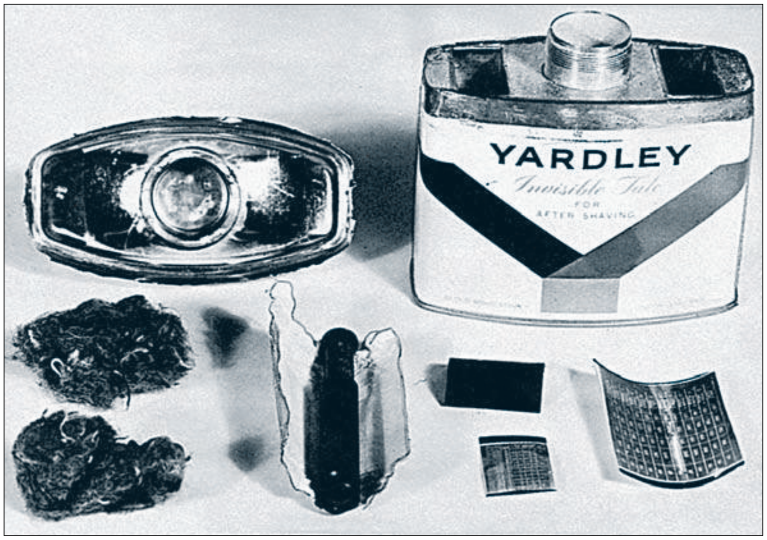
MORRIS AND LONA COHEN, ALIAS PETER AND HELEN KROGER

KGB FIRST CHIEF DIRECTORATE

The KGB was divided into a number of directorates, the most prominent of which were the First Chief Directorate, commonly known as the FCD, and the Second Chief Directorate, commonly known as the SCD, which was in charge of domestic security. The FCD was responsible for overseas operations, and had several subdirectorates. Directorate T gathered scientific and technical intelligence. Directorate K infiltrated foreign intelligence services and was in charge of the security of Soviet embassies. Directorate S ran Soviet illegals worldwide, including Molody.

KGB FIRST CHIEF DIRECTORATE EMBLEM

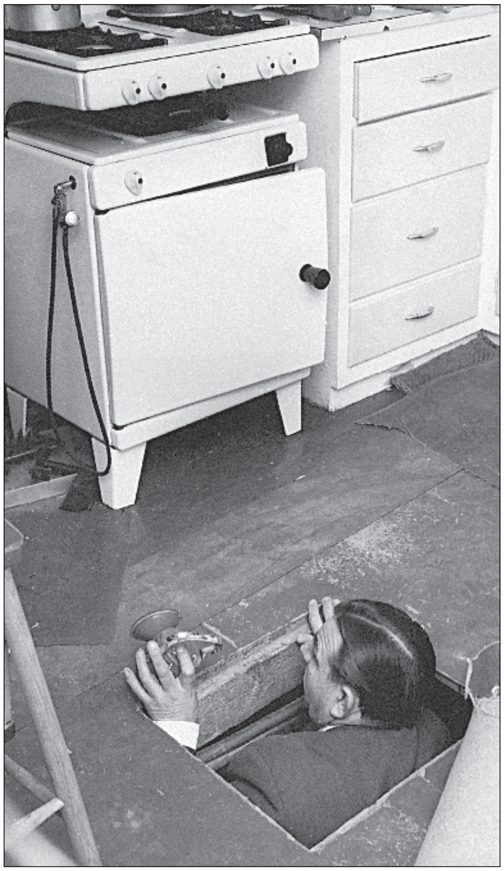




Talcum powder can concealment
The British security services MI5 and Special Branch discovered this concealment after searching the Krogers' bungalow. Inside the can of talcum powder were hidden radio communication schedules recorded on microfilm.

ETHEL ELIZABETH "BUNTY" GEE

HARRY FREDERICK HOUGHTON



Searching the Krogers' cellar
This trapdoor led to a small cellar beneath the kitchen at 45 Cranley Drive. A search carried out by MI5 personnel revealed the KGB agents' radio and burst transmitter attachment used by the Krogers to send urgent messages to Moscow.

Spy gadgets

The Krogers' bungalow contained the espionage equipment needed to support Lonsdale's spy network. In a space under the kitchen floor, entered by a hole just large enough to crawl through, an agent's radio and burst transmitter were kept. Microfilm was hidden in a can of talcum powder, while one-time pads and signal plans were concealed inside a flashlight battery (see p. 166 for a similar form of concealment) and a cigarette lighter. A box of face powder held a tiny microdot reader. The Krogers also had false passports, thousands of dollars, and equipment to make microdots.

Betrayal of the ring

The Lonsdale spy network was finally broken when the British security service MI5 (see p. 208) received information from a Polish defector. MI5 placed the so-called Portland spies under watch, and this led them to Lonsdale and subsequently to Helen and Peter Kroger.

The Portland spies were Harry Houghton (b.1906), a clerk at a weapons research establishment in Portland, England, and his lover, Ethel Gee (b.1914), a clerk who also had access to secret information. For money, these two passed Lonsdale details of a new submarine-detection system, naval maneuvers, and NATO plans. On January 7, 1961, Lonsdale was arrested receiving a package from Gee and Houghton, who were arrested soon after.

At his trial, Molody refused to reveal his identity. His legend as Lonsdale, prepared by the First Directorate of the KGB, was flawless except for one detail. The real Lonsdale had been circumcised at birth, whereas Molody had not. Molody and the Krogers were jailed, but Molody was freed in a spy swap in 1964. Houghton and Gee were given 15-year sentences. They were married after their release and faded into obscurity, but are known to have died. Molody probably controlled other spies, but their number and identities are not known.

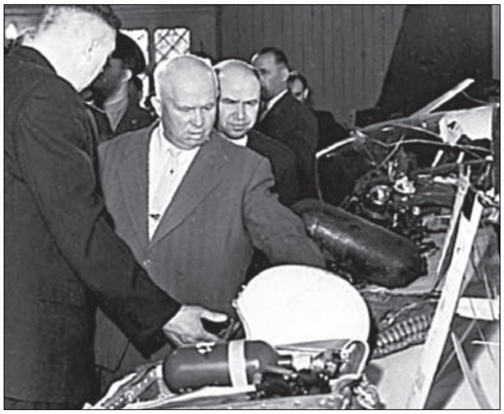
KONON MOLODY

SPY PROFILE

Russian-born Konon Molody (1922–70) lived in the US from 1932 to 1938, where he learned English. In 1938 he went to the Soviet Union and joined the NKVD (see p. 25). Molody went to Canada in 1954, where he adopted the identity of Gordon Lonsdale, a dead Canadian. He moved to London in 1955 and became a highly successful businessman, a cover for his espionage activities. He is believed to have controlled many agents, but only four were arrested.

U-2 spy aircraft

CONVENTIONAL INTELLIGENCE-GATHERING by the Americans in the early 1950s had failed to provide effective monitoring of the Soviet Union's growing nuclear capability. The Soviets tested their first nuclear bomb in 1949, and Moscow was building jet bombers that were believed to be capable of attacking the United States. Aerial photographs providing clear information about the new Soviet military threat were urgently needed, and in late 1954 the CIA commissioned the design and construction of an advanced spy aircraft that could be used to obtain them.



Krushchev inspects U-2 wreckage
Soviet Premier Krushchev (in light suit) examines equipment salvaged from the wreckage of Powers' aircraft after it crashed in Soviet territory.

The new spy aircraft, the U-2, was designed to photograph Soviet military installations from a very high altitude. Operating at over 80,000 ft (24,000 m), the U-2 was immune from attack by all the Soviet interceptors and antiaircraft missiles of the early 1960s. The U-2 Hycon Model 73C camera that was carried in U-2s was capable of recording details as small as 12 in (30 cm) across, and the 73B Pan Camera, also carried by U-2s, could take more than 4,000 pictures in the course of a single mission. The aircraft looked much like a motorized glider. It had a wingspan of 79 ft (23.5 m), and was powered by a single engine. Operating at high altitudes where there was little oxygen, the U-2 risked engine failure through lack of oxygen, known as a "flame-out." To relight the engine, the pilot would have to glide down to an altitude where there was more oxygen.

Operation Overflight

The first U-2 unit to be formed was the 1st Weather Reconnaissance Squadron (Provisional). By 1960, ten U-2s were operational, all under the cover of an organization called the National Advisory Committee for Aeronautics, which was supposedly engaged in meteorological research. The U-2 missions were codenamed Operation Overflight and flew from bases in the United Kingdom, Turkey, and Japan. Although the Soviet Union knew of the violations of its airspace, it was unwilling to admit publicly that its fighter aircraft and antiaircraft missiles were incapable of stopping them. Once the U-2 reconnaisance had established that the Soviet bomber threat was imaginary, attention was switched

Francis Gary Powers
CIA pilot Francis Gary Powers (1929–77) is shown here in captivity, shortly after his U-2 spy aircraft was shot down over Soviet territory.

A crashed U-2
Russian citizens examine the wreckage of Francis Gary Powers' U-2 after its crash near Sverdlovsk, 700 miles (1,120 km) east of Moscow in the Ural Mountains.

U-2 spy aircraft
Powered by a single jet engine, the U-2 had a wingspan of 79 ft (23.5 m), optimizing its performance at extreme altitudes.

U-2 in Moscow
The wreck of Powers' U-2 was put on public display to embarrass the Americans. Here, residents of Moscow inspect the wreckage.

to the Soviet Union's nuclear missile program. Information on this program was needed by US President Dwight D. Eisenhower before attending the Paris Summit with Soviet Premier Nikita Krushchev. Eisenhower consulted the CIA director, Allen Dulles, who assured him there was no chance of a U-2 pilot being captured alive. On May 1, 1960, confident that neither the U-2 nor the pilot would fall into Soviet hands, Eisenhower authorized a flight over the Soviet intercontinental ballistic missile test center at Tyuratam.

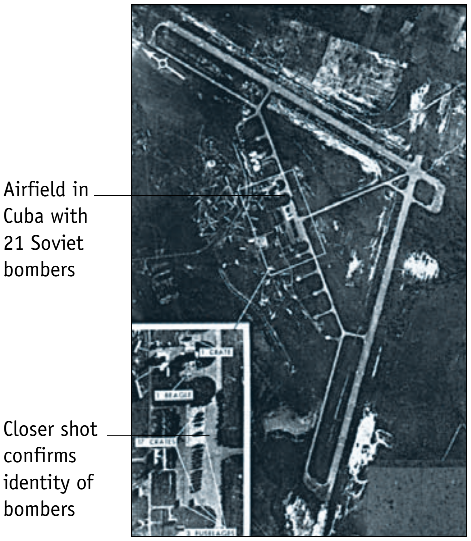
Powers crashes

The mission was flown by CIA pilot Francis Gary Powers. Powers took off from Peshawar in northern Pakistan, intending to fly over the missile test sites, as well as over other military and industrial areas, and land in Norway. Near the Soviet city of Sverdlovsk, his U-2 suffered an engine flame-out that forced him to descend to an altitude low enough for him to relight his engine. This brought the aircraft within range of a newly developed type of Soviet antiaircraft missile, the SA-2.

One of the missiles fired went off close to the aircraft, causing the fragile wing of the U-2 to buckle and sending the aircraft into a spin. Powers was thrown from the aircraft before he could set it to self-destruct. He parachuted to safety and the U-2 crashed. However, the aircraft's systems remained intact and were available for the Soviets to inspect. Believing that the U-2 and its pilot had been destroyed, the US government announced that an aircraft on a weather reconnaissance mission had been lost after it had strayed into Soviet airspace. Krushchev then revealed that Powers was in Soviet hands and had admitted aerial espionage, catching the Americans in a very embarrassing lie. The Paris Summit ended in disarray, to the Soviet Union's political advantage. Powers was found guilty of espionage at a Moscow trial; he was later exchanged for a KGB spy in American hands (see p. 208).

U-2S AND THE CUBAN MISSILE CRISIS

During the early 1960s, the CIA focused on gathering intelligence from Cuba because it had a communist government that was on friendly terms with the Soviet Union. On October 14, 1962, a U-2 spy aircraft photographed evidence of the installation of Soviet missiles near Havana, the Cuban capital. The missiles appeared to be medium-range nuclear SS-4s, easily capable of reaching the United States. On October 22, President John F. Kennedy announced a maritime quarantine of Cuba, to prevent further stockpiling of missiles. Tension between the United States and the Soviet Union escalated, reaching a peak on October 27, when a U-2 flying over Cuba was shot down. There was the real prospect of war. However, on October 28, the Soviet Union announced that it would withdraw the missiles. U-2 missions later verified this withdrawal.


Airfield in Cuba with 21 Soviet bombers
Closer shot confirms identity of bombers

Soviet bombers in Cuba
U-2 pictures proved that not only missiles, but Soviet Il-28 nuclear bombers were present in Cuba, well within range of the United States.

Walker spy ring

THE KGB'S MOST IMPORTANT SPY in the United States in the 1970s was John Anthony Walker, Jr. He was a chief warrant officer in the US Navy who had access to naval secrets, and decided to become a spy because he needed money after a series of business failures. Walker made his first contact with the KGB in early 1968 by asking to see "someone from security" at the Soviet embassy in Washington, DC. He had calculated correctly—the Soviets were willing to reward him, as they did in similar cases, with cash payments.

Walker's Minox camera
In the course of his long career as a spy, Walker photographed so many secret documents that his Minox C camera wore out.

John Walker
As part of his cover, Walker (b.1937) espoused a variety of anticommunist political causes and joined fringe groups such as the Ku Klux Klan (KKK).

Walker took with him a month's key settings for the KL-47 cipher machine used at the US Navy's command center for Atlantic submarine forces, where he worked. Announcing that he had easy access to such settings, Walker demanded $1,000 per week. He was given some cash in advance and, at a later meeting, received $5,000 in return for a series of cipher key settings' cards. Walker was also given a Minox camera (see p. 94) to copy secret documents and cipher material.

Dealings with the KGB

During the next 17 years, Walker gave the KGB more cipher key cards as well as various technical manuals. These items enabled the Soviets to obtain important naval secrets, including the movements of the American nuclear submarine fleet. Besides this, the Soviets gained advance knowledge of American bombing raids on North Vietnam in the early 1970s.

The KGB gave Walker a rotor reader with which to analyze the inner wiring of US Navy cipher machine rotors. They also trained him in espionage tradecraft at a series of secret meetings in Austria. In the US, Walker seldom met his KGB handler personally, but used a series of dead drops (see p. 170) to pass over information and receive payment.

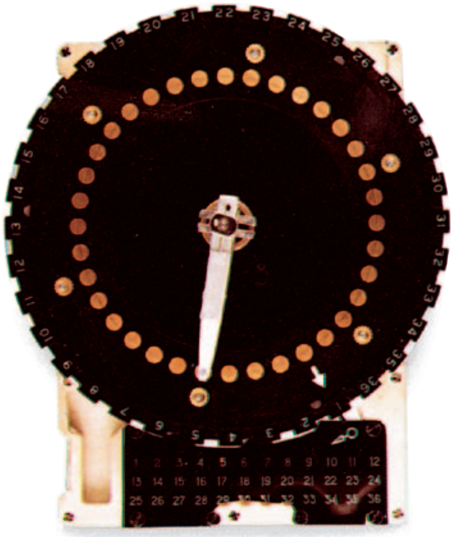
Family and friends

When Walker saw his access to secret material ending because of his imminent retirement from the navy, he drew his family into the spy ring. He recruited his brother Arthur and his son Michael, who was serving in the navy. John Walker also recruited his friend Jerry Whitworth, a navy communications specialist.

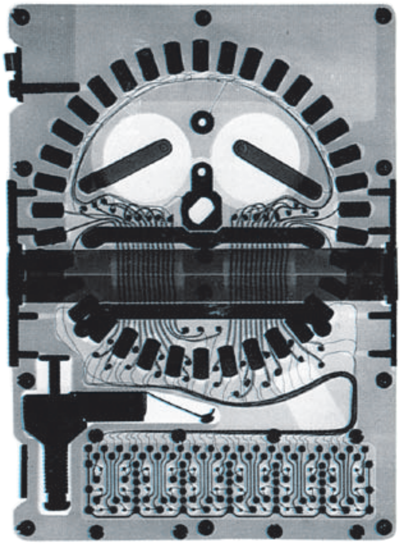
ROTOR READER

Walker was given this device by the KGB to trace the internal wiring of the rotors used in the US Navy's KL-47 cipher machine. Walker removed the rotors from the KL-47 and placed them over the disk of the rotor reader. Contacts inside the disk sent signals through the rotor reader's internal circuitry to light up numbers on a display board. Walker was taught how to interpret these numbers so as to work out the internal wiring of the cipher rotors.

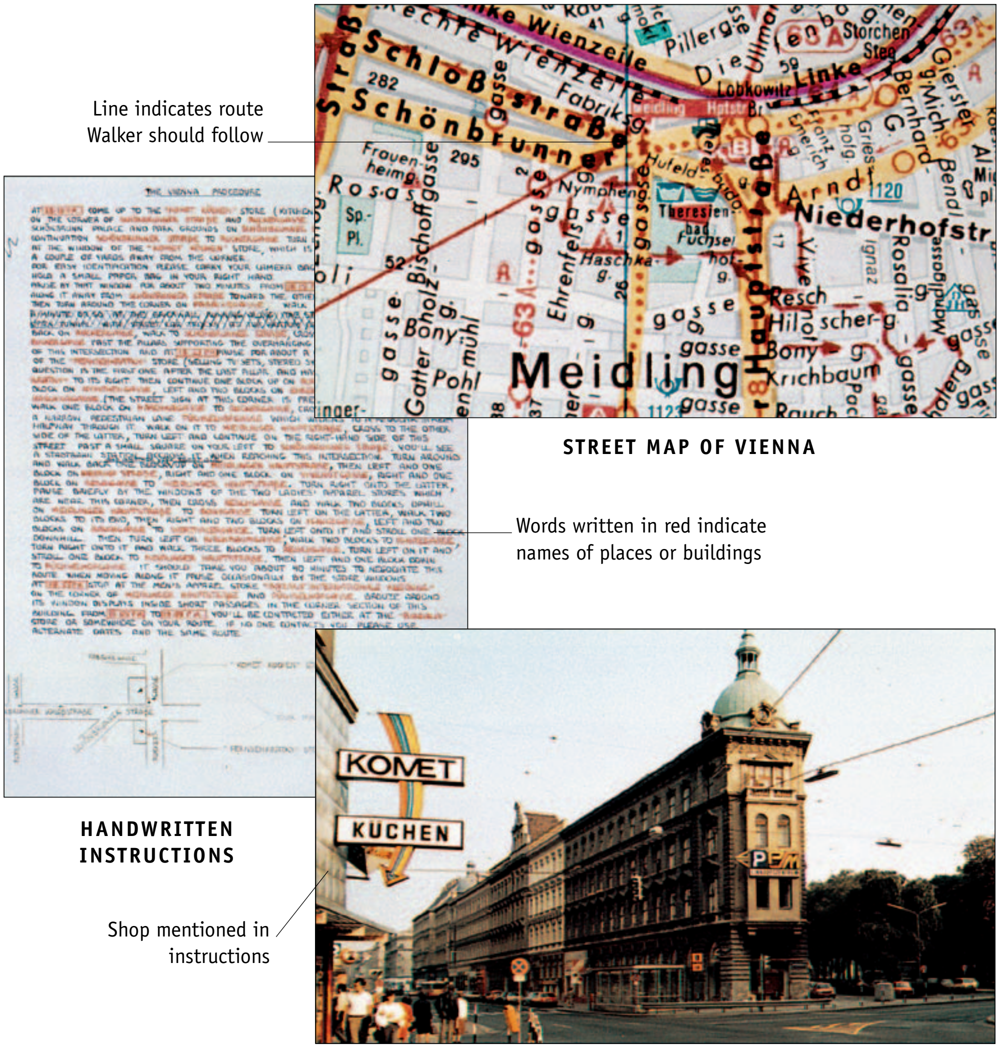
The KGB already had lists of the key settings of the KL-47, as these had been stolen by Walker. Knowledge of both the key settings and the internal rotor wiring enabled the KGB to decipher some of the US Navy's radio messages.



KL-47 ROTOR MOUNTED ON READER



X-RAY OF READER SHOWING WIRING



Line indicates route Walker should follow
Words written in red indicate names of places or buildings
Shop mentioned in instructions
KOMET
KUCHEN

STREET MAP OF VIENNA

HANDWRITTEN INSTRUCTIONS

BUILDING MENTIONED IN INSTRUCTIONS

THE VIENNA PROCEDURE

Once Walker was established as an agent, the KGB avoided direct meetings with him in the United States for security reasons. Instead he was instructed to travel abroad, usually to Vienna (or sometimes to Hong Kong), for training, instructions, and payment from his KGB case officer.

Vienna was often used for such purposes by the KGB, because of both its status as an international city and the neutrality of its counterintelligence service. To direct him to his meetings, Walker was given maps and written instructions. Complex routes were used in order to give the KGB time and opportunity to detect whether Walker was under surveillance.

Along his route he was watched by KGB agents with body-worn surveillance radios (see p. 140). All likely frequencies were monitored for signs of any unusual activity by Austrian counterintelligence or the CIA, which operated from the American embassy. If any of the KGB agents involved noticed anything suspicious, the meeting would be aborted. Walker was given backup instructions for an alternative meeting in case this happened.

The instructions and map shown here were used on a trip Walker made to Vienna in 1978. It is known that during the course of a 40-minute meeting with his handler he received money and instructions, and handed over cryptographic secrets stolen by his accomplice Jerry Whitworth.

Walker's wife knew for many years that he was a spy, but she kept silent. After the couple divorced, she eventually did inform the FBI. One evening in 1985, FBI personnel followed John Walker to a dead drop site outside Washington, where Walker left a package of secret material obtained from his son.

The FBI intercepted this material, missed a chance to pick up the KGB handler, and arrested Walker later that evening at a nearby hotel.

John Walker was sentenced to life imprisonment; his accomplices also received long terms. What the ring's activities had cost the US in terms of security remains beyond calculation.

MICHAEL WALKER: CODENAME S—ON ACTIVE SERVICE IN THE US NAVY

ARTHUR WALKER: CODENAME K—ELDER BROTHER OF JOHN WALKER

JERRY WHITWORTH: CODENAME D—NAVY COMMUNICATIONS EXPERT

East German foreign intelligence

HVA CREST

EAST GERMANY'S FOREIGN intelligence service was called the Hauptverwaltung Aufklärung, or HVA. It was created in 1952 by the Ministerium fur Staatssicherheit (MfS), East Germany's State Security Ministry, popularly known as the Stasi (see p. 99). Throughout the Cold War, the HVA served East Germany for the primary purpose of preventing surprises, especially military surprises, against the state or its Eastern bloc allies. In this respect, the HVA was a highly effective organization, and its director for over 30 years, Markus Wolf, was one of the most successful spymasters of the Cold War.

The newly formed HVA recognized that its fledgling service lagged behind the experienced West German intelligence service, led by former Nazi General Reinhard Gehlen. To compensate, the HVA developed innovative techniques to target people who had access to the secrets that it wanted to know.

Through experience, the HVA learned that a lowly US Army sergeant in Nato or a technical employee in the Ministry at the West German capital Bonn could provide a larger quantity of higher-quality secret information than a senior government official or senior military officer. Such "lowly" agents were also easier to control and less demanding.

Recruiting and positioning agents

In HVA colleges, recruiters were taught how agents could be found by focusing on and exploiting human needs and weaknesses. Many of these were of a sexual nature; for example, someone could be blackmailed into becoming an agent after being secretly photographed with a prostitute.

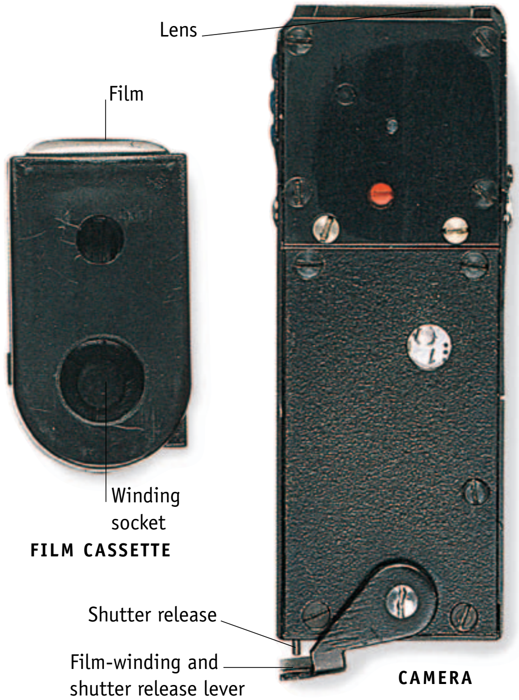
However, the HVA found that the best way to recruit was to offer money. In some cases, the money was needed to pay debts or maintain a gambling addiction, but in most cases the lust for money was the main motivation for most of the people recruited by the HVA.

Among the HVA's principal successes was the positioning of agents inside the government in West Germany. In addition, the HVA carried out spying operations against the United States and other Nato countries, and foreign military forces stationed in Germany.

MARKUS WOLF

SPY PROFILE

From 1952 to 1986, Markus Wolf (1923–2006) was the director of the HVA and became the longest-serving head of a major intelligence service during the Cold War. Wolf was identified by the CIA soon after he took over the HVA, but was "the man without a face" to other intelligence services. His skillful recruitment and handling of agents made him communism's most successful spymaster. In 1986, Markus Wolf resigned after becoming disillusioned with the direction of the MfS.



Venus document camera

In 1986, the final subminiature document camera was produced for the HVA, using the Minox film format and a uniquely designed 150-shot cassette. The tiny camera could be operated with one finger.

In 1974, Gunter Guillaume (1927–95), the personal assistant to West German Chancellor Willy Brandt, was unmasked as an HVA agent. Guillaume had access to top secret government documents, and revelation of his spying led to the collapse of the West German government when Brandt resigned.

The Romeo method

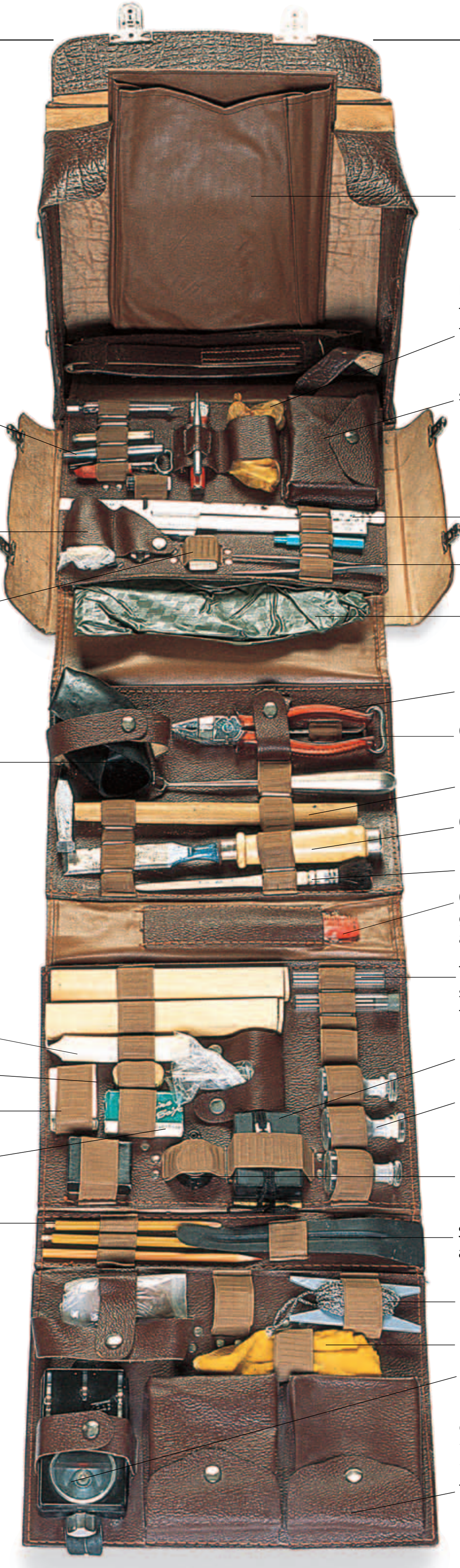
The HVA initiated a policy of instructing its male agents sent to the West on spying assignments to look for future wives and lovers from among government secretaries and others with access to secrets. This simple plan, later known as the "Romeo method," worked with great effectiveness, much to the detriment of Nato and the West German government in Bonn.

Technical support

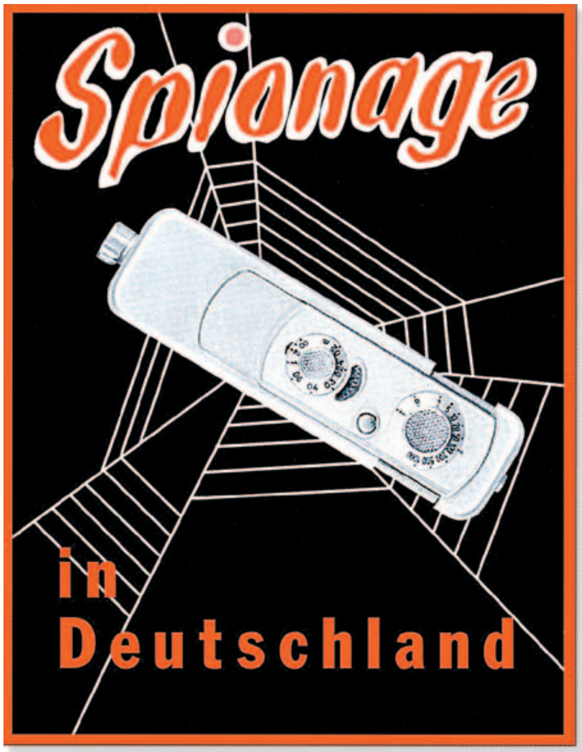
The HVA had its own technical group that worked with the OTS, the technical service for all of the MfS, to support its agents and clandestine operations with specialized technology. For example, technicians developed a unique method of secret communication in which HVA agents in West Berlin could call a local telephone number and have their messages automatically transmitted across the Berlin Wall by means of an embedded infrared voice-link that was impossible to intercept.

Specialized cameras were developed for the HVA. Silent subminiature cameras could photograph 150 documents on a single film cassette. Uranus microdot cameras (see pp. 162, 163) were part of a communication system that allowed agents to send and receive documents photographically reduced to less than 1 x 1 mm in size.

The skill of the technical specialists working within the HVA enabled many of its agents to remain undetected long after the collapse of East Germany and the end of the Cold War.


Pocket for evidence forms and carbon paper
Rubber gloves to avoid leaving fingerprints
Precision tools for scoring lines and marking evidence
Pocket containing slides for samples
Sponge for collecting liquids as evidence
Steel ruler
Tweezers
Eraser
Waterproof holder for documents
Pliers
Gimlets
Cup for mixing plaster
Hammer
Chisel
Brush
Comb for gathering hair and fibre samples
Candle that can be melted to make wax impressions
Test tubes for storing hair and fibre samples
Compass
Tape measure
Glass bottles for storing samples
Matches
Soap
Magnifying glass
Pencils
Spatula for applying plaster
Cord
Cloth
Flashlight
Pocket containing plaster for making impressions

Criminalist kit
In East Germany, the crime of espionage was investigated by graduate "criminalists." The tools of their trade were packaged in this small leather case, which contained everything necessary to catch spies.



Cold War poster
This poster warned of the presence of spies in West Germany. The modified Minox camera in the center of the poster was unique to the MfS.

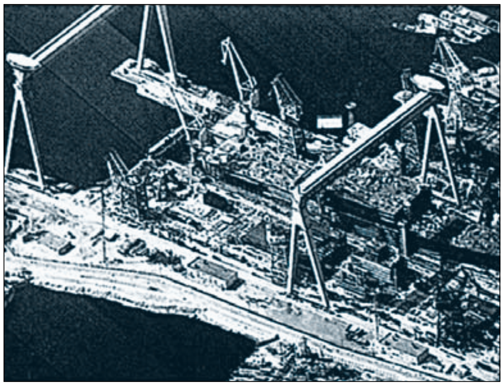
Spying from space

THE LAUNCH OF THE FIRST man-made satellite, by the Soviet Union in 1957, opened up new opportunities for intelligence-gathering. A camera on a satellite could carry out surveillance of any part of enemy territory that lay beneath its orbit. The first spy satellite was launched by the Americans in 1961. For 15 years, pictures from a satellite took longer to reach the analyst than those from a spy plane, although, of course, they could cover a far greater area. All this changed in the 1970s, when digital technology made pictures immediately available.

The early satellites had to jettison their film in a container to be retrieved and flown to a processing point, often over long distances. This process was known as "bucket dropping" and was so slow that the Arab–Israeli Six-Day War of 1967 was over before the first satellite photographs of it reached Washington. Satellites were for strategic (long-term) surveillance, while tactical (day-to-day) observation was done by spy planes.

The KH-11

The Americans initiated a top secret program to produce better satellites. The result, the KH-11 satellite, became operational in 1976. It was different from earlier models in that it carried no film. Instead, it beamed its images in digital form to ground stations as soon as they were taken. In addition to making pictures rapidly available for analysis, this system has other advantages. The digital images are capable of extremely high definition. From its orbit 200 miles (322 km) above the Earth, the KH-11 could resolve detail as small as 6 in (15 cm) across. The images can then be enhanced further by computer manipulation. At America's National Photographic Interpretation Center, a library of visual

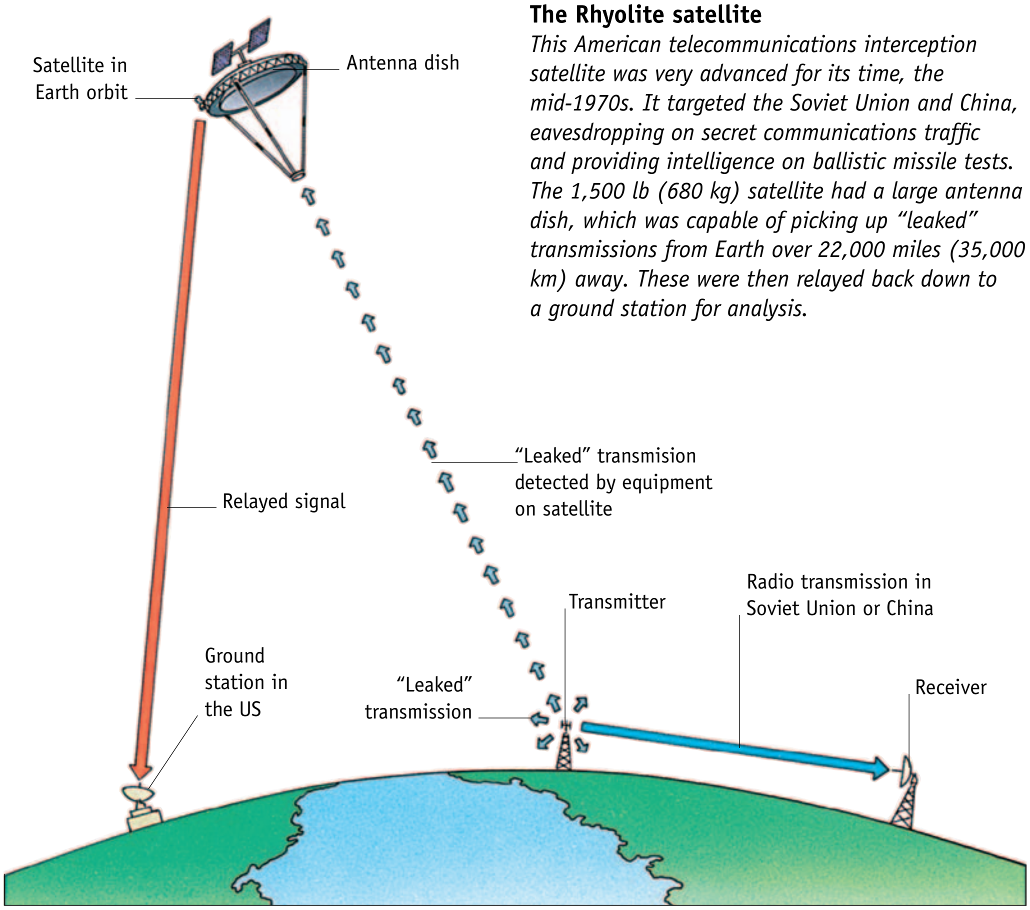


American satellite image

KH-11 satellite image of a Soviet aircraft carrier under construction. A US naval intelligence analyst was jailed for releasing this image.

THE US NATIONAL RECONNAISSANCE OFFICE (NRO)

This office was officially declassified as a secret organization in 1992. President Eisenhower established the NRO in 1961 in recognition of the new intelligence dimension promised by satellites. The NRO manages the US Photographic and Electronic Listening Satellites Program and the US Airborne Reconnaissance Program. Its powerful computers analyze data and were used to identify Iraqi weapons systems in the 2003 invasion of Iraq.



The Rhyolite satellite

This American telecommunications interception satellite was very advanced for its time, the mid-1970s. It targeted the Soviet Union and China, eavesdropping on secret communications traffic and providing intelligence on ballistic missile tests. The 1,500 lb (680 kg) satellite had a large antenna dish, which was capable of picking up "leaked" transmissions from Earth over 22,000 miles (35,000 km) away. These were then relayed back down to a ground station for analysis.

Soviet satellite image
The CIA obtained this Soviet satellite image of Washington, DC, and its own headquarters; the image was later displayed in an agency internal poster.

interpretation keys is maintained. An intelligence analyst can check a satellite image against the visual keys in order to recognize a major weapons system.

A satellite codenamed Lacrosse was launched in 1988, using radar to "see" through clouds. It was joined in 1989 by an infrared version. Both satellites have "night vision." With these capabilities, satellites continue to be the chief means of monitoring Strategic Arms Limitation Treaties between the United States and the Soviet Union (and now Russia).

Satellite spies

Inevitably, satellite technology became the target of espionage, and its secrets have to be closely guarded. American agencies do not release their satellite images for public use until the pictures have been modified to reveal as little as possible of the technology involved.

A major spy scandal did, however, occur in the United States in 1977, which showed that security in some satellite companies was not tight enough. The scandal concerned a pair of self-taught and somewhat amateurish, though mercenary, spies: Christopher Boyce and his childhood friend Andrew Lee.

Through the influence of his ex-FBI father, Boyce had obtained a job with TRW, the company that produced and operated the Rhyolite satellite for the CIA. The Rhyolite was a spy satellite that monitored Soviet and Chinese secret telecommunications.

Boyce's job was in a top-secret office, known as the Black Vault, where he helped to coordinate communications between TRW, the national intelligence agencies, and the satellite monitoring stations. Security in the Black Vault was so lax that Boyce found he had easy access to classified material.

Lee's role was to make contact with the KGB. He would travel to Mexico City, and sometimes as far as Vienna, to sell the information to the Soviets. The material he sold concerned, among other things, the Rhyolite program, the KH-11 satellite, and various ciphers.

The pair were brought to trial after Lee was arrested by the Mexican police for suspicious activity outside the Soviet embassy. He was carrying a pocketful of satellite secrets on strips of Minox film.

CHRISTOPHER BOYCE

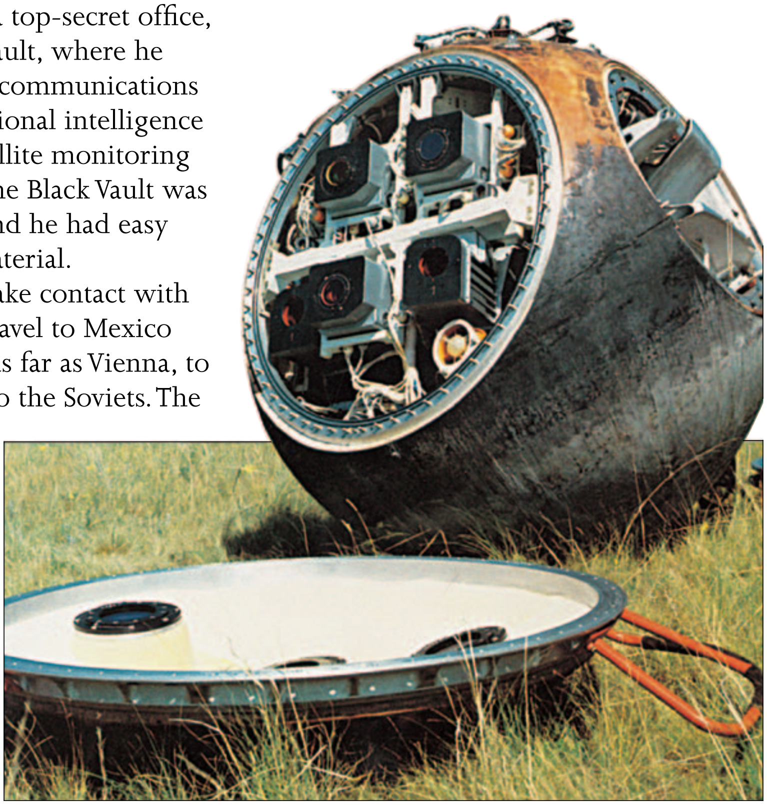
SPY PROFILE

Christopher Boyce (b.1953) took a job with the American satellite company TRW and used it to obtain information about America's satellites. The information he and Lee sold to the KGB alerted the Soviet Union to the vulnerability of its military communications to eavesdropping by American satellites. Arrested in 1977, Boyce was sentenced to 40 years, escaped, and received 20 more years on recapture. He was paroled in 2003.

ANDREW DAULTON LEE

SPY PROFILE

Andrew Daulton Lee (b.1952) is a documented example of a spy whose motive was to find money to pay for his drug habit. In 1975 he began to sell satellite secrets, provided by his friend Christopher Boyce, to the KGB. Lee traveled to Vienna and Mexico City to carry out these transactions. After his arrest in Mexico, he was handed over to the FBI. Lee was tried and sentenced to life imprisonment in the United States. He was paroled in 1998.



Camera pod from a spy satellite
A Soviet camera pod lies on the ground in Kazakhstan, after its film has been extracted for processing. Soviet satellites relied on cameras that used conventional film long after the Americans introduced digital transmission.

Moscow: spy city

ONE CITY TO RIVAL BERLIN (see p. 44) as a hotbed of espionage in the Cold War—and one that remains a "city of spies"—was the Russian capital. The Soviets tried to bug foreign embassies as a matter of course, sometimes going to the most extraordinary lengths to do so. In its own efforts to spy on the Soviets, the United States struggled against tight Soviet security in Moscow in the early years of the Cold War. But by the 1970s a new generation of CIA agents with improved tradecraft based on advanced technology had come to the fore, as shown by the success of the spy codenamed Trigon and his young case officer.

Walls have ears

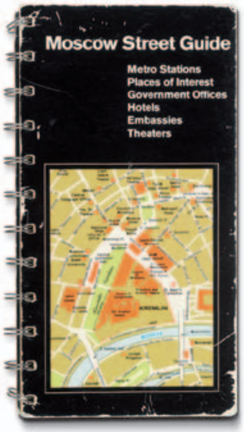
The US embassy in Moscow has long been a top eavesdropping target for the Soviet security services. They had their first success in 1941, when embassies were evacuated ahead of the advancing Germans. The NKVD (see p. 217) seized this chance to hide bugs in empty foreign embassies. Then, at the end of World War II, a group of Soviet Young Pioneers presented the US ambassador with a carving containing a bug that went undetected until 1952 (see p. 112).

Also in 1952, the US embassy moved into a new building—one specially built by the Russians. Over the years it was found to be riddled with bugs. Wires from the bugs led down to the basement, where they vanished into the floor … In the late 1970s and early 1980s, an extra eight-story office block was built on the grounds of the US embassy. The Americans had to use Russian contractors, who insisted on making the concrete supports offsite. These supports were subsequently found to be full of bugs (right). The office block was so heavily compromised that the Americans never even used it until after the Cold War, by which time US contractors had demolished the top two floors and added four new secure ones. At the end of the Cold War, the Russians gave startled embassy officials plans that purportedly showed all the bugs originally built into the block. Wires from both these and the bugs in the main embassy building ran down through the basement and on to an underground KGB listening post.

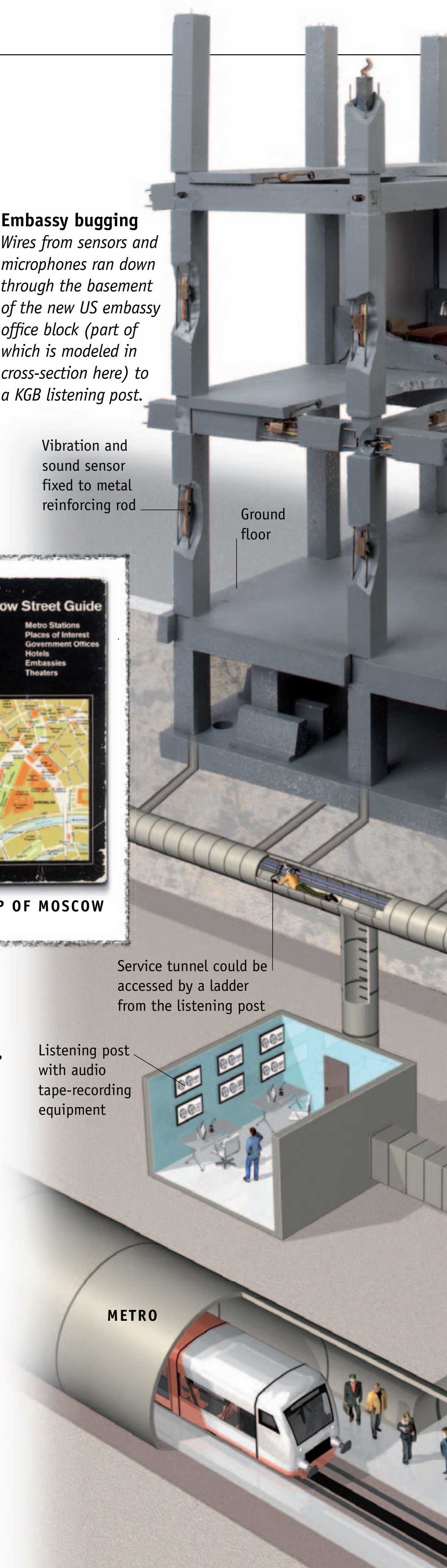
The US embassy in Moscow
In 1963 alone, 40 hidden microphones were found in the walls of the building that has been the US embassy in the Russian capital since 1952.

MAPPING MOSCOW

Soviet-produced Moscow street maps were deliberately inaccurate, to hinder foreign intelligence services. So, early in the Cold War the CIA began making its own maps and produced its first Moscow street map in 1953. In 1974 it brought out a useful pocketbook version. The CIA maps were invaluable for operations on the streets, and the whole process of mapping the city helped the CIA to identify previously unknown Soviet installations and facilities.

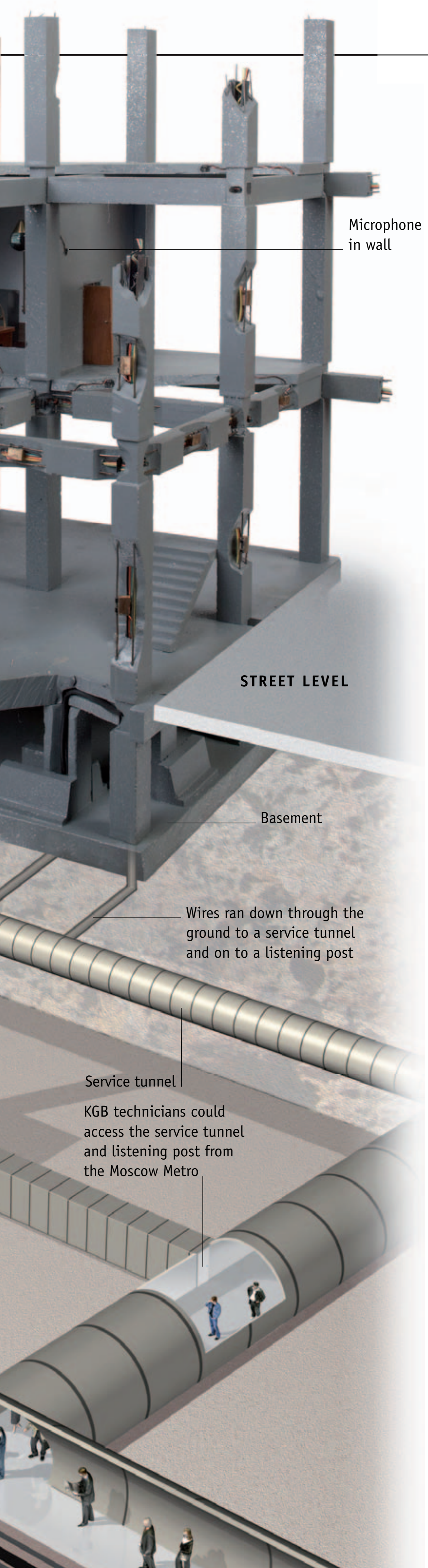


CIA MAP OF MOSCOW



Embassy bugging
Wires from sensors and microphones ran down through the basement of the new US embassy office block (part of which is modeled in cross-section here) to a KGB listening post.

Vibration and sound sensor fixed to metal reinforcing rod
Ground floor
Service tunnel could be accessed by a ladder from the listening post
Listening post with audio tape-recording equipment
METRO


Microphone in wall
STREET LEVEL
Basement
Wires ran down through the ground to a service tunnel and on to a listening post
Service tunnel
KGB technicians could access the service tunnel and listening post from the Moscow Metro

Trigon and Peterson

Aleksandr Ogorodnik (b.1939) was a married Soviet diplomat in Colombia in South America. In 1973 he agreed to spy for the US when the CIA told him they knew his mistress was pregnant. The CIA gave him the codename Trigon and trained him to copy documents with a revolutionary new camera concealed in a fountain pen: the tiny T-100 (see p. 96).

In 1975 Ogorodnik took up a key post in the Soviet Foreign Ministry's American Department in Moscow. The same year, Martha Peterson (b.1945) arrived in the city to be his CIA case officer, in the guise of a US embassy official. The two never met, their only contact being through dead drops. For months all went well. With his T-100, Ogorodnik copied reports sent in from Soviet embassies all over the world. Peterson, meanwhile, attracted little attention from the KGB, who never dreamed that a woman—and a young woman, at that—could ever be involved in espionage. Then a Czech intelligence officer who had infiltrated the CIA betrayed Ogorodnik to the KGB.

On July 15, 1977, Peterson had just made a drop for Ogorodnik when she was detained by the KGB. Ogorodnik never came to collect the drop, for he had already committed suicide.

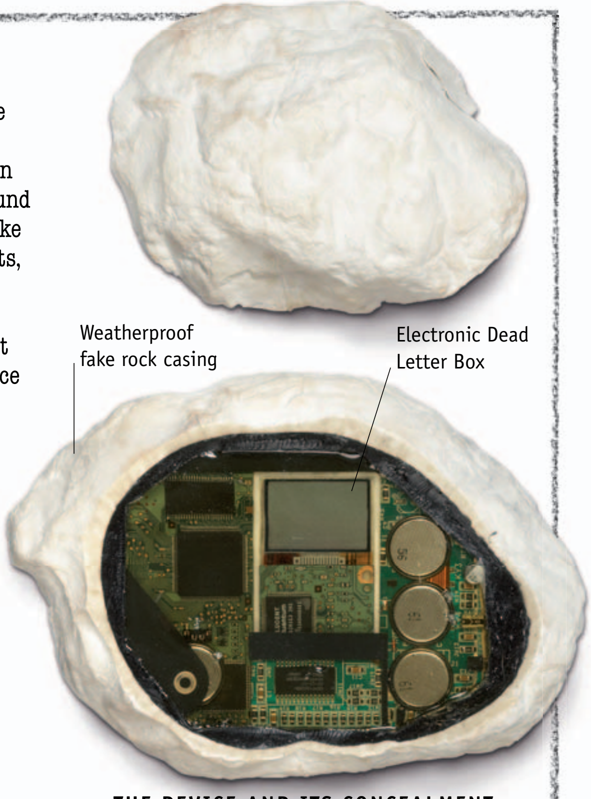
A drop in the dark
The KGB detained Martha Peterson after she make a dead drop one night after work in a tower of the Krasnoluzhskiy Rail Bridge, which spans the Moscow River (left). After she was interrogated she was released, but her diplomatic status was revoked and she had to leave the Soviet Union.

Suicide surprises KGB
When Ogorodnik took up his new post in Moscow in 1975, he insisted the CIA give him a suicide pill (an "L-pill", or lethal pill). The CIA hid the pill in a pen. While being interrogated by the KGB, he bit through the pen and into the pill.

SPYING IN MOSCOW CARRIES ON

The CIA was not the only Western intelligence agency active in Moscow in the Cold War, nor has spying stopped there. In 2006 the Russian Federal Security Service (FSB) said it had found an Electronic Dead Letter Box (EDLB) in a fake rock in the city. The FSB said Russian activists, and MI6 officers posing as British embassy staff, used modified handheld computers to communicate via the rock as they walked past it. Russian state television showed surveillance footage purporting to support the claim.

RUSSIAN SURVEILLANCE FOOTAGE



THE DEVICE AND ITS CONCEALMENT

POST-COLD WAR SPYING

FORMER CIA DIRECTOR James Woolsey once stated that with the end of the Cold War the great Soviet dragon was slain. He wryly noted, however, that in its place intelligence services were now facing a "bewildering variety of poisonous snakes that have been let loose in a dark jungle; it may have been easier to watch the dragon." These days, the superpowers face an array of threats from around the globe that sap their resources and dilute their effectiveness.

FAPSI crest
Russia's FAPSI—federal agency of governmental communication—is responsible for the security of all encrypted and government communications, as well as intelligence gathering in the sphere of special communications. The organization operates intercept stations around the world.

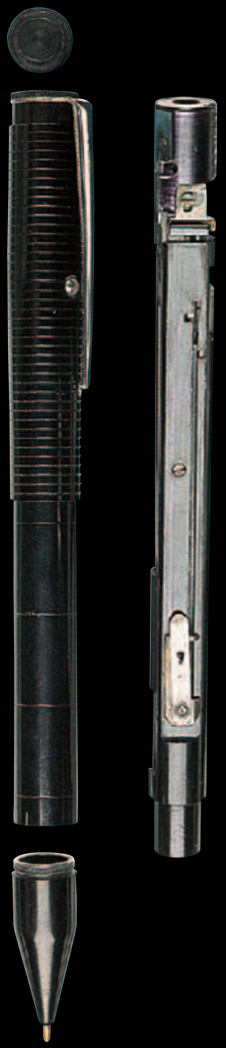
CHANGING FACE OF ESPIONAGE

Spying is more prevalent today than at the height of the Cold War. One reason for the increase is that espionage is now a greater necessity for many nations to survive. Blurring of traditional roles of friends and foes is another factor—there are friendly nations but no friendly intelligence services. At the same time, the superpowers' growing reliance on new technologies has made them more vulnerable in several ways. The infrastructure is more difficult to protect and the increasing use of satellites and electronic spies instead of human intelligence sources, also known as HUMINT, leaves gaps in intelligence gathering.

ESSENTIAL ESPIONAGE

The necessity for espionage grows as the gap between the superpowers and other countries increases; stealing economic and military information becomes the only way for many countries to compete. Conversely, the need to invest in counterintelligence becomes essential as nations strive to protect their own secrets and deny their use to others.

Robot S-C electronic 35 mm camera
The Robot S-C camera is specially designed for surveillance and security missions, as well as for document reproduction. Its tiny size makes it easy to camouflage for operational use.

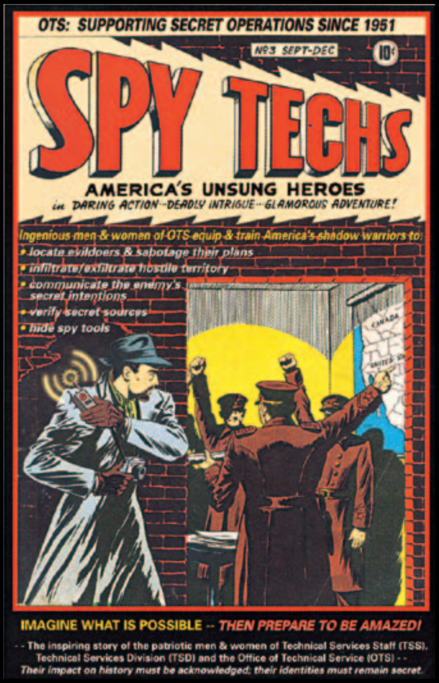


David pen
As well as functioning as a writing pen, this Czech device called "David" could secretly photograph a dozen documents. The pen's end cap unscrewed to reveal the lens.

GRU badge
Russia's military intelligence service is called GRU. Since the collapse of the Soviet Union in 1992, the importance of GRU's foreign intelligence gathering operations has increased.

FRIEND OR FOE

The major superpowers always collected intelligence and attacked the ciphers, or codes, of their friends as well as their enemies. The national interests of former friends and foes are now being redefined in terms of competing economic interests. Cultural and historic friendships between nations continue to fade as they are replaced by trading partnerships and other interdependent economic relationships. The importance of spies and counterspies is increasing as a nation's first line of defense.


OTS: SUPPORTING SECRET OPERATIONS SINCE 1951
Nº3 SEPT-DEC
10¢
SPY TECHS
AMERICA'S UNSUNG HEROES
in DARING ACTION--DEADLY INTRIGUE--GLAMOROUS ADVENTURE!
Ingenious men & women of OTS equip & train America's shadow warriors to:
• locate evildoers & sabotage their plans
• infiltrate/exfiltrate hostile territory
• communicate the enemy's secret intentions
• verify secret sources
• hide spy tools
CANADA
UNITED STATES
IMAGINE WHAT IS POSSIBLE -- THEN PREPARE TO BE AMAZED!
-- The inspiring story of the patriotic men & women of Technical Services Staff (TSS), Technical Services Division (TSD) and the Office of Technical Service (OTS) --
Their impact on history must be acknowledged; their identities must remain secret.

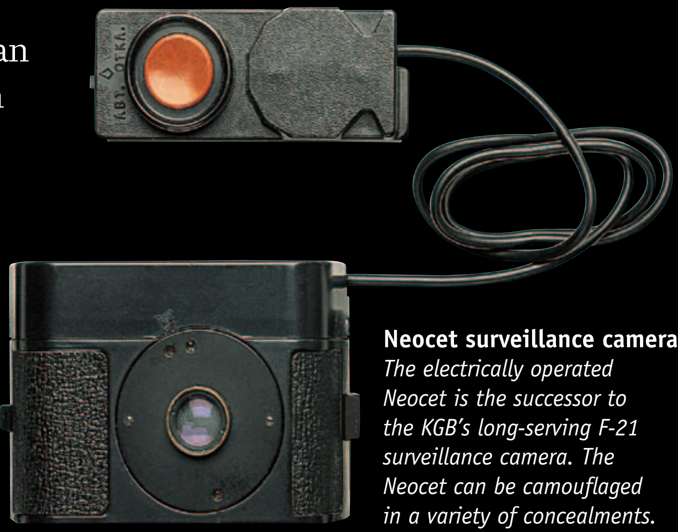
OTS 50th-anniversary poster
The CIA's Office of Technical Service (OTS) has been equipping and training America's spies for over half a century. The organization's motto is, "Imagine what is possible and then prepare to be amazed."

DIGITAL WORLD

The internet and computers have altered the ways in which spies collect and communicate information to their handlers. "Agent communication" is still an area of vulnerability to a spy, but less so with the advent of the internet. Spies now employ wireless burst communications, encrypted messages, and digital dead drops in ways that place security and counterintelligence forces on the defensive. The principle of asymmetrical warfare dictates that a weaker opponent attack a stronger opponent at their point of greatest vulnerability. Intelligence services identify and exploit the weaknesses of stronger countries, whose information infrastructure has become more vulnerable with every new technological advance. Superpowers expand networked systems at a faster rate than they protect them, leaving them vulnerable to exploitation and attack by "cyberspies."

HUMAN SOURCES MUST BE DEVELOPED

Satellites can show exactly what an enemy is doing, but they cannot show what they are thinking or planning. Western nations must reverse the trend toward reliance on technology to gather intelligence and refocus on recruiting human sources. An agent inside a terrorist cell is as important as an email intercept.



Neocet surveillance camera
The electrically operated Neocet is the successor to the KGB's long-serving F-21 surveillance camera. The Neocet can be camouflaged in a variety of concealments.

Russian foreign intelligence

AS THE SOVIET UNION COLLAPSED AND the KGB was broken up, the PGU, or First Chief Directorate, was reborn as the SVR (Foreign Intelligence Service) in December 1991. Its first director, Yevgeniy Primakov (b.1929), would report directly to the Russian president and oversee a vast global intelligence network. Although initially reduced in size, the SVR refocused its resources against its main opponent, the US, and continued to rebuild its strength under then Russian President Vladimir Putin. The end of the Cold War only served to intensify confrontations between intelligence services, therefore.

СЛУЖБА ВНЕШНЕЙ РАЗВЕДКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ОТЕЧЕСТВО
ДОБЛЕСТЬ
ЧЕСТЬ

SVR CREST

Birth of the SVR

Until the dissolution of the Soviet Union, the KGB had been its "sword and shield" and the PGU (First Chief Directorate), its "eyes and ears." Operating from a secret headquarters on the outskirts of Moscow (Yasenevo), the PGU gathered intelligence globally on every country considered important by Soviet leaders.

In late 1991, the PGU became an independent agency reporting directly to the Russian president and was eventually renamed the SVR (Foreign Intelligence Service). Still based in Yasenevo, the new SVR was meant to be free of a historical legacy in which intelligence reports were invariably filtered and altered to reflect the current perceptions of the Soviet leadership. Primakov set quite a precedent when he briefed the new Russian president, Boris Yeltsin, for the first time using only the facts.

Despite Yeltsin's support, the SVR was hemorrhaging experienced intelligence officers to the emerging Russian private sector and lacked the financial resources even to house its employees adequately. During this time of chaos, the SVR shrank by an estimated 30 to 40 percent and was forced to consolidate its intelligence-gathering activities by eliminating coverage of many smaller countries. Even this step, however, did not produce surpluses of intelligence officers or money, since it was also forced to increase its coverage of the Baltic States and members of the Former Soviet Union (FSU) that were now turning toward Nato and the West.

Early SVR strategy

Using a strategy unchanged since the heated days of the Cold War, Primakov focused his available resources against the US. Relationships between the SVR and CIA reached a post-Cold War low in February, 1994, when CIA intelligence officer Aldrich Ames (see p. 202) was unmasked following a nine-year career as a mole in which he betrayed the CIA's human assets in Moscow and its most sensitive operational secrets.

SVR headquarters buildings
The headquarters of the SVR is located on Moscow's outer-ring road at Yasenevo. The architecture was influenced by the design of the original headquarters of the CIA in Langley, Virginia.

HIDDEN SVR RADIO RECEIVER

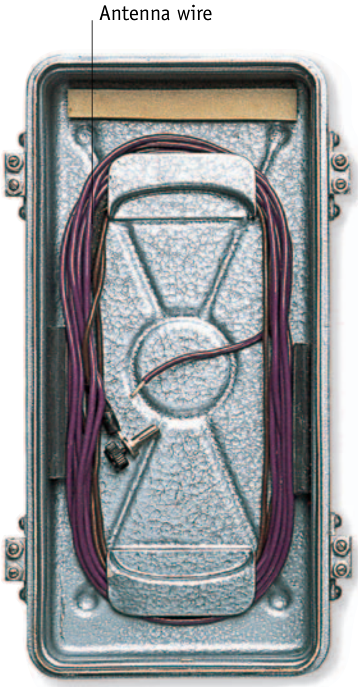
In 1999 an SVR radio receiver was recovered from a secret KGB cache outside the Swiss town of Befaux. KGB defector Vasili Mitrokhin (1922–2004) had revealed the presence of booby-trapped KGB caches of espionage equipment throughout Europe. Using his instructions, the Swiss federal police located the Swiss cache near a small chapel just outside Befaux buried 3 ft (1 m) deep beneath a large stone. An attempt was made, unsuccessfully, to deactivate the booby trap. Nevertheless, the cache was recovered. Apart from the radio receiver, it contained a burst (cipher) encoder. An unknown number of caches in deteriorating condition remain buried throughout Europe.

CHAPEL OUTSIDE BEFAUX, SWITZERLAND

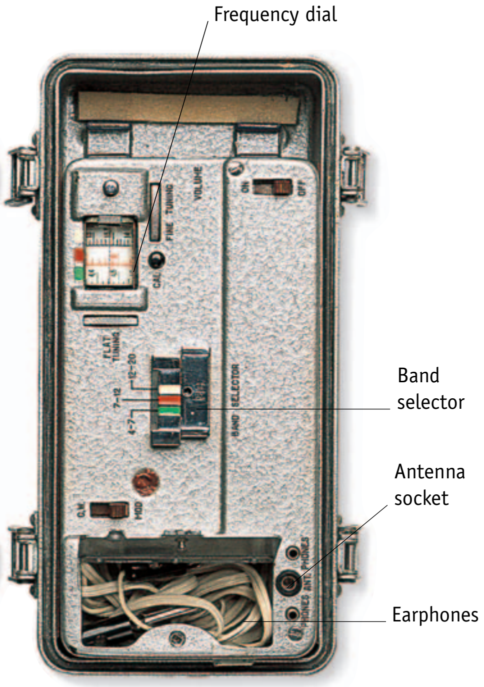
EARPHONE

KGB cache
The first landmark to the booby-trapped cache was a small chapel on the edge of the woods outside Befaux, Switzerland.

BOOBY-TRAPPED CACHE



LID OF RECEIVER



RADIO RECEIVER

In 1996, Primakov was promoted to Minister of Foreign Affairs and replaced by his First Deputy, Vyacheslav Trubnikov (b.1944). Trubnikov inherited a Russian intelligence service focused on three main areas: understanding US intentions as they operated against Russian interests in FSU states; the increasing threat of Islamic fundamentalism; and the troubles in Yugoslavia. Additional intelligence was needed for Russia's role in the global fight against international terrorism, and against international organized drug trafficking and other organized crime.

Growing strength of the SVR

In the late 1990s, the authorized strength of the SVR grew to 15,000 and was further bolstered with additional resources following the election of former intelligence officer Vladimir Putin as the new Russian president in late 2000. Accurate intelligence was seen as essential to President Putin if Russia was to regain its prominence in the international arena, and the SVR was still considered among the world's best intelligence services.

HUMINT (human intelligence) has always been a strength of the SVR and often compensates for its continuing lack of resources for technology and satellites; human spies are less expensive, and frequently more effective. The arrest in 2001 of FBI Special Agent Robert Hanssen (see p. 66) as a Russian/Soviet mole since 1979 removed any lingering doubt that the intelligence conflicts of the Cold War had abated. The SVR has been quick to identify and foster "anti-Americanist" feeling among member countries of the European Union as a strong motivation for recruitment, but it still relies on money as the primary lure for new recruits.

Major General Yuri Kobaladze
An accomplished intelligence officer, Kobaladze (b.1949) was head of the SVR's press office in the 1990s. He gave many public interviews and was known for his skill in managing the media.

Hanssen spy case

THE MOST IMPORTANT FBI EMPLOYEE to spy for Russia was Robert Hanssen (b. 1944). A onetime Chicago policeman, Hanssen joined the FBI in 1976, and soon took advantage of his top secret clearance status to sell sensitive classified information to Russia and the former Soviet Union for money and ego satisfaction. He was finally arrested by the FBI in 2001 after leaving a package containing highly classified information at a prearranged site, or dead drop, near his home in Vienna, Virginia.

FBI field office emblem
Hanssen worked for the Washington field office for several years; this FBI element later played a key role in his arrest.

In 1979, Hanssen walked into the offices of AMTORG, the trade organization in Manhattan that provided cover for Soviet military intelligence (GRU) and offered to sell US government secrets. To establish his credibility, Hanssen betrayed one of America's most important GRU moles, Major General Dmitri Polyakov (b.1921), whose codename was Tophat. (Polyakov was executed by the Russians in 1988 for his activities).

Robert Phillip Hanssen
Hanssen held key counterintelligence positions at the FBI and, as a result, had direct access to many highly classified documents.

Hanssen "gives up" spying

A year after Hanssen had started spying, his wife, Bonnie, came across nearly $20,000 in their house and confronted him. Hanssen maintained that he had sold only "worthless information" but vowed to stop. He severed contact with the GRU, confessed to his priest (Hanssen had converted to Catholicism), and told Bonnie the ill-gotten money had been given to charity. At this time, the FBI knew nothing of Hanssen's betrayal.

In 1981, Hanssen accepted a position with the Intelligence Division's budget unit at FBI Headquarters in Washington, DC. He was now privy to financial details about the supersecret programs run by not only the FBI, but also the CIA, National Security Agency, and Defense Intelligence Agency. Hanssen performed well but was not promoted as rapidly as his peers; his dissatisfaction grew. In September 1985, to advance his career, he accepted a promotion to field supervisor in the Intelligence Division of the FBI in New York City. Even with his larger salary, Hanssen felt under financial strain since he now had a family of six children to support. Financial worries, coupled with career dissatisfacton, made Hanssen decide to sell secrets to the Soviets for money once again.

Selling secrets to the KGB

In October 1985, Hanssen sent a letter to the KGB, offering his services. Signing the letter "B," Hanssen established his credibility by betraying three KGB officers secretly working for the FBI (Sergei Motorin, Valery Martynov, and Boris Yuzhin—Motorin and Martynov were executed and Yuzhin imprisoned), for which he asked to be paid $100,000. Henceforth—bar the period 1992–99, due to the collapse of the Soviet Union—Hanssen received $1.4 million dollars in cash and diamonds over the next 17 years for revealing details of highly classified counterintelligence

DIGITAL SPYING

Hanssen used computers to support his work as a spy. In 1988, he mailed a disk to the KGB that appeared to be blank but contained a hidden message. By using a procedure called 40-track mode, he had reformatted the disk to have slightly less capacity than usual so that secret messages could be concealed in the "lost area."

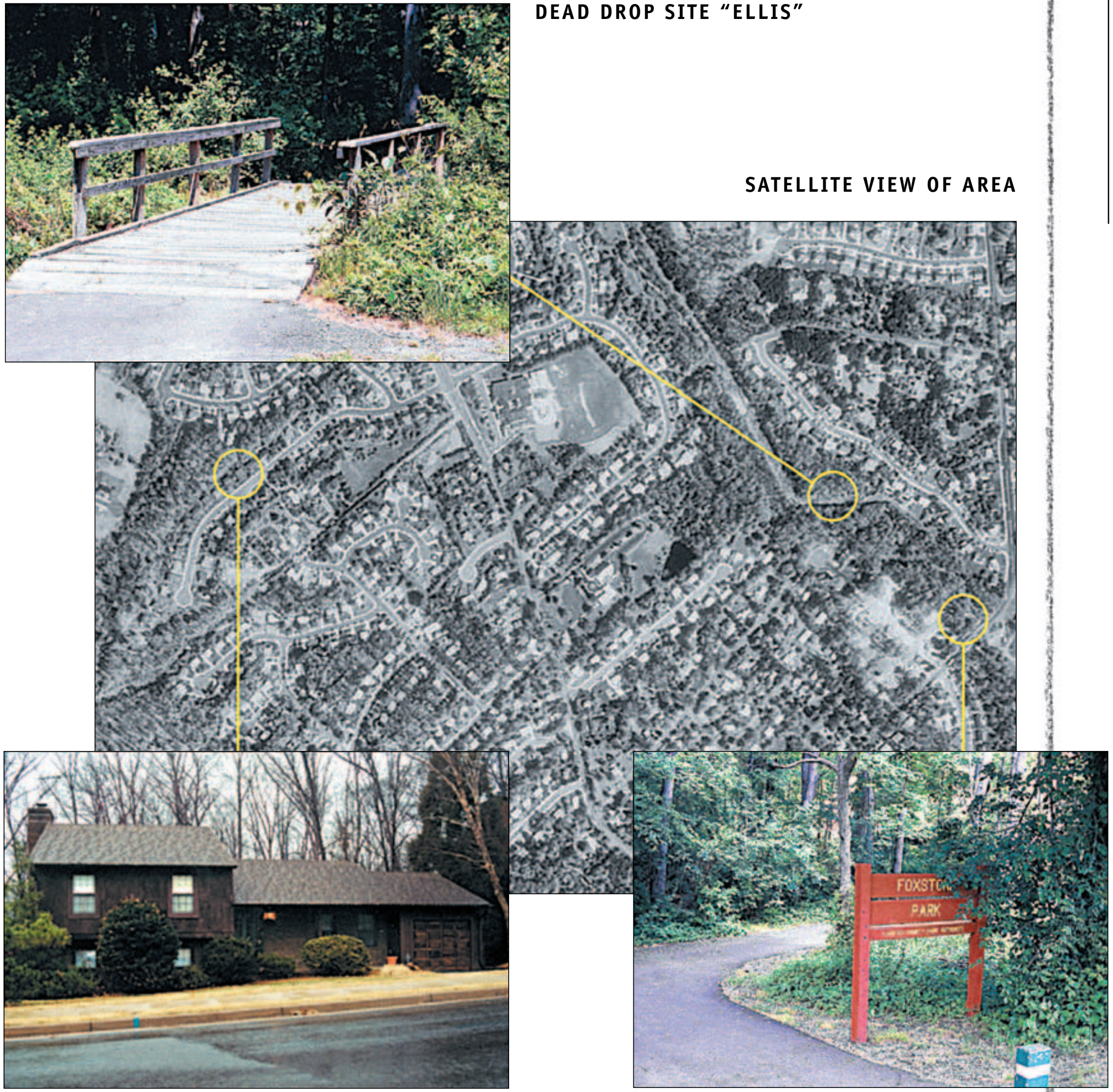
Hanssen wrote letters to the SVR (the KGB's successor) on his home computer and kept copies on a removable 8MB Versa memory card hidden in his briefcase. He used a Palm III handheld computer to schedule appointments with the SVR. On February 5, 2001, the FBI secretly searched Hanssen's Palm and found "Ellis" scheduled for February 18; agents waited there to arrest him.

Palm III
Hanssen could easily carry the compact Palm III in his briefcase. He later asked the SVR for a Palm VII, which could use wireless internet connectivity.

HANSSEN'S FINAL DEAD DROP

At 4:34 p.m. on February 18, 2001, Hanssen drove to Crossing Creek Road, not far from his residence on Talisman Drive in Vienna, Virginia. He parked the car and walked across the road to the entrance of Foxstone Park. On the dark-red wooden post that supported the entrance sign he placed a small strip of white adhesive tape to indicate to the SVR that he was "loading" the dead drop site. An SVR officer driving down the road would spot the tape as a "signal" and arrange for the drop to be "cleared." Similar procedures are used by spies around the world to transfer money and materials without ever having to meet each other.

With the signal in place, Hanssen walked into Foxstone Park along the trail to dead drop "Ellis," which was located beneath the first footbridge over the meandering Wolftrap Creek. He carried with him a slim package that contained seven secret FBI documents and an encrypted letter to the SVR on a computer disk, all wrapped in a black plastic trash bag. The package was placed in the drop site—on a rusted beam beneath the footbridge—invisible to anyone who did not know precisely where to look. Retracing his steps, Hanssen reappeared from the woods nine minutes later. As he crossed the road and approached his car, he was arrested by the FBI, who had had him under surveillance for many months. The FBI had even secretly purchased the house across from Hanssen's, where they had set up an observation post to monitor his activities.



DEAD DROP SITE "ELLIS"

SATELLITE VIEW OF AREA

HANSSEN'S RESIDENCE

SIGNAL SITE IN FOXSTONE PARK

programs. The scope of the secrets Hanssen gave away to the KGB and SVR (the KGB's successor) was catastrophic to American national security interests. Included were technical programs for gathering intelligence on the Soviets in the US, agent names, and more than 6,000 pages of classified documents.

Only five weeks before retirement, on February 18, 2001, when his access to marketable secrets would end, Hanssen sensed he was under FBI surveillance. Nevertheless, he continued spying, leaving a final package at dead drop "Ellis" in Foxstone Park, Vienna, Virginia (Hanssen had by this time been reassigned to Washington, DC). Observed by the FBI, he was arrested. He later pleaded guilty and received a life sentence without the possibility of parole, avoiding the death penalty only by agreeing to reveal all that he had done. Bonnie was allowed a pension.

Money for Hanssen
At the time of his arrest, Hanssen was unaware the Russians had left $50,000 in cash at "Lewis," another drop site at a nearby park.

Sergei Motorin
KGB officer Motorin was one of the FBI agents that Hanssen betrayed in order to establish his credibility.

Ana Belen Montes

THE SENIOR CUBAN ANALYST in the US Defense Intelligence Agency (DIA), Ana Belen Montes (b.1957) spied for Cuba for 16 years before the FBI finally caught up with her in September 2001. In that time, among other acts of betrayal, she told the Cuban General Intelligence Directorate, or DGI, the identities of four US intelligence officers operating on the Caribbean island: the first in May 1994, another in September 1996, and two more in May 1997. Pleading guilty in 2002, she told the trial judge: "Your honor, I engaged in the activity that brought me before you because I obeyed my conscience rather than the law." She was sentenced to 25 years in prison, with no possibility of parole.

Defense Intelligence Agency crest
Montes worked at the DIA's largest facility, the Defense Intelligence Analysis Center (DIAC) at Bolling Air Force Base in Washington, DC.

Recruited by Cuba

The DGI recruited Montes in 1984 on campus at The Johns Hopkins University School of Advanced International Studies in Washington, DC, when she openly criticized US foreign policy while studying for a masters degree. She agreed to spy for Cuba because she saw it as a small country bullied by the United States.

Portrait of an American who spied for Cuba
Of Puerto Rican descent, Montes was born in West Germany, where her father was a US Army doctor. She grew up back in the United States, in Kansas and Maryland, and earned a degree in foreign affairs from the University of Virginia in 1979.

At the time Montes was also a clerk at the US Department of Justice in the US capital. As such, she had no access to secrets useful to Cuba, so in 1985 she considered joining the CIA. But the CIA would have made her take a polygraph (lie detector) test, so instead she successfully applied to become a junior intelligence analyst with the DIA, also in Washington, DC.

At the DIA, Montes was very private and avoided making friends. She always arrived early and stayed late, and dined not in the cafeteria with her colleagues but at her desk, working as she ate. But Montes excelled at her work on Central American affairs and by 1992 she was a senior analyst and the DIA's top expert on Cuba. As such, she was the ideal spy for the DGI, with access to all US intelligence service documents on Cuba, and direct influence on US military policies toward Cuba.

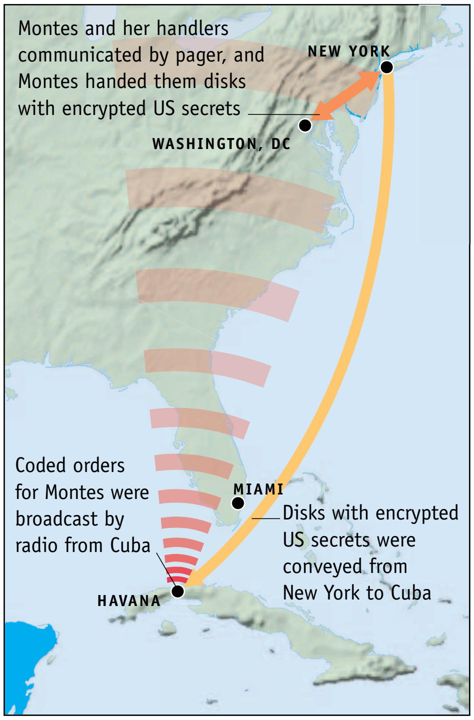
Suspected

The DIA became suspicious of Montes in 1993, when a report she wrote on the Cuban military did not match known facts. Yet in 1994 she somehow passed a polygraph test. She aroused suspicion again in 1996 when, after Cuba shot down two US-registered civilian aircraft, she left an urgent meeting about the attack to take a suspicious call—then declared she would be leaving work early that day.

Two years later, when the FBI rounded up the Hernandez spy ring in Florida, analysis of its covert communications hinted at another Cuban spy in the United States. The FBI assigned the codename Scar Tissue to this UNSUB, or unknown subject. Then in 2000, when US intelligence services asked for help in

HOW MONTES SPIED FOR CUBA

1 *Montes had a series of handlers (see p. 217), all DGI officers posing as diplomats at the Cuban Mission to the United Nations in New York. To contact her in Washington, DC anonymously, they paged her from public phones using prepaid cards, not coins, so that the calls could not be traced. When her pager responded, they entered a three- or four-digit number corresponding to a pre-agreed code. So, "635" might mean "receive orders at eight o'clock tonight." Montes acknowledged such calls in the same way.*


Montes and her handlers communicated by pager, and Montes handed them disks with encrypted US secrets
NEW YORK
WASHINGTON, DC
Coded orders for Montes were broadcast by radio from Cuba
MIAMI
Disks with encrypted US secrets were conveyed from New York to Cuba
HAVANA

FLOW OF INFORMATION

identifying the spy, the DIA suggested Montes. The FBI gave her the codename Blue Wren in November that year.

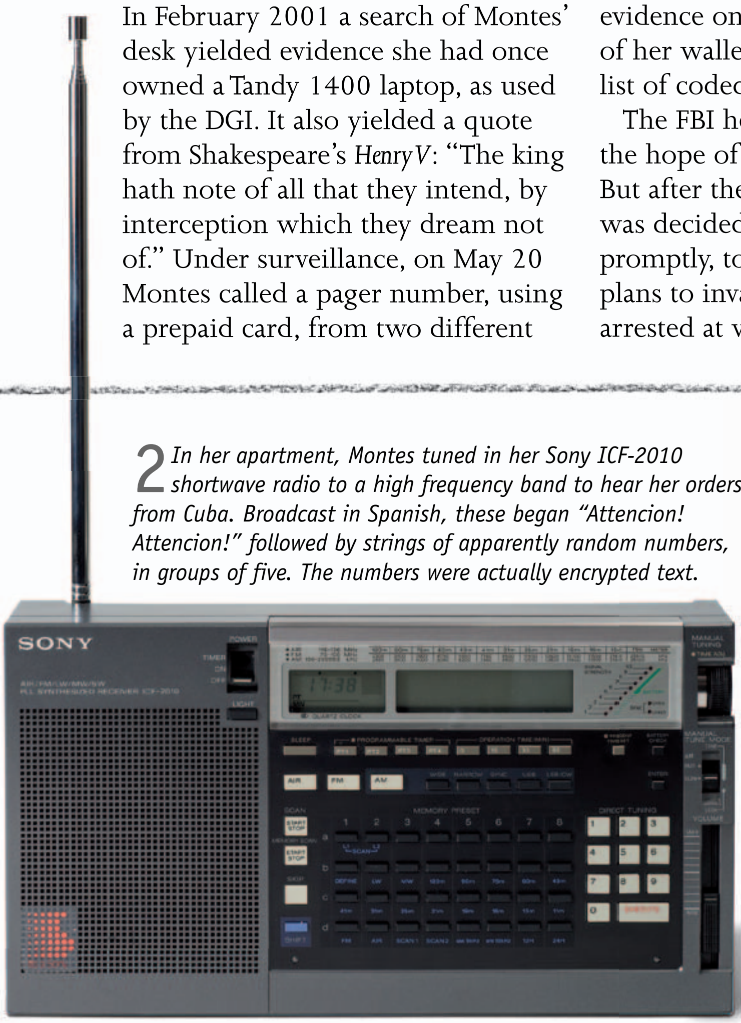
The net closes in

In February 2001 a search of Montes' desk yielded evidence she had once owned a Tandy 1400 laptop, as used by the DGI. It also yielded a quote from Shakespeare's *Henry V*: "The king hath note of all that they intend, by interception which they dream not of." Under surveillance, on May 20 Montes called a pager number, using a prepaid card, from two different public phones: very suspicious behavior for someone known to carry a cell phone. Then on May 25 a search of her apartment uncovered a Sony shortwave radio, and a Toshiba laptop with forensic evidence on its hard drive. Last, a search of her wallet on August 16 turned up a list of coded numbers on soluble paper.

The FBI held off arresting Montes, in the hope of identifying her handler. But after the 9/11 terrorist attacks it was decided to take her into custody promptly, to prevent her disclosing US plans to invade Afghanistan. She was arrested at work on September 21, 2001.

FBI surveillance photograph of Montes
The FBI observed Montes going to public phones in various places to make prepaid card calls on several occasions. One of these places was just outside the entrance to the National Zoo in Washington, DC.

2 *In her apartment, Montes tuned in her Sony ICF-2010 shortwave radio to a high frequency band to hear her orders from Cuba. Broadcast in Spanish, these began "Attencion! Attencion!" followed by strings of apparently random numbers, in groups of five. The numbers were actually encrypted text.*



MONTES' SONY ICF-2010 SHORTWAVE RADIO

3 *Montes keyed the numbers into her laptop and inserted an "R" ("receive") disk given to her previously by a handler. A decrypting program embedded in the disk converted the numbers back into readable text. Until 1996 Montes used a Tandy 1400 laptop. After that she used a Toshiba 405CS.*

"RECEIVE" DISK

4 *To give classified information to Cuba, Montes memorized it at work, then back home inserted an "S" ("send") disk—embedded with a text-encrypting program—into her laptop, keyed in the information, then saved the encrypted text onto a blank disk. She gave these disks to her handler, or to a "cut-out" (see p. 216), in secret meetings in Washington, DC cafés. The disks were probably then conveyed to Cuba in diplomatic pouches.*

"SEND" DISK

MONTES' TANDY 1400 LAPTOP

5 *The DGI instructed Montes to wipe clean the hard drive of her laptops after each "send" or "receive." Crucially, she did not, leaving digital evidence that helped bring about her downfall.*

Counterterrorism

TERRORISM, OR THE PURSUIT of political ends through violence and intimidation, has a history as long as that of espionage. During the second half of the 20th century, however, the phenomenon became more widespread and more dangerous. As a consequence, countering terrorism has come to absorb a large proportion of the efforts of the world's intelligence and security services. Counterterrorist work involves many different types of activity, including human intelligence, direct action, and the use of linked computer networks and powerful databases.

WMD Operations Unit crest
The WMD (Weapons of Mass Destruction) Operations Unit of the FBI receives incident information and provides technical assistance during a suspected or actual chemical, biological, or nuclear incident.

The role of human intelligence

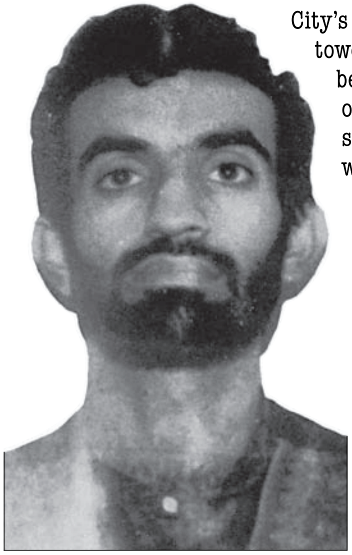
To combat terrorism, governments require accurate intelligence regarding the plans and intentions of terrorist groups. To acquire such information, security services must gather human intelligence from inside the terrorist organizations. This may be achieved through spies who are members of the intelligence services, or through informers recruited from the ranks of the terrorists themselves or from the community within which they operate. The use of such individuals has formed an important part of the British strategy against terrorist groups in Northern Ireland, which is conducted under the overall control of MI5. The Israeli agency responsible for internal security, Shin Bet, has also made much use of spies and informers in infiltrating Palestinian terrorist organizations.

Direct action

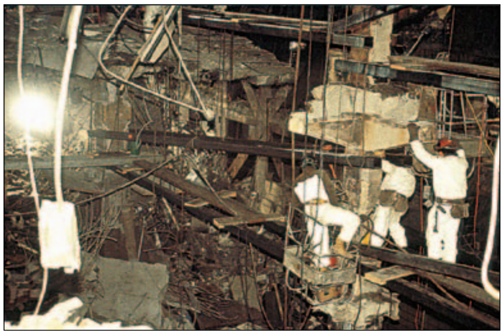
Occasionally, intelligence services have taken direct action against terrorists. Operatives of Israel's Mossad have been active over the years in the assassination of Arab terrorist suspects. Their most notable feat was in 1988, when they penetrated a heavily guarded house in Tunis to assassinate Abu Jihad, a leading figure in the Palestinian liberation movement. Other countries have been less eager to take such obviously traceable action. But there have been cases where proxy organizations have

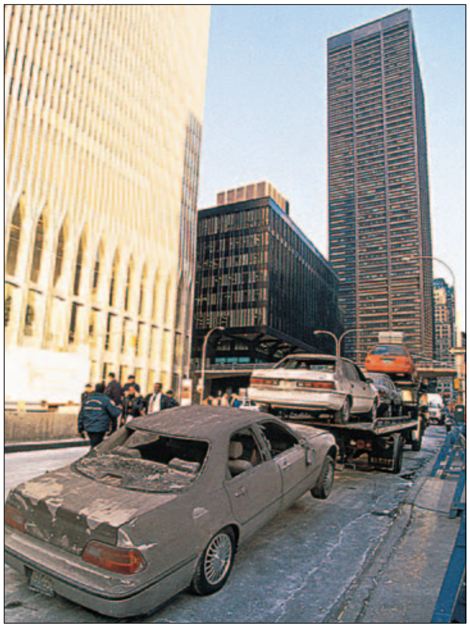
RAMZI YOUSEF

On February 26, 1993, Ramzi Yousef (b.1967) attacked New York City's World Trade Center in an unsuccessful attempt to topple both towers. Two years later, he would flee a hideout in Manila, leaving behind a laptop computer that contained encrypted files outlining a plot to blow up 11 US commercial aircraft in a single day. Yousef was arrested in Pakistan and, in 1998, he was sentenced to life in prison in the United States.



RAMZI YOUSEF





WORLD TRADE CENTER AFTER 1993 ATTACK

been employed to kill terrorist suspects. For example, during the 1980s, the Spanish security services assisted in the creation of Grupos Antiterroristas de Liberación (GAL), which murdered a number of people suspected of membership of the Basque separatist terror group ETA. There has also been criticism of the CIA's activities in El Salvador and Guatemala during the 1970s and 80s, where it is accused of involvement with right-wing "death squads," responsible for killing many left-wing revolutionary suspects.

Tactics since the Cold War

The end of the Cold War during the final decades of the 20th century saw a period of global instability that allowed the rise of Islamic extremist groups and "rogue" nations around the world.

Terrorist groups are able to use the worldwide web to add a truly global dimension to their activities. Terrorist cells employ the internet to communicate with each other in secrecy. Encrypted messages carrying instructions or maps can be posted on existing sites, and their origins are effectively untraceable. Internet communication may also be used by terrorists to launch cyber-attacks on electronic data held by those whom they identify as their enemies. As a consequence, security agencies must find ways to monitor these communications; however, the vast scale of the internet makes this task very difficult.

The internet works in many ways to the advantage of terrorists. However, security services have been aided in their hunt for terrorists by digital technology that permits the creation of linked computer networks, powerful databases, and the use of artificial intelligence.

A further threat that has risen to prominence recently is the possibility that a terrorist group might launch a biological, chemical, or even nuclear attack in pursuit of its goals. All these things are possible in theory although, thankfully, not so easy to put into practice. However, intelligence agencies are very aware of the need to forestall attacks by such "weapons of mass destruction," especially the necessity of preventing fissionable material, capable of being made into a nuclear device, from falling into the wrong hands.

Osama bin Laden
Osama bin Laden (b.1957) founded the Islamic extremist movement, al Qaeda, and has claimed responsibility for the attack on 9/11. He is the "most wanted man in the world" and is believed to be hiding in the rugged mountainous area between Afghanistan and Pakistan.

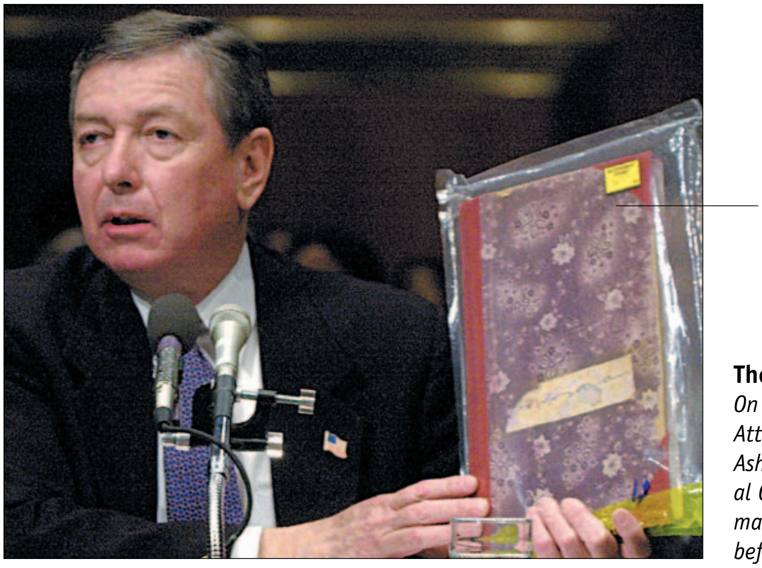
September 11, 2001

The terrorist attack on the United States on September 11, 2001—9/11—saw the dawn of a new era in counterterrorism. Over 3,000 people lost their lives when hijacked airliners were crashed into the World Trade Center in New York City and into the Pentagon building in Virginia.

The perpetrators were members of the extreme Islamic organization al Qaeda, who were at that time operating covertly from several countries and, more openly, from Afghanistan. The goal of al Qaeda is to rid Muslim countries of Western (and particularly American) influence. The scale of the attack was unprecedented in the annals of terrorism. As a direct result, there arose an international commitment to wage a "war on terrorism," which would involve both intelligence services and conventional forces. For the world's security and intelligence services, this means that counterterrorist operations have become central to their role.

AL QAEDA TRAINING MANUAL

A manual produced by al Qaeda that passed into American hands contains chilling evidence of the Islamic extremist organization's goals. The 11-volume manual provides instructions on the best ways to kill thousands of people and spread fear in the United States and Europe by attacks against targets "with high human intensity," such as skyscrapers, airports, and packed football stadiums. It also urged actions against Jews in every country, by attacking their organizations, institutions, clubs, and hospitals.

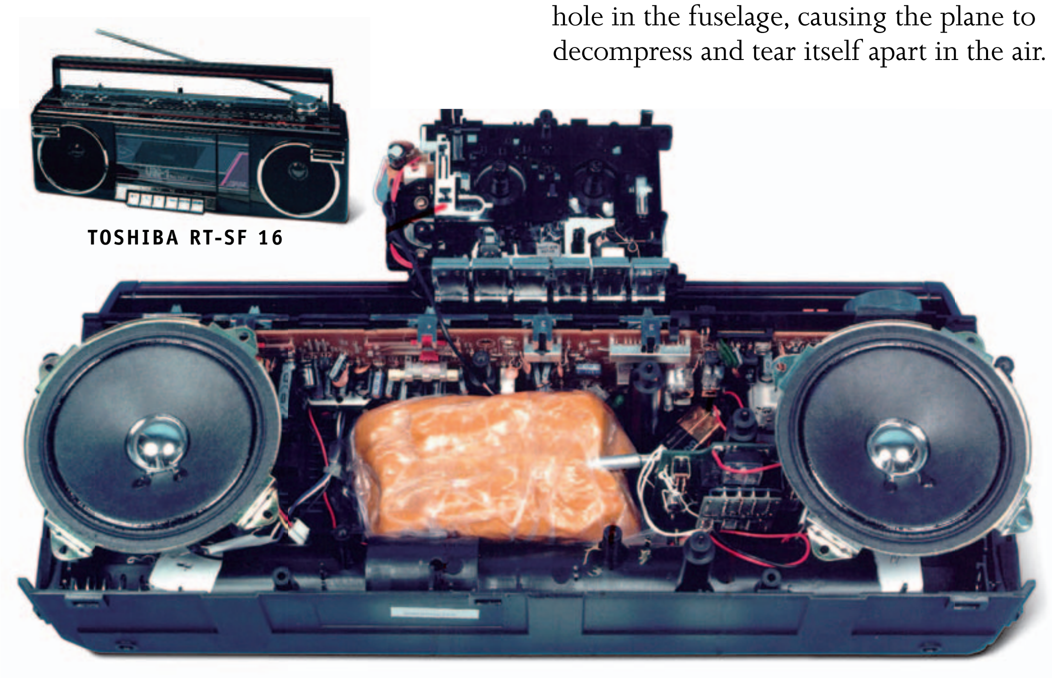


The manual exposed
On December 6, 2001, Attorney General John Ashcroft showed the al Qaeda training manual in testimony before the US Senate.

Pan Am 103

ONE OF THE BIGGEST TERRORIST INVESTIGATIONS involving intelligence agencies was that into the downing of Pan American World Airways Flight 103 on December 21, 1988. Half an hour after it took off from London, bound for New York, *Clipper Maid of the Seas,* a Boeing 747, disintegrated in the air just after it had leveled off at about 31,000 ft (9,500 m). Moments later, debris and flaming fuel from the plane rained down on the town of Lockerbie in Scotland and on the surrounding area. All 259 people on board the plane—243 passengers and 16 crew—and 11 people on the ground were killed in the disaster.

Among the passengers were several US intelligence officers, including Matthew Channon, Deputy Chief of the CIA's office in Beirut in Lebanon. The CIA quickly concluded that the plane had been brought down by a terrorist bomb, but they needed evidence. For months more than a thousand police officers and soldiers combed hundreds of square miles, recovering thousands of bits of wreckage. Within a week, the British government's Air Accidents Investigation Branch (AAIB) had found traces of Semtex plastic explosive on the circuit board of a Toshiba RT-SF 16 Bombeat radio-cassette player. Tests by the US Federal Aviation Administration (FAA), the FBI, and Britain's Defence Evaluation and Research Agency (DERA) confirmed that an improvised explosive device (IED) had been built inside the radio-cassette player, which was in a brown Samsonite suitcase stored in a baggage container in the forward cargo hold. It had blown a hole in the fuselage, causing the plane to decompress and tear itself apart in the air.



The improvised explosive device (IED) reconstructed
Following a series of test explosions, experts from the FBI and Britain's Defence Evaluation and Research Agency (DERA) determined that as little as 14 oz (400 g) of Semtex was enough to blast the hole found in the plane's fuselage.

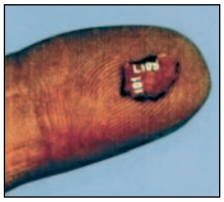
A crash investigator at work on the plane
More than 10,000 bits of wreckage were recovered from in and around Lockerbie. Investigators were then able to reconstruct the fuselage of the plane, revealing an 18 in (45 cm) blast hole in one side.

The forensic breakthrough

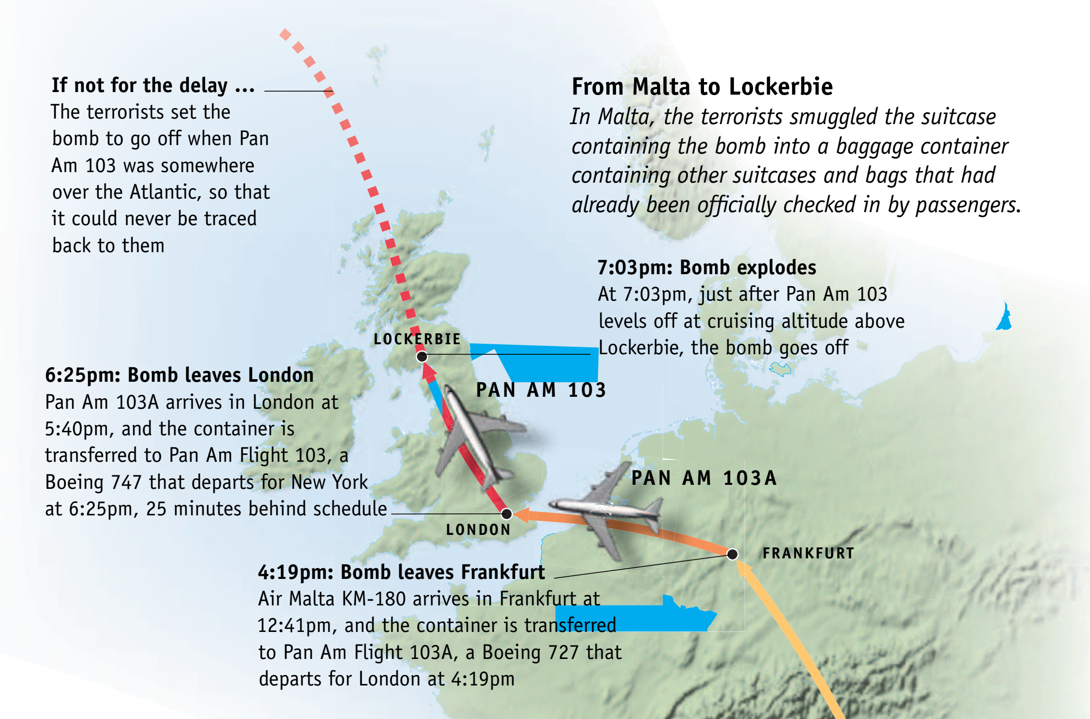
Semtex is widely used by many Middle Eastern terrorist groups, but for many months there was no evidence of who had made the IED or placed it on the plane. Then remnants of a T-shirt embedded with a tiny piece of circuit board were found in a field nearly 80 miles (130 km) from Lockerbie.

The shirt bore the label of Mary's House, a shop in the town of Sliema in Malta. When British police officers visited the shop, its owner recalled a Middle Eastern man buying clothes indiscriminately, without regard to size, as if he simply wanted to fill a suitcase. The clothes had included an identical T-shirt to the one found in the field.

To learn more about the fragment of circuit board, the FBI's explosives unit contacted the CIA's top electronics investigator, a man with the cover name "Mr Orkin." Amazingly, he was able to identify it as being part of a particular type of timer board, the MST-13, made



Timer-board fragment
Although measuring only ½ sq in (25 sq mm), the fragment was identified as part of a timer board made by a firm in Switzerland.



If not for the delay ...
The terrorists set the bomb to go off when Pan Am 103 was somewhere over the Atlantic, so that it could never be traced back to them

From Malta to Lockerbie
In Malta, the terrorists smuggled the suitcase containing the bomb into a baggage container containing other suitcases and bags that had already been officially checked in by passengers.

7:03pm: Bomb explodes
At 7:03pm, just after Pan Am 103 levels off at cruising altitude above Lockerbie, the bomb goes off

6:25pm: Bomb leaves London
Pan Am 103A arrives in London at 5:40pm, and the container is transferred to Pan Am Flight 103, a Boeing 747 that departs for New York at 6:25pm, 25 minutes behind schedule

4:19pm: Bomb leaves Frankfurt
Air Malta KM-180 arrives in Frankfurt at 12:41pm, and the container is transferred to Pan Am Flight 103A, a Boeing 727 that departs for London at 4:19pm

9:52am: Bomb leaves Malta
The suitcase containing the bomb, which is timed to go off at 7:00pm, is put in a baggage container. This container is loaded onto Air Malta Flight KM-180, a Boeing 737 that departs for Frankfurt at 9:52am

The nose cone where it landed
Britain's Air Accidents Investigation Branch (AAIB) concluded that the nose cone of the Boeing 747 broke away from the fuselage within three seconds of the blast, giving the cockpit crew no time to react.

by a Swiss firm, Meister and Bollier, or MEBO, in Zurich. The firm admitted it had made just 20 MST-13 timer boards: all for Libya's Ministry of Defense.

As part of an IED, an MST-13 could be set to delay the explosion for up to 10,000 hours. In the Pan Am 103 IED, the MST-13 had been set to detonate when the plane was somewhere over the Atlantic, so that any physical evidence that could be traced back to the terrorists would be lost in the ocean. But the plane's take-off from Heathrow was delayed by nearly half an hour. If Pan Am 103 had taken off on time, it is highly unlikely that any evidence of what had caused the disaster would ever have been found, or that anyone would have eventually been convicted of the crime.

Brought to trial

But how had the suitcase containing the IED evaded security scans and made its way onto Pan Am 103? The container it was in had originally been loaded onto a plane in Malta, but there was no record of the suitcase being checked in there.

Then a Libyan defector named two Libyan intelligence officers as the bombers: Abdel Basset Ali Megrahi (b.1952) and Al Amin Khalifa Fhimah (b.1956). Megrahi was head of security for Libyan Arab Airlines, and was identified by the owner of Mary's House in Malta as the man who had bought the T-shirt and other clothes. Fhimah was the station manager for Libyan Arab Airlines at Malta's Luqa Airport. Investigators concluded that Megrahi and Fhimah had smuggled the suitcase onto the original plane in Malta, knowing that the baggage container it was in would be transferred in Frankfurt to a feeder flight—Pan Am 103A—for Pan Am 103.

The acquitted and the convicted
Fhimah (left) was acquitted, but Megrahi (right) received a 21-year sentence in 2001. In 2007 the Scottish Criminal Cases Review Commission granted Megrahi an appeal that is still pending.

Megrahi and Fhimah were indicted in 1991, but Libyan leader Muammar Gaddafi refused to extradite them. By 1998, however, economic sanctions against Libya had taken their toll, and Libya handed the two men over. They were tried in the Netherlands, chosen for its neutrality in the affair. To secure a conviction, "Mr Orkin" had to testify. But if he had been identified in court, his cover would have been blown and his life and his family's lives endangered. So specialists from the CIA's Office of Technical Service (see p. 96) expertly crafted a physical disguise to change his appearance and so protect his identity.

Largely as a result of "Mr Orkin's" testimony, on January 31, 2001, Megrahi was found guilty of masterminding the bombing. Fhimah was found not guilty.

Digital espionage

DIGITAL TECHNOLOGY has made it possible for intelligence agencies to gather and analyze vast amounts of information. However, the wide availability of the personal computer and the internet have changed the ways that spies operate and brought new challenges for intelligence. For example, whereas government code-breakers were once able to intercept and break most enemy ciphers, the ready availability of advanced encryption software now strains even the most advanced supercomputers. In addition, as the superpowers become increasingly reliant on networked systems so they become more vulnerable to digital spies and sabotage.

Supercomputers

Powerful, super-fast computers with massive storage capacities enable intelligence agencies to analyze vast amounts of information quickly.

Gathering information

Satellites that could produce electro-optical digital images were first used in the 1970s. The images could be beamed to ground stations as soon as they were taken, making them immediately available for analysis. Moreover, such image-collecting spy satellites have been joined by "ears in space," satellites that are capable of eavesdropping on all forms of communication signals and transmitting them back to terrestrial stations. The increasing use of radio frequencies for the transmission of telephone and computer data makes these listening satellites capable of collecting ever larger amounts of information. With speech recognition software, the satellites are able to filter out unnecessary pieces of information and recover messages that incorporate specified keywords being communicated by both friends and foes. More than 50 years ago, CIA Director Allen Dulles observed that 80 percent of everything spies need to know is openly available. The internet has become the repository of the information needed to fuel the economies of the world's superpowers and the analysts of intelligence services. The keys to this "fountain of knowledge" are high-speed internet access, advanced networking, and massive computer power to analyze billions of bits of data in order to discover the secrets hidden inside. Powerful internet browsers are even now traveling through cyberspace into the computers and networks of both the suspecting and unsuspecting in order to record their secrets. In the immediate future, a clever computer programmer will unleash "cyber-agents" to recover more vital information in a day than a thousand fictional James Bonds could recover in a lifetime.

MENWITH HILL MONITORING STATION

Menwith Hill, in Yorkshire, England, is one of the world's most sophisticated communications monitoring posts. It employs more than 1,000 Americans belonging to the US National Security Agency (NSA) and 600 British staff working closely with the UK's GCHQ (Government Communication Headquarters). With its dozens of satellite receivers housed inside huge white domes, the site is thought to be the center for Project Echelon, a global system for intercepting all email, phone, fax, and telex communcations. Its massive computers can lock onto conversations or messages for analysis if certain key words (such as terrorist) are used.

Recruiting spies

Convicted KGB spy John Walker (see p.54) noted after his arrest that the defenses of the United States were constructed to protect against enemies from outside, not from the treachery of Americans within. Purchasing secrets from traitors still remains an extremely effective and profitable means of intelligence collection. Hostile

DIGITAL STEGANOGRAPHY

Steganography is the science of hiding messages. While cryptography attempts to scramble a message in a systematic manner so that it can only be read by the intended recipient, steganography hides the message in a way that conceals the fact it even exists. Microdots are forms of steganography, as is secret writing. Modern digital steganography can combine the two techniques by encrypting (systematically scrambling) the message and then hiding it to conceal its existence. Messages or images can be hidden inside any form of digital media including graphic images, websites, and recorded music.

ORIGINAL IMAGE

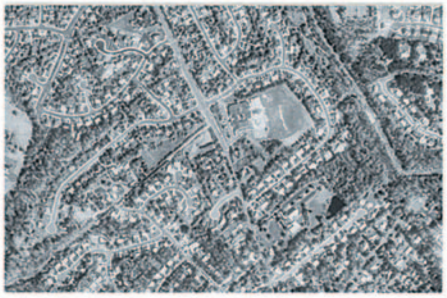
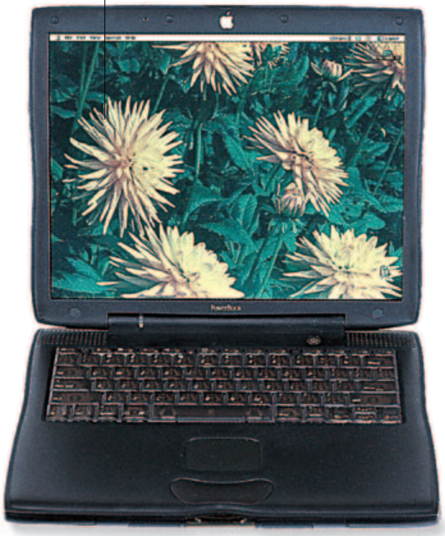


IMAGE TO BE HIDDEN



Innocent-looking image containing "secret" image ready to be emailed

COMBINED "HARMLESS" IMAGE

intelligence services traditionally relied on intuition and informants to identify people who could be recruited as spies. Excessive personal debt, substance abuse, and failed careers were often the first indicators of weaknesses that could be used as levers for recruitment. Digital spies can now carry out computerized checks on the internet to uncover spending habits, debt loads, medical records, and job-change patterns in order to identify potential recruits. By using the internet as a spotting tool, the efforts of intelligence services can be focused on a small pool of potential recruits who have existing weaknesses waiting to be exploited.

Communicating

A spy operating in hostile territory was most vulnerable not when stealing secrets, but rather when attempting to communicate them to his handler. The internet has reduced this area of vulnerability for the spy. The use of chat rooms, internet auction sites, and innocent-appearing web pages makes it easy to send and receive coded messages and instructions. Advanced encryption techniques may be combined with digital steganographic techniques for embedding messages or images into a scan, or a voice or music recording. Even the most powerful computers strain under the power required to analyze trillions of individual pieces of data for patterns that may indicate the presence of an embedded message.

Analysis

Espionage analysts have always worked behind the scenes to convert many individual pieces of information from sources around the world into a useful intelligence product—information that political and military leaders need to make better decisions. Analysts rely increasingly on technology. Powerful computers, supplemented by artificial intelligence programs, neural networks, and three-dimensional databases are used to collate information from all sources to discern patterns and make predictions. Still, the ability to collect intelligence is growing faster than our abilities to create a usable report from a mass of seemingly unrelated information. Sorting the few grains of wheat from the vast mass of chaff is the key to successfully compiling a meaningful report.

Phil Zimmermann
Zimmermann created PGP, an advanced encryption software program, and is noted for work in Voice Over Internet Protocol encryption. Use of encryption by terrorists and spies presents new challenges.

Counterintelligence

Digital technology works in many ways to the spy's advantage, but it can also be useful to counterspies. The internet makes it much harder to establish the identity of a spy who has adopted a cover or legend (see p. 206). It enables a vast range of personal information to be quickly checked by searching such sources as local property tax records and professional association memberships.

EQUIPMENT AND TECHNIQUES

The equipment and techniques of spying have become far more complicated and imaginative than the earliest spies could ever have envisaged. Most spies operate in unique situations, so each needs techniques and equipment tailored to his or her needs.

To operate effectively, a spy must be able to gain access to secret information, duplicate or steal it, escape undetected, and communicate with his or her controller. This has meant the development of an enormous range of cameras, listening devices, lockpicks, communication devices, enciphering and deciphering techniques, concealments, and weapons. All this equipment must be capable of being easily disguised or hidden to ensure the safety of the spy, and must be designed to work even if it is not used for years at a time.

The sophistication of espionage equipment is closely matched by that of the spycatchers, who are constantly engaged in attempting to apprehend spies. This section shows in great depth the incredible range of spying equipment and techniques.

CAMERAS

SINCE ITS INVENTION in 1827, photography has played an increasingly important role in intelligence-gathering and espionage. Spies use cameras for taking photographs of people; places such as airfields or other military installations; and objects from bridges to military equipment and from aircraft designs to documents. To be most effective, a spy may need to avoid taking photographs openly. In these cases, a small, easily concealed camera capable of taking high-quality pictures is needed. Many cell phones now include digital cameras that take good spy photos, and don't arouse any suspicion. Film cameras for document photography are being replaced by digital devices to steal secrets from computer networks.

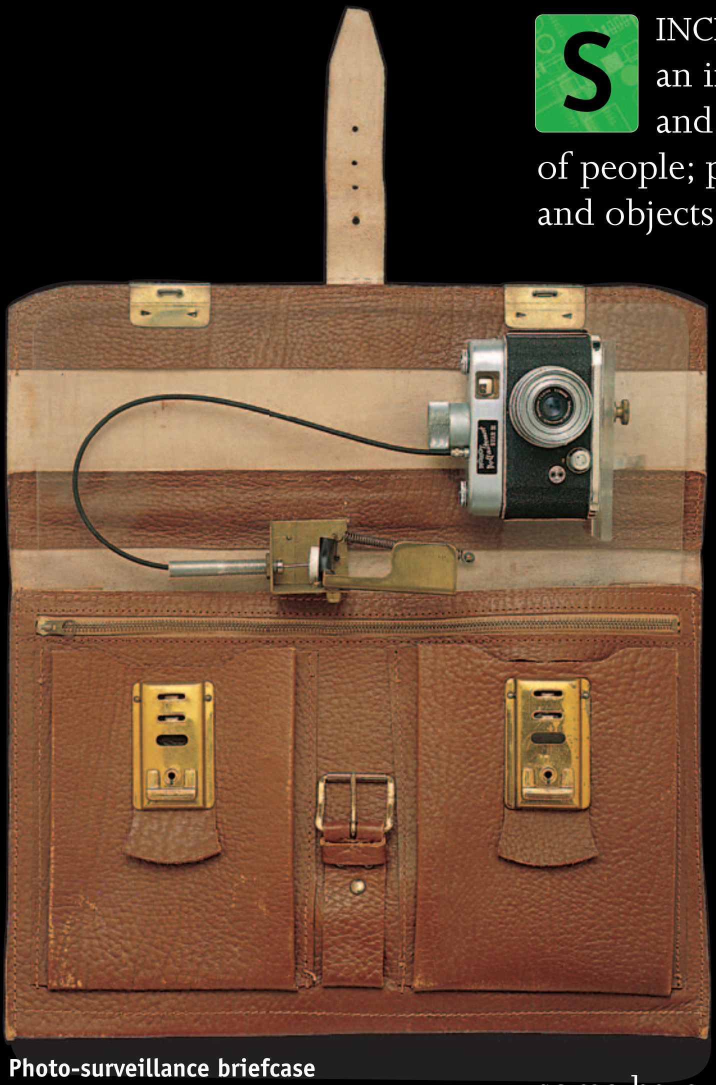


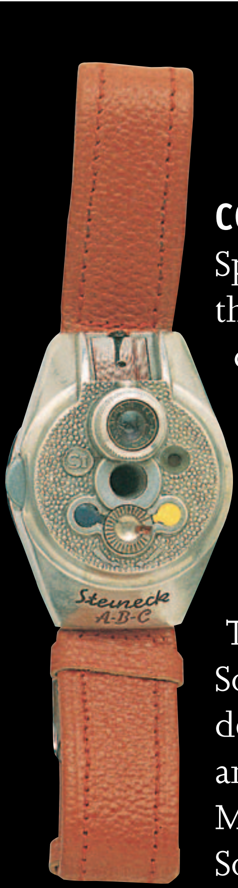
Photo-surveillance briefcase
A Robot camera is concealed in a briefcase for surveillance use. The camera has to be aimed instinctively, without the use of a viewfinder, while the case is held under the user's arm.

Miniature cassettes
These modern film cassettes are designed for clandestine CIA cameras. They are shown here actual size.

SUBMINIATURE CAMERAS

Small enough to carry in the pocket, subminiature cameras can be adapted for a variety of uses. In addition to general photography, most are suitable for surveillance photography and document copying. To make them easier to conceal, some have no viewfinder, and must be aimed instinctively. The most famous and successful one is the Minox, first made in 1938. Although not originally intended for use in espionage, its excellent lens, small size, and quality of construction made it eminently suitable. Accessories enable it be used in concealments or for document photography, and it has been widely used by intelligence services. Other commercially produced subminiature cameras include the Echo 8 cigarette-lighter camera and the Steineck wristwatch camera, both used in the Cold War. In World War II, intelligence services, unable to obtain enough Minox cameras, developed their own cameras, notably the matchbox cameras of the French secret service and the OSS (see p. 32).

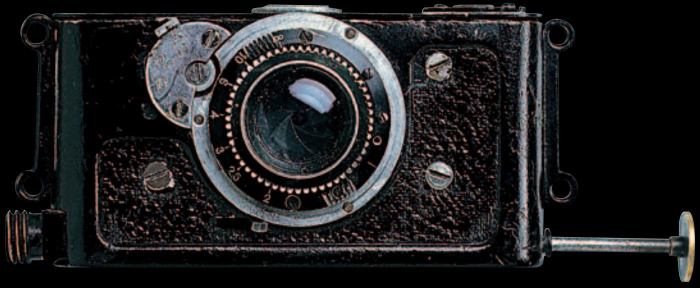
Minox film canister
First produced in 1938, the Minox camera used preloaded cassettes of film providing 50 exposures.



Steineck ABC wristwatch camera
This camera could take six pictures, under the pretense of checking the time.

CONCEALED CAMERAS

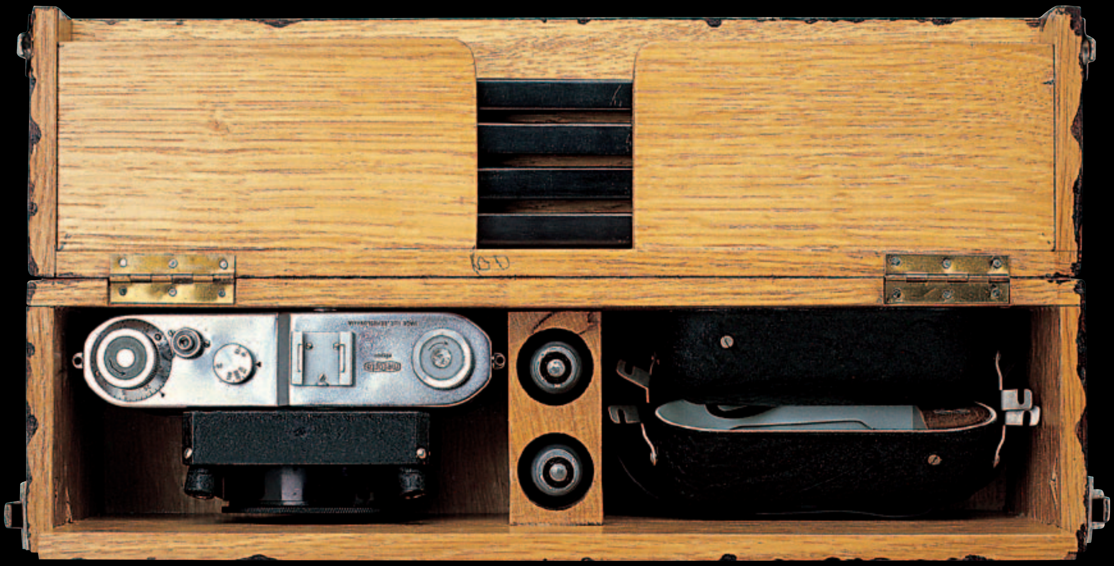
Spies often need cameras that will enable them to take photographs without being detected. Cameras may be hidden inside an object such as a handbag, or strapped to the body, with the lens hidden behind a fake tiepin or button. With the latter, pictures are taken by means of a remote shutter release hidden in a pocket. Two commonly used concealed cameras were the Soviet F21 and the West German Robot. Both were developed from a pre-World War II German design, and used spring-driven motor winding mechanisms. Many concealments have been devised, some by Soviet and Western intelligence agencies and some by the Robot factory itself (see p. 86).



KGB surveillance camera
Designed to be concealed in the hand, or worn by the spy in a body harness, this camera was operated by pressing the actuating rod.

COPY CAMERAS

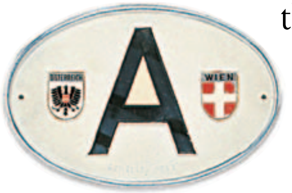
A special class of cameras exists for the task of photographing documents. They are often custom-made, but commercial copy cameras are available, with special accessories. A standard camera can be used when necessary, but skill and practice are needed to obtain acceptable images. Most intelligence services issue special copy camera kits, housed in unobtrusive boxes or attaché cases, which can be used by agents who do not have specialized photographic skills. The KGB developed a miniature copy camera the size of a Minox film cassette for smuggling past security checks. Later, the same agency issued a "brush" camera that is swept across documents like a hand-held photocopier, photographing as it goes.



Czech copy camera
Used for document photography by personnel of the Czech security agency StB, this camera was housed in an anonymous-looking wooden case.

Concealed cameras I

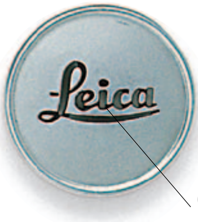
SPIES USE CONCEALED CAMERAS for covert photography. The camera may be hidden under a spy's clothing, or disguised as another object. While some subminiature cameras have only one fixed disguise, there are concealed cameras that may be disguised in a number of ways. For example, the Tessina, Robot (see p. 86), and F21 (see p. 88) each have a special line of concealments. Standard cameras can be used clandestinely if equipped with special attachments like the vehicle nationality plate (left) with one-way glass in the "A" through which pictures can be taken.



VEHICLE PLATE CONCEALMENT

CIA-modified lens cap

The word "Leica" has been cut out of this standard camera's lens cap. Pictures can be taken through the cutout while the lens cap is on and it appears as though the camera is not being used.

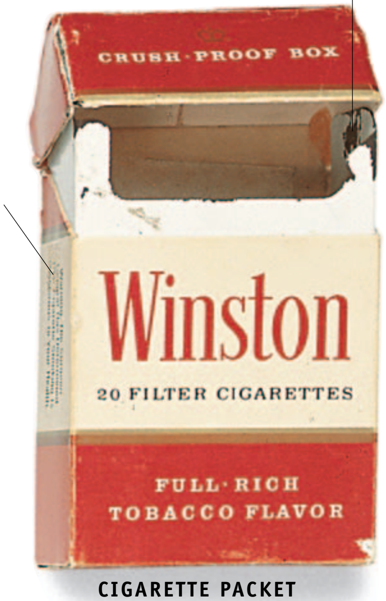


MODIFIED LENS CAP

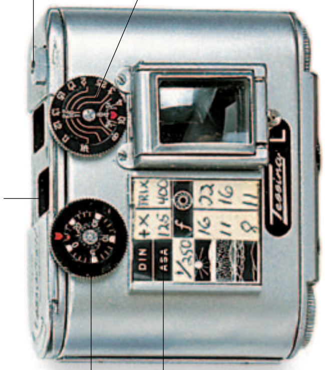
STANDARD LEICA CAMERA

Tessina camera in cigarette packet

The world's smallest motor-driven 35mm camera, the Swiss Tessina fits in a cigarette pack (this should be a brand recognized in the country where it will be used). An internal frame holds the lens aligned with tiny holes in the pack. The shutter release is pressed through the pack, to take up to 10 pictures before rewinding is necessary.



CIGARETTE PACKET CONCEALMENT



TESSINA CAMERA

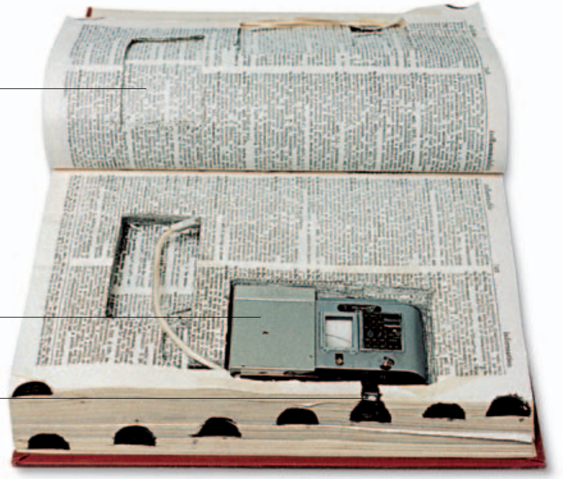
VICTOR OSTROVSKY

SPY PROFILE

Canadian-born Victor Ostrovsky (b.1949) was brought up in Israel and served in the Israeli navy. In 1983 he joined the Israeli secret service, Mossad (see p. 178 and p. 209). He became a case officer, or *katsa*, and developed many original concealment and photographic techniques for his employers. Ostrovsky recorded his experiences working for Mossad in his best-selling book *By Way of Deception*, which was published in 1990, after he had left Israel.

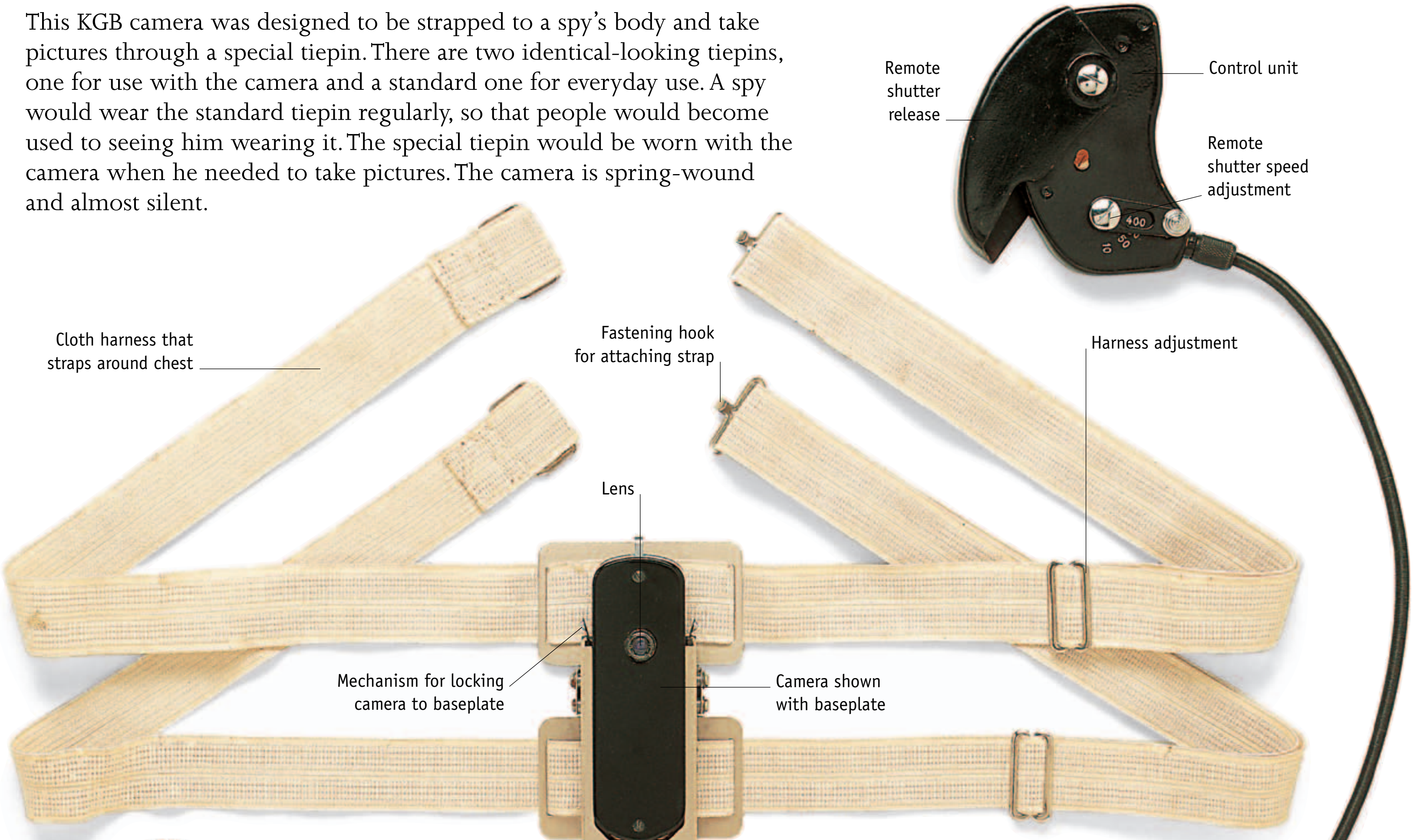
Tessina camera concealed in book

The tiny Tessina camera may alternatively be hidden inside a cutout section of a book. Pictures can be taken through the side of the book by applying pressure to the cover, and thereby operating a shutter release plate.

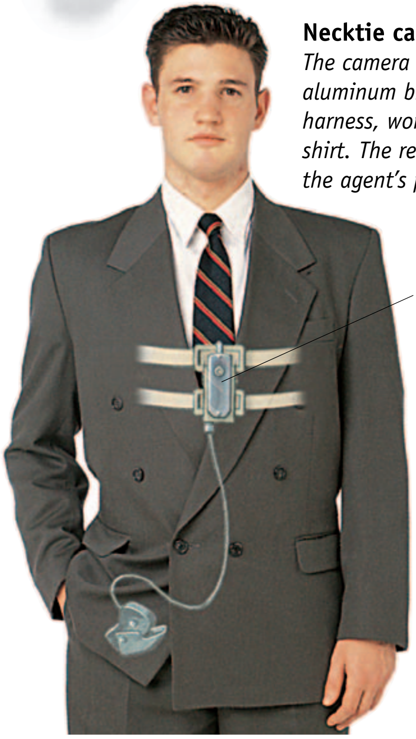


Toychka 58-m necktie camera

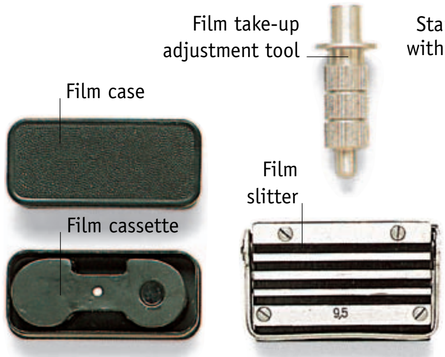
This KGB camera was designed to be strapped to a spy's body and take pictures through a special tiepin. There are two identical-looking tiepins, one for use with the camera and a standard one for everyday use. A spy would wear the standard tiepin regularly, so that people would become used to seeing him wearing it. The special tiepin would be worn with the camera when he needed to take pictures. The camera is spring-wound and almost silent.


Remote shutter release
Control unit
Remote shutter speed adjustment
400
50
10
Cloth harness that straps around chest
Fastening hook for attaching strap
Harness adjustment
Lens
Mechanism for locking camera to baseplate
Camera shown with baseplate
K-№657514
Remote cable to control unit

KGB NECKTIE CAMERA



Necktie camera in use
The camera is held by an aluminum bracket to a cloth harness, worn under the agent's shirt. The remote cable runs to the agent's pants pocket.



FILM LOADING EQUIPMENT

TIEPIN

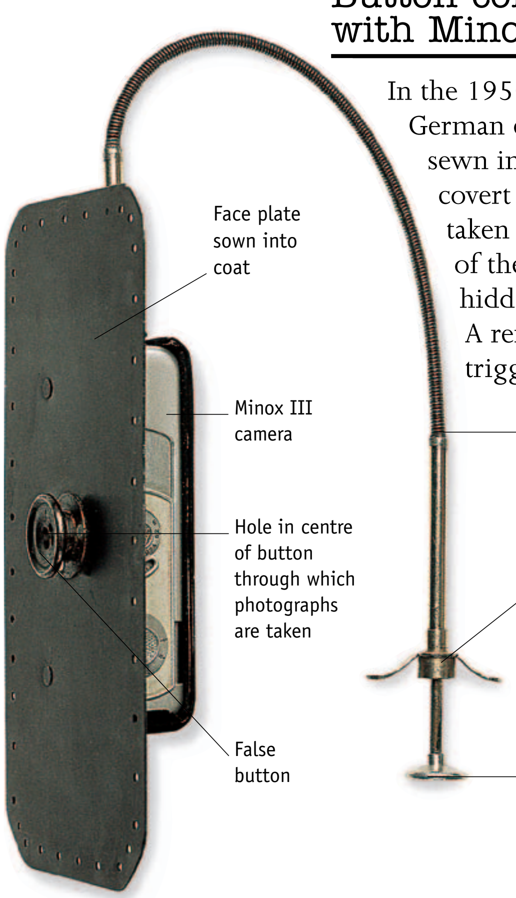
TECHNICAL DATA

Negative size	⅓ x ½ in (8.5 x 11 mm)
Film	9.5mm Minox cassette format; special film slitter provided for reduction of 35mm film
Cassette	Standard Minox cassette with 50 exposures
Shutter speeds	1/10, 1/50, 1/150, and 1/400 second
Winder	Spring-wound; 27 exposures in sequence
Dimensions	3¼ x 1¼ x ⅝ in (8.3 x 3 x 1.5 cm)

Concealed cameras II

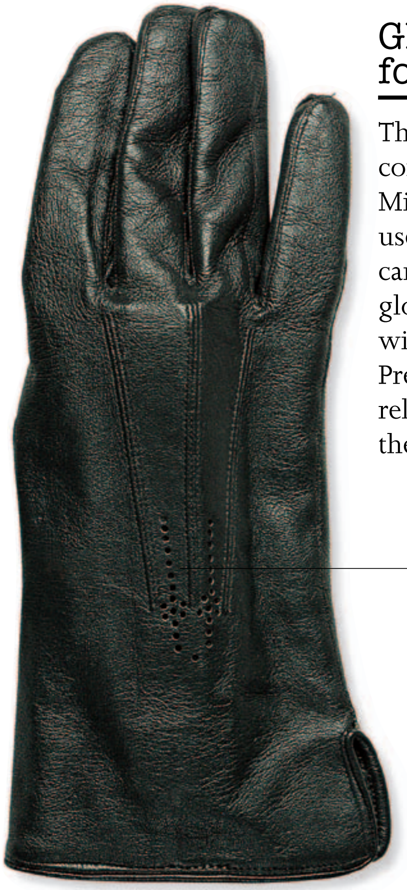
Button concealment with Minox III camera

In the 1950s, this special East German concealment was sewn inside a coat to allow covert photographs to be taken through the center of the button by using a hidden Minox camera. A remote shutter release triggered the camera.

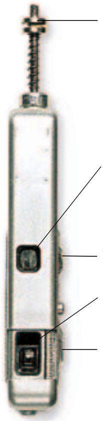

Face plate sown into coat
Minox III camera
Hole in centre of button through which photographs are taken
False button
Cable
Finger grip
Remote shutter release

Glove concealment for modified Minox

The Stasi made this glove concealment for a modified Minox camera that can be used with one hand. The camera is hidden inside the glove so that its lens lines up with a hole in the leather. Pressing the spring-rod releases the shutter and then advances the film.



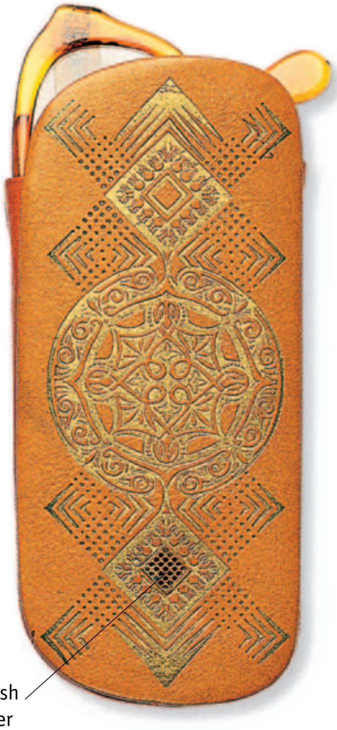
GLOVE CONCEALMENT



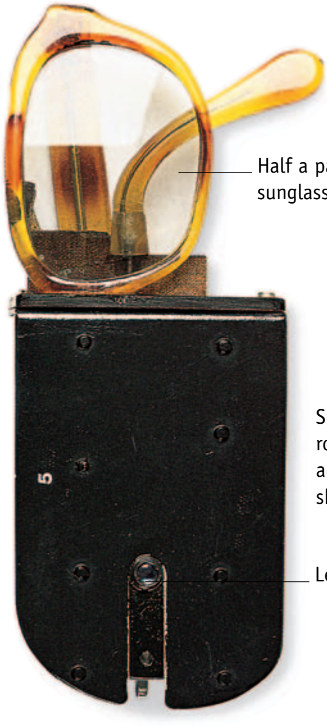
MINOX CAMERA

Sunglasses case concealment

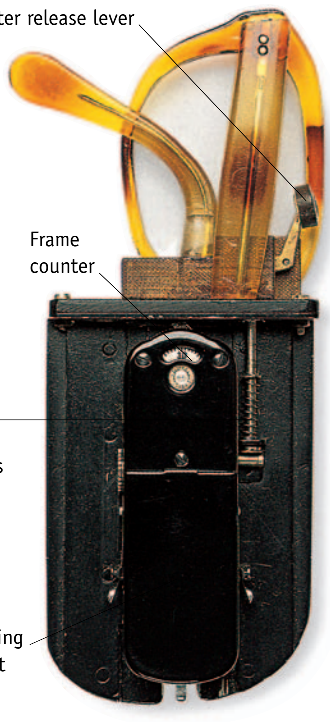
The surveillance department of the Stasi (see p. 99) created this intriguing concealment. Inside a false sunglasses case is hidden a KGB Toychka surveillance camera. Half a pair of sunglasses in the case adds to the illusion that masks the presence of the camera. The operator would carry the case in one hand and take pictures by depressing a lever on the side of the case. A spring-driven winder inside the camera allowed many photographs to be taken without having to remove the camera from its case to wind on the film.



CAMERA IN CASE



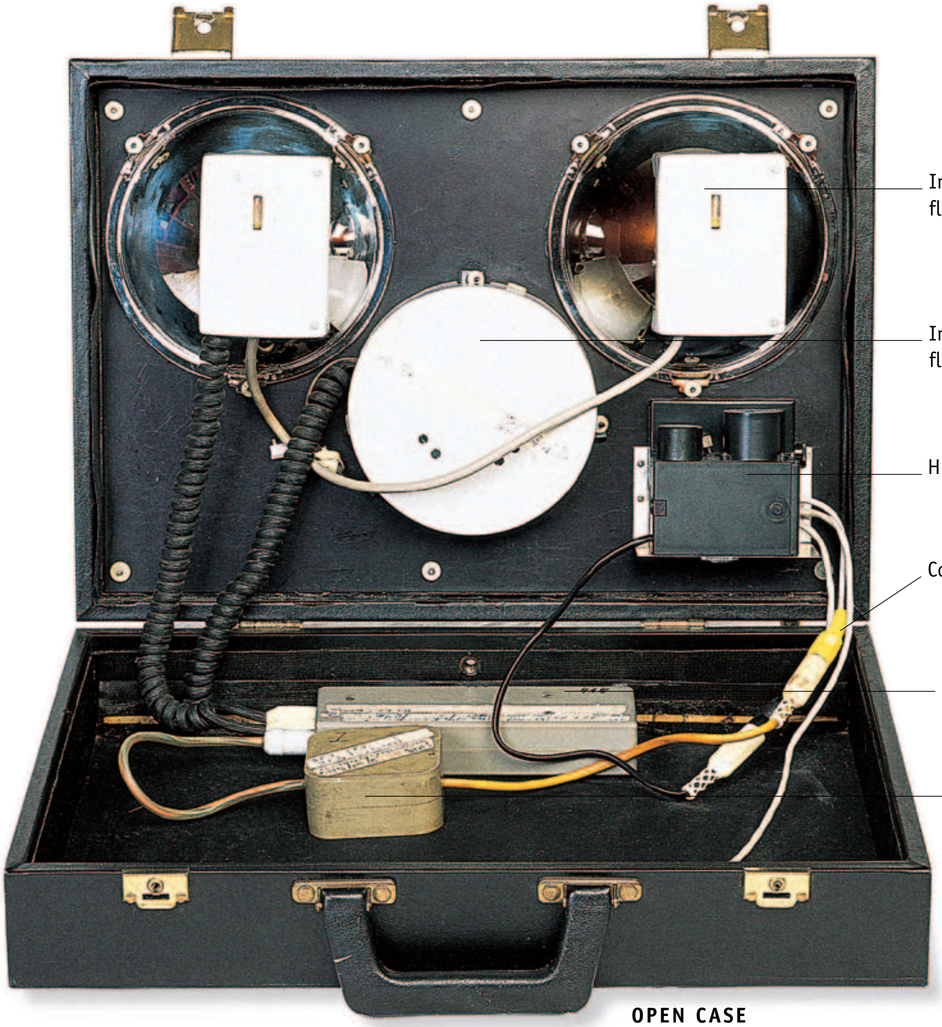
FRONT VIEW OF CAMERA



BACK VIEW OF CAMERA

Surveillance attaché case

This surveillance briefcase, made by the Stasi, can take infrared (IR) flash photographs in complete darkness. The internal Zeiss HFK camera, with a silent electronic shutter, photographs onto IR film through a small opening in the attaché case. The case is covered in a special fabric that allows IR light to pass through but appears opaque to the eye. The infrared flashes through the case's covering are invisible to the human eye.

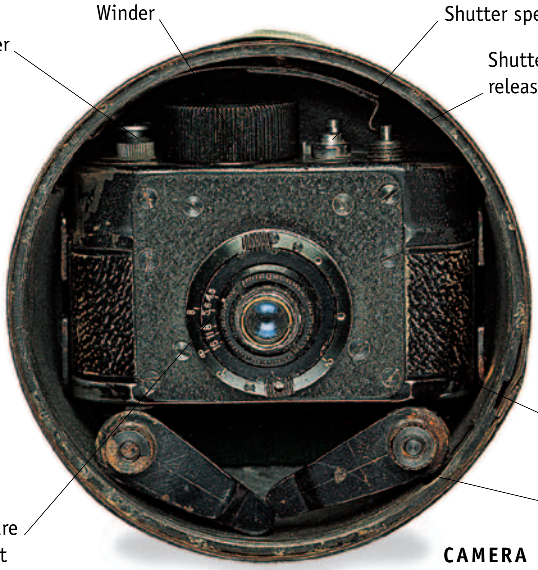


OPEN CASE

CLOSED CASE

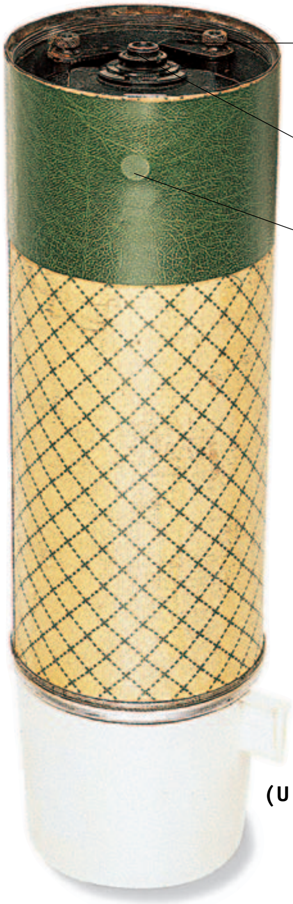
Thermos concealment

The KGB modified this functioning thermos to conceal an F21 camera (see p. 88). The thermos would be carried by a member of the 7th Directorate (KGB's surveillance team) on the street or inside a factory to secretly photograph an unsuspecting target. The F21's spring-driven winder allowed multiple photographs to be taken rapidly.



CAMERA IN FLASK BASE

BASE COVERING WITH LENS OPENING



THERMOS (UPSIDE DOWN)

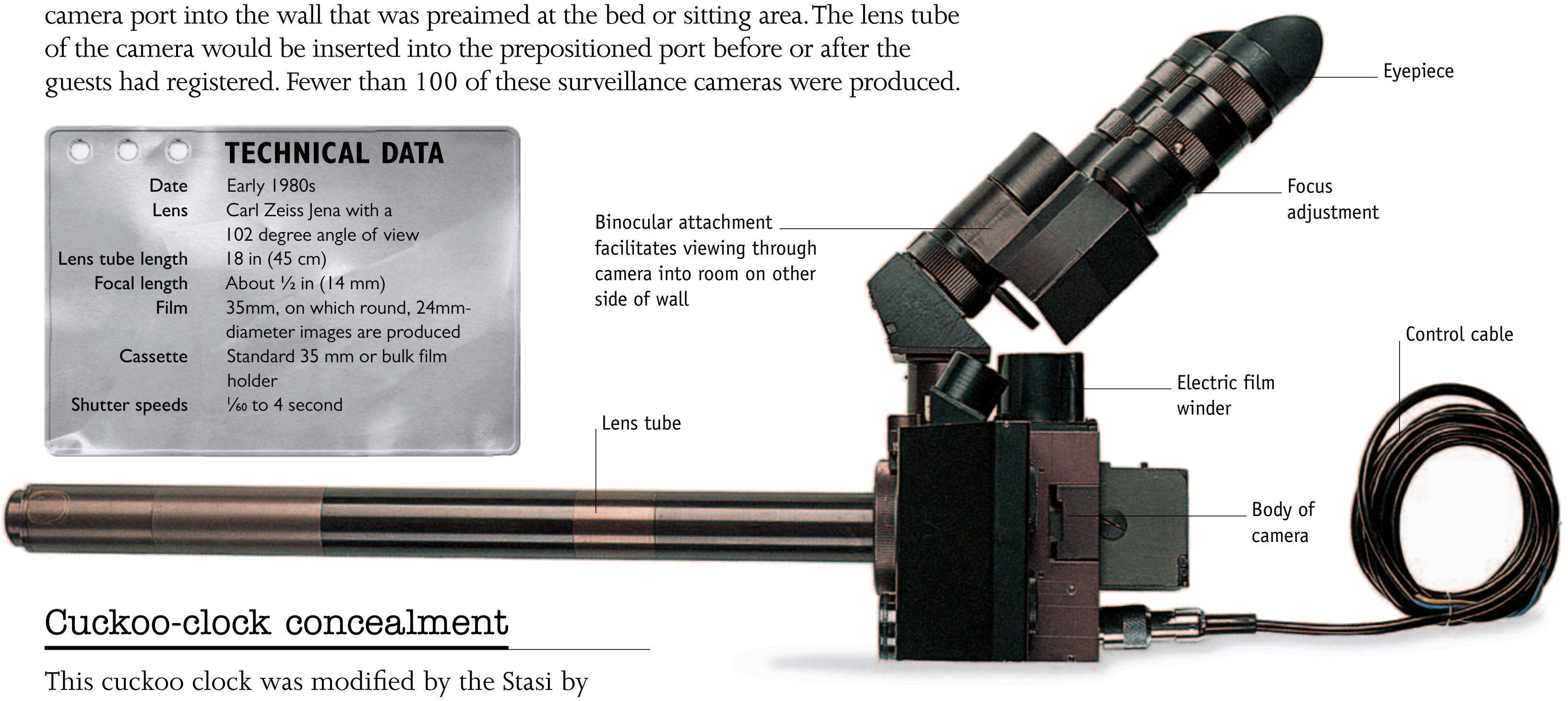
Concealed cameras III

Beobachtungskomplex II through-the-wall camera

The East German Stasi (see p. 99) produced this specialized camera during the 1980s for clandestine photography in hotels. Selected rooms were modified by building a camera port into the wall that was preaimed at the bed or sitting area. The lens tube of the camera would be inserted into the prepositioned port before or after the guests had registered. Fewer than 100 of these surveillance cameras were produced.

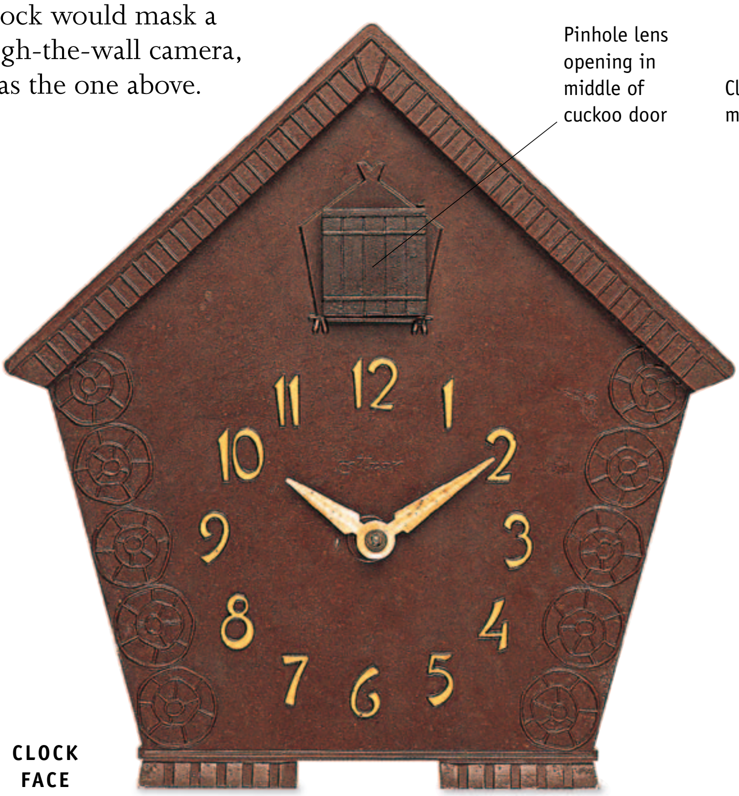
TECHNICAL DATA

Date	Early 1980s
Lens	Carl Zeiss Jena with a 102 degree angle of view
Lens tube length	18 in (45 cm)
Focal length	About ½ in (14 mm)
Film	35mm, on which round, 24mm-diameter images are produced
Cassette	Standard 35 mm or bulk film holder
Shutter speeds	1/60 to 4 second

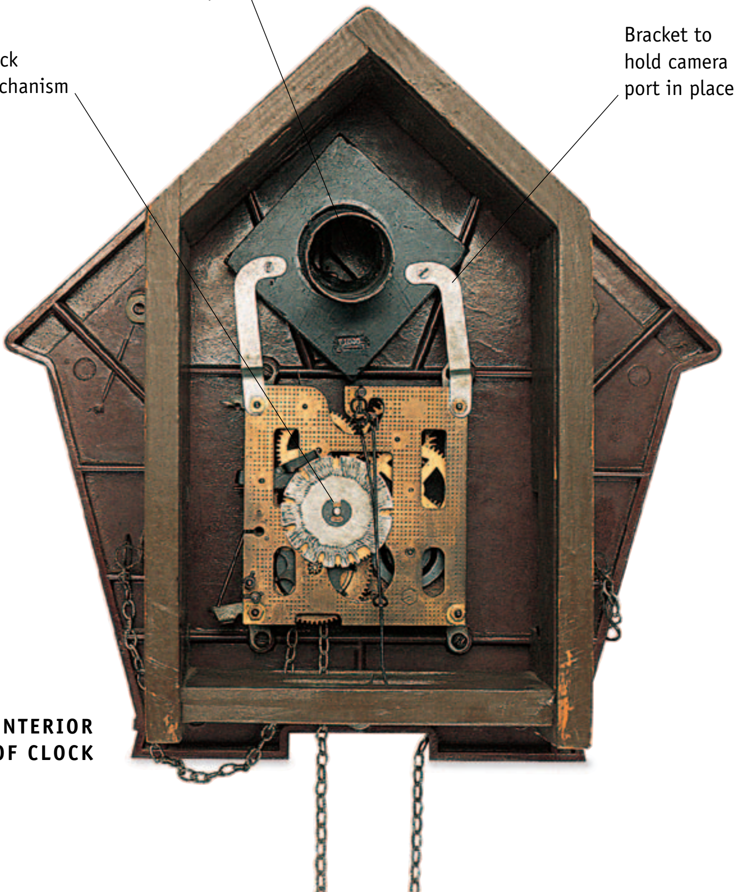

Eyepiece
Focus adjustment
Binocular attachment facilitates viewing through camera into room on other side of wall
Control cable
Electric film winder
Lens tube
Body of camera

Cuckoo-clock concealment

This cuckoo clock was modified by the Stasi by adding a camera port and concealed lens opening above the number 12 on its face. When mounted, the clock would mask a through-the-wall camera, such as the one above.



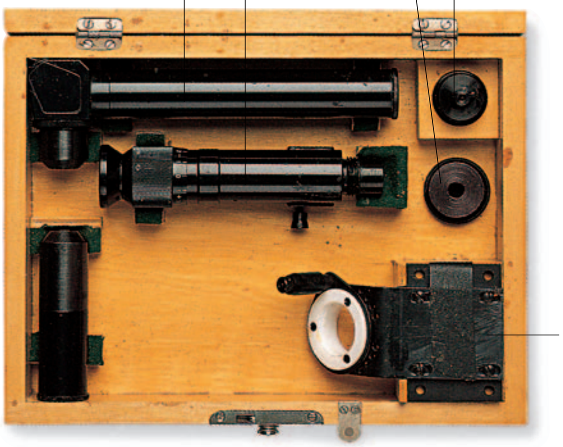
CLOCK FACE



INTERIOR OF CLOCK

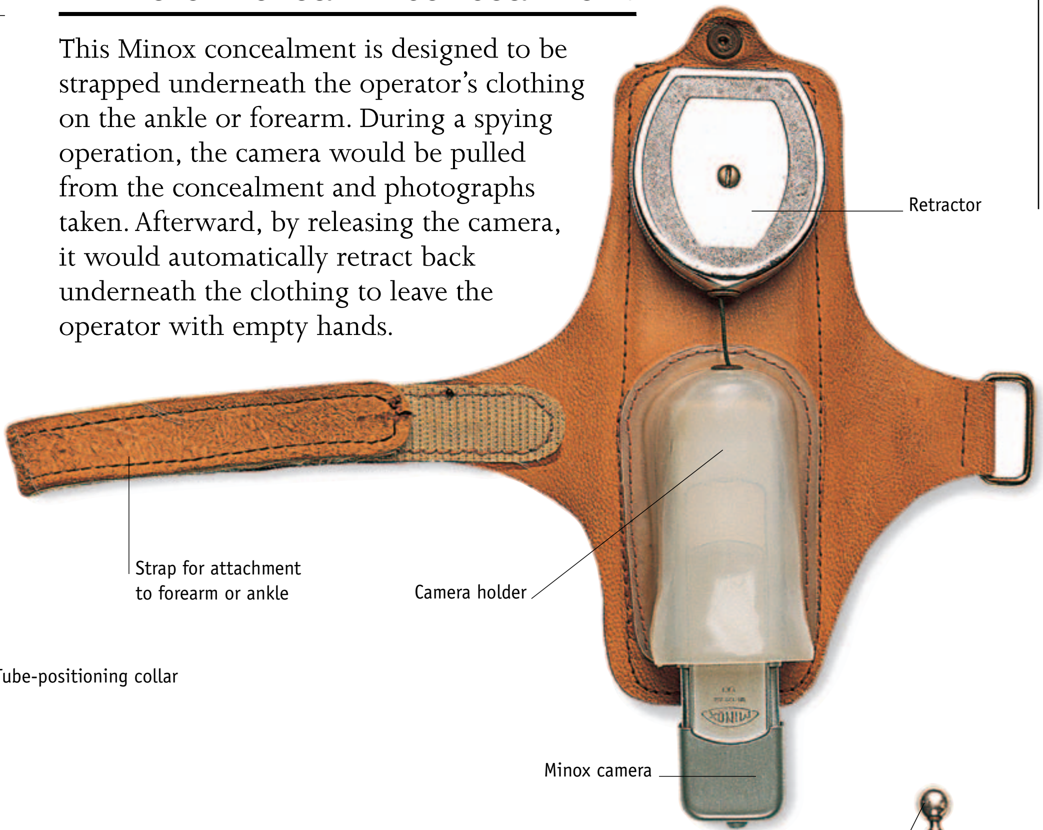
Through-the-wall viewing kit

Made by the KGB, this kit comprises a viewer and optical tubes for the surveillance of a targeted meeting or hotel room. The tubes go through a wall as far as a pinhole opening on the other side. By using the viewing tubes, the operator would know when to trigger a remote camera.



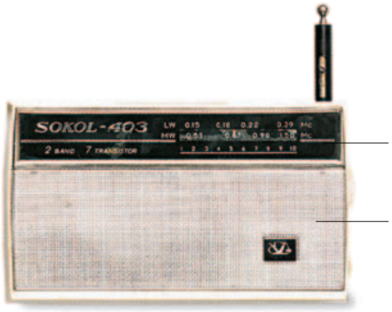
Ankle or forearm concealment

This Minox concealment is designed to be strapped underneath the operator's clothing on the ankle or forearm. During a spying operation, the camera would be pulled from the concealment and photographs taken. Afterward, by releasing the camera, it would automatically retract back underneath the clothing to leave the operator with empty hands.

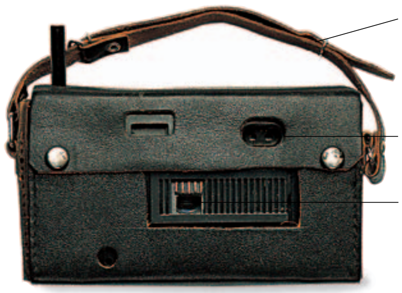


Radio with F21 camera

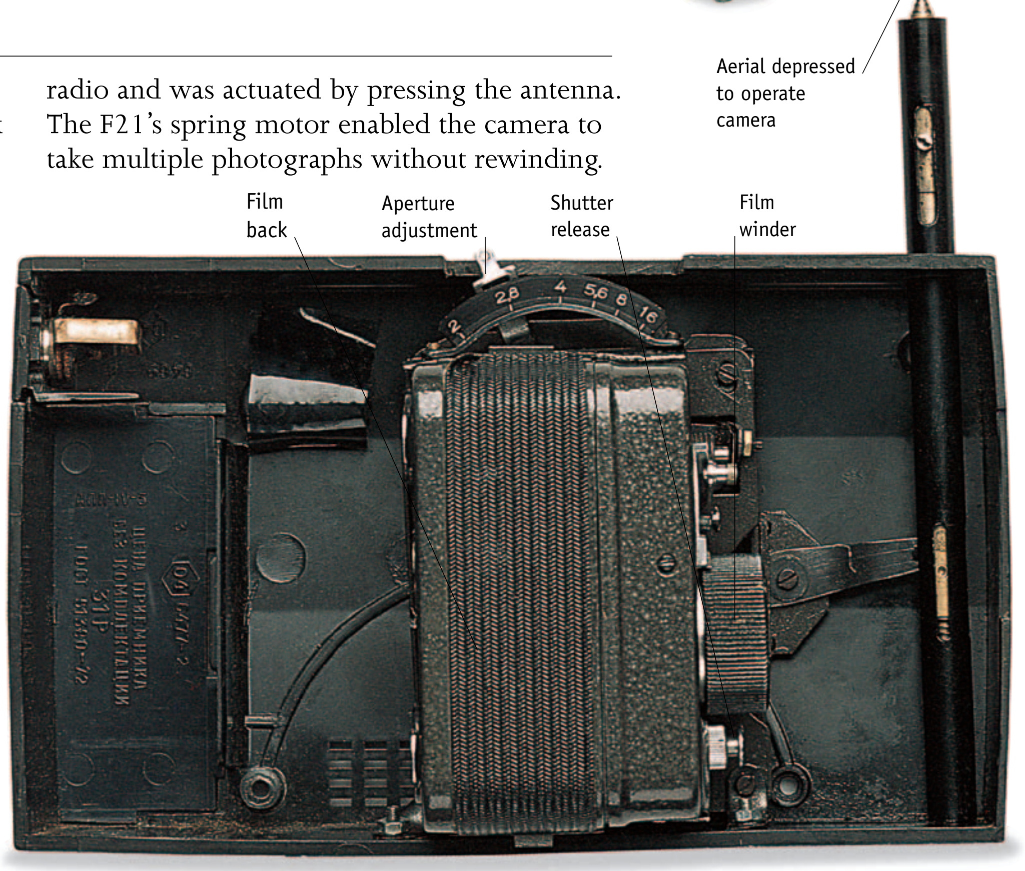
This small radio was used to conceal a KGB F21 surveillance camera (see p. 88). The camera took pictures through an opening in the back of the radio and was actuated by pressing the antenna. The F21's spring motor enabled the camera to take multiple photographs without rewinding.



RADIO FACE



RADIO IN CASE



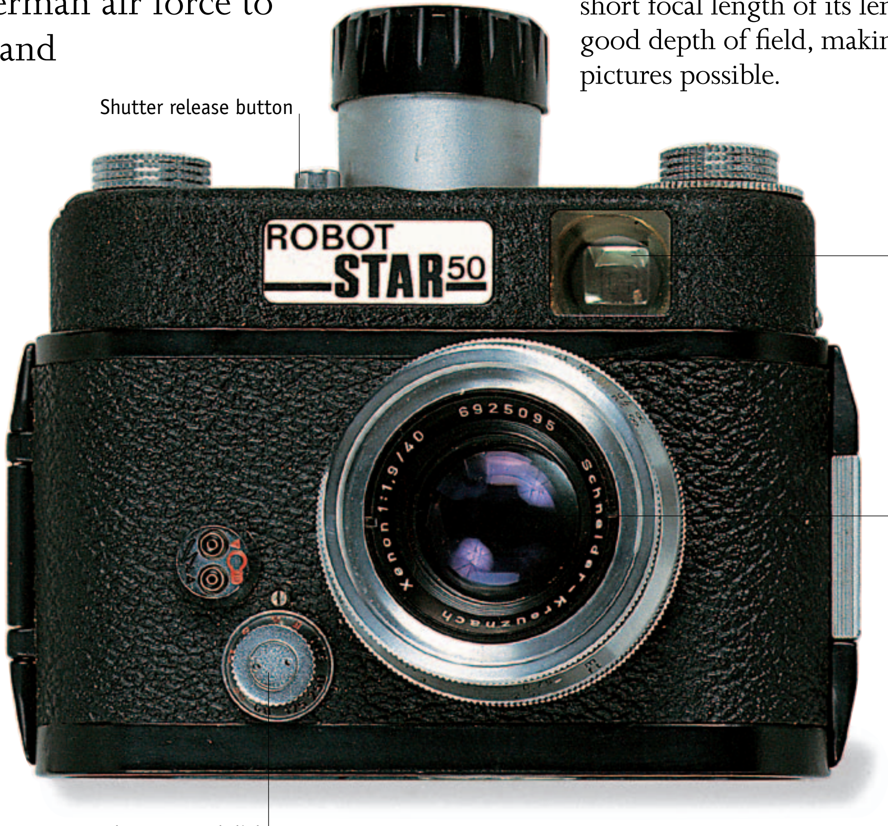
INTERIOR OF RADIO SHOWING CAMERA

Robot camera

THE ROBOT CAMERA, dating from 1934, was powered by a spring-driven motor that allowed successive pictures to be taken without the user having to wind on manually. It was used in World War II by the German air force to provide proof of destroyed targets and by the German intelligence service (see p. 34). In the early years of the Cold War, spies in both the communist bloc and in the West used it because, with no need for hand winding between photographs, it could be used in a variety of concealments.

Robot star 50 camera

The Star 50 was the last Robot model to evolve from the World War II design. It could take 50 pictures and the short focal length of its lens meant good depth of field, making sharp pictures possible.

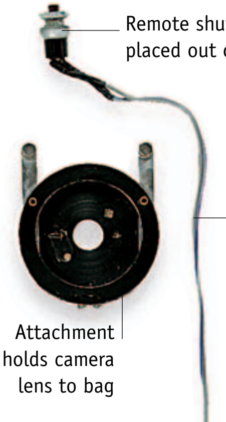


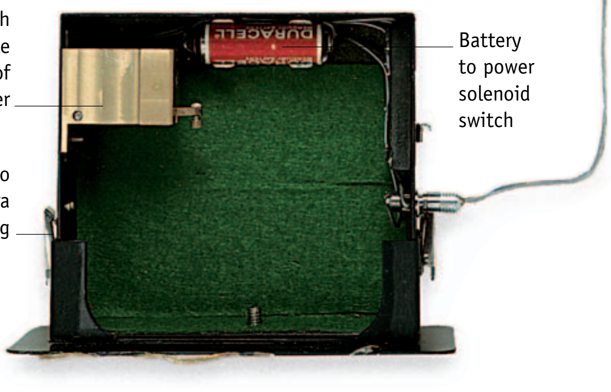
TECHNICAL DATA

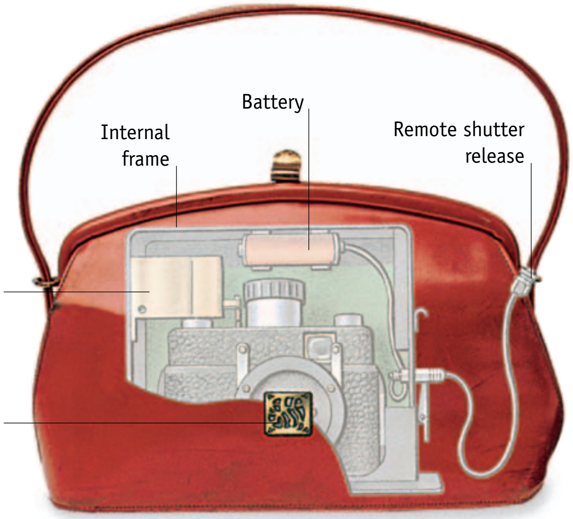
Date	1969
Lens	Xenon 40 mm f1.9
Negative size	About 1 x 1 in (24 x 24 mm)
Film	Standard 35 mm or special film, depending on application; 50 exposures
Shutter speeds	Rotating shutter, ¼ to ¹⁄₅₀₀ second plus bulb setting
Motor	Double spring-wound
Options	Special silent, slow-winding model available from factory

Handbag concealment kit

The Robot factory owners were aware of the different intelligence applications of its line of cameras, and made kits that enabled them to be installed in a variety of objects. This kit allows the user to hide a Robot Star 50 inside a handbag. The hidden camera takes the photographs through a decorative metal ornament, of which a wide selection was available from the manufacturer.


Remote shutter release, placed out of sight
Cable
Attachment holds camera lens to bag


Solenoid switch for remote operation of shutter
Internal frame to hold camera inside bag
Battery to power solenoid switch



METAL ORNAMENTS

Handbag concealment
The Robot concealment kit could be installed in a variety of bags. Care was taken to select a type of bag that was commonly carried in the intended country of use and that was also strong enough to support the camera.

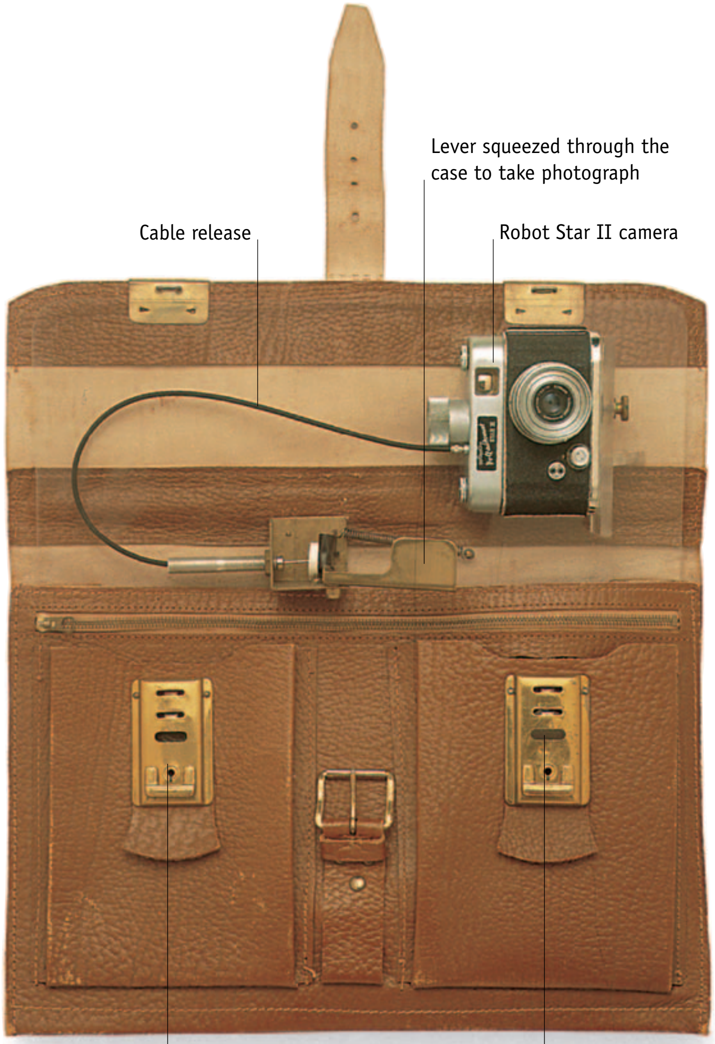
Photo-surveillance briefcase

This briefcase, with its concealed camera, was used during the 1950s and 1960s for photo-surveillance operations by the United States intelligence services. Intelligence officers would carry the briefcase under one arm and take photographs at right angles to the way they were facing. Since the viewfinder could not be used, a great deal of practice was needed to take accurately framed photographs. The officer had to learn instinctively how to position the briefcase correctly in order to photograph the desired subject. The camera is operated by pressing the shutter release lever through the briefcase.

PHILIP AGEE

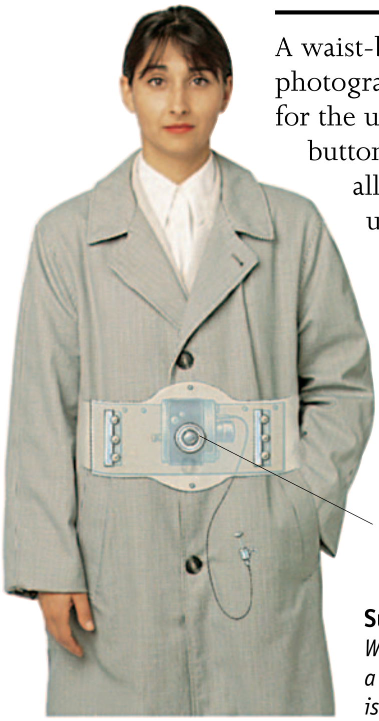
SPY PROFILE

A CIA officer, Agee (1935–2008) resigned in 1968. In a book published in 1975, he exposed the details of every CIA officer he encountered in his 12-year career and falsely identified many State Department officers as working for the CIA. He denied cooperating with hostile agencies, but former KGB officers revealed he had worked with the KGB. Under surveillance after resigning, Agee was secretly photographed by means of a Robot camera hidden in a briefcase. He died in Cuba.

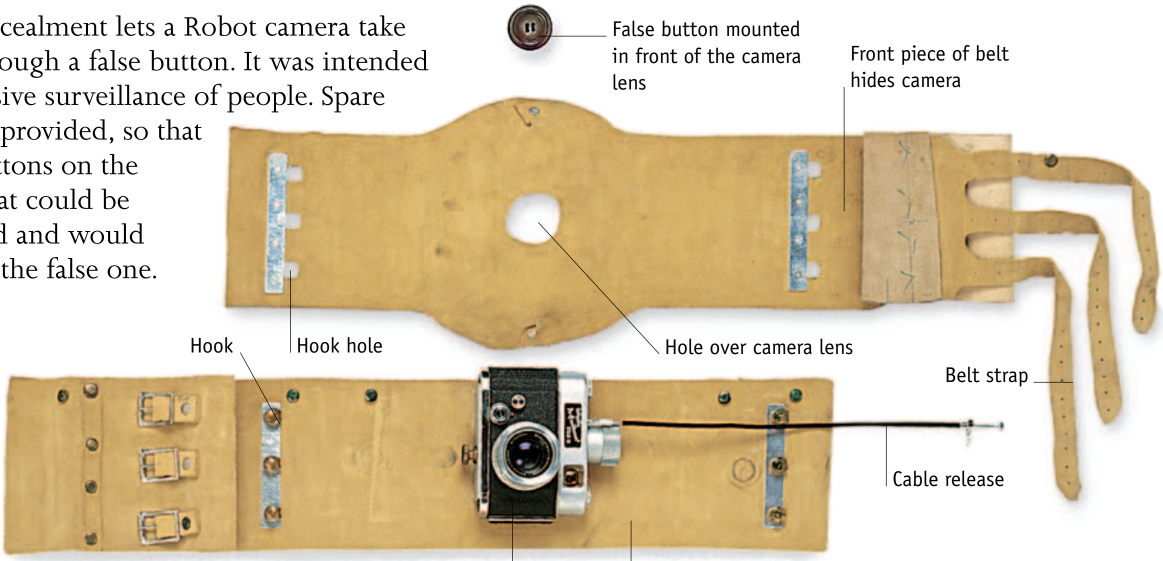

Cable release
Lever squeezed through the case to take photograph
Robot Star II camera
Standard latch
Camera lens takes photograph through latch

Waist-belt surveillance camera

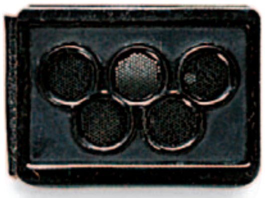
A waist-belt concealment lets a Robot camera take photographs through a false button. It was intended for the unobtrusive surveillance of people. Spare buttons were provided, so that all the buttons on the user's coat could be replaced and would match the false one.



Surveillance camera in position
When the Robot camera is worn on a waist belt hidden under a coat, it is virtually impossible to detect.

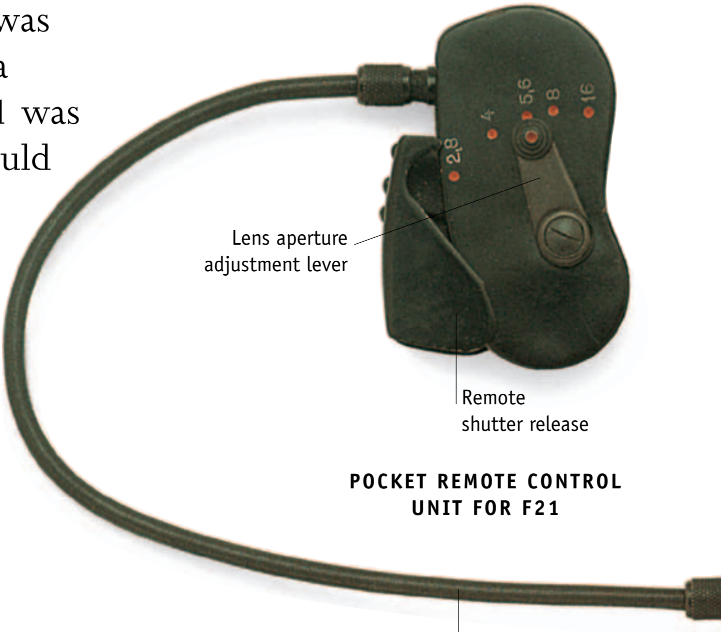

False button mounted in front of the camera lens
Front piece of belt hides camera
Hook
Hook hole
Hole over camera lens
Belt strap
Cable release
Robot Star II camera
Back piece of belt supports camera

F21 concealed camera



BELT BUCKLE CONCEALMENT

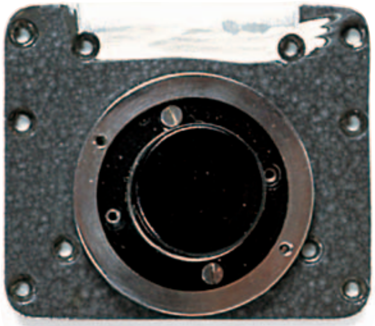
THE SMALL, LIGHTWEIGHT F21 camera was adapted from the German Robot camera (see p. 86) in 1948 by the KGB. The F21 was used for surveillance photography; it could take several pictures in quick succession with a spring-driven winder, and it fitted into many concealments, so spies could use it in a wide variety of different situations. A version of the F21, the Zenit Model MF1, has been sold commercially without concealments since the end of the Cold War.



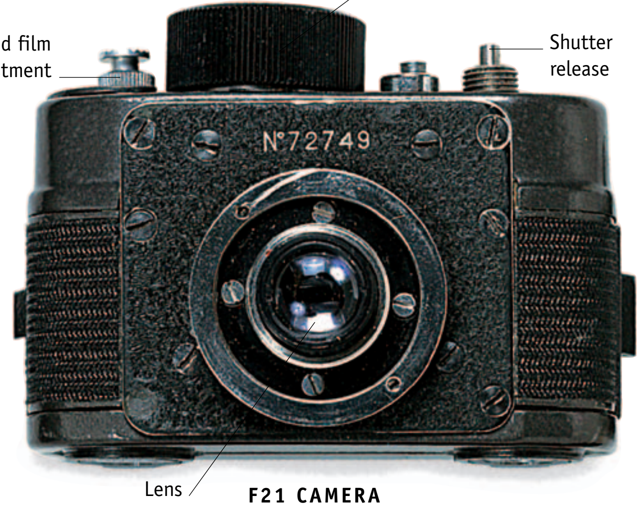
POCKET REMOTE CONTROL UNIT FOR F21

F21 camera and accessories

The F21, with lenses, accessories, and concealments, makes a versatile kit for clandestine photography. Its small size (it is shown here full size) and quietness make it unobtrusive. Because it has no viewfinder, it must be aimed instinctively.



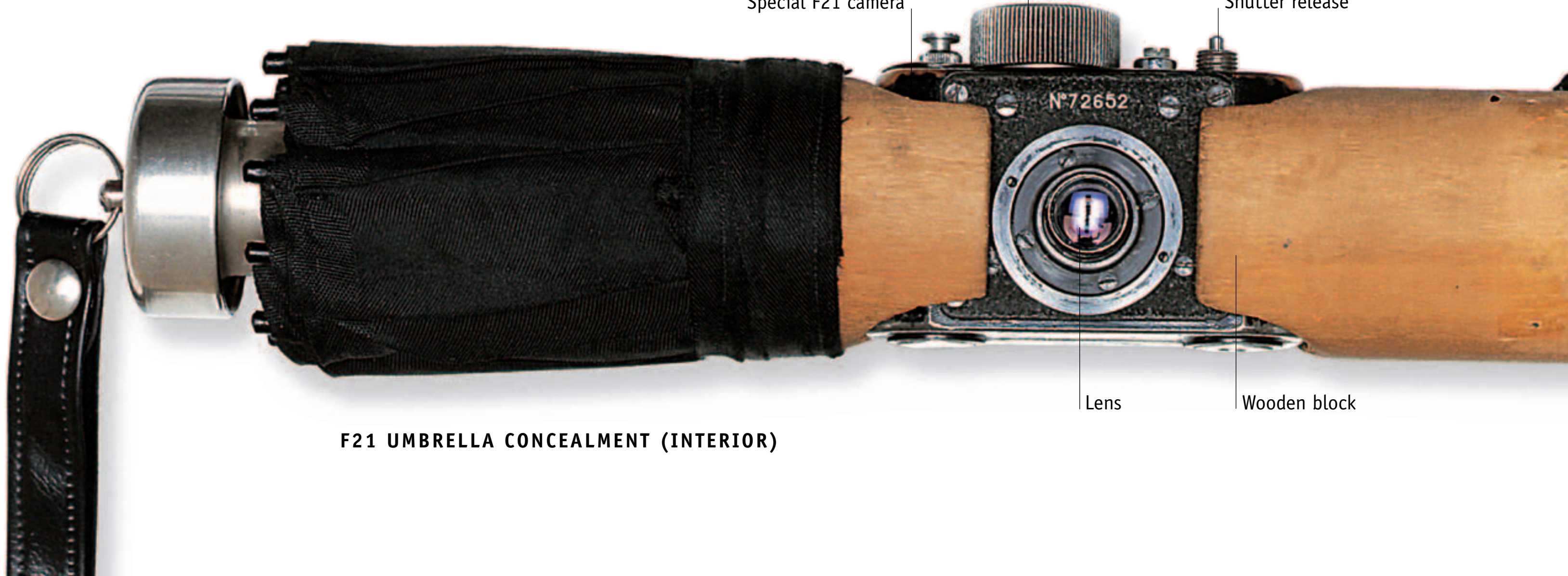
ALTERNATIVE FACEPLATE AND LENS FOR CAMERA



F21 CAMERA

TECHNICAL DATA

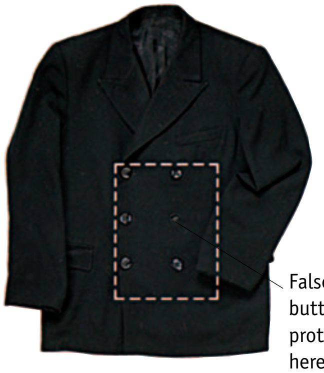
Lens	28 mm f2.8
Focusing range	10 ft (3 m) to infinity
Negative size	About ¾ x 1 in (18 x 24 mm)
Film	Standard issue, 21 mm
Cassette	14–100 frames, depending on thickness of film
Shutter speeds	1/10, 1/30, 1/100 second
Dimensions	3 x 1⅝ x 2⅛ in (77 x 41 x 55 mm)
Weight	6⅜ oz (180 g)
Temperature range	–4 °F to 131 °F (–20 °C to 55 °C)



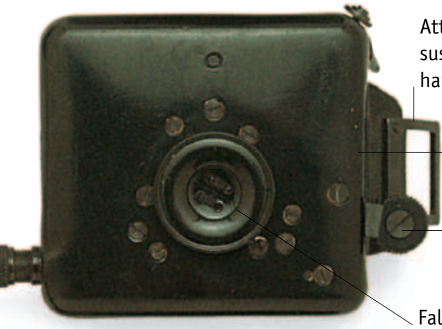
F21 UMBRELLA CONCEALMENT (INTERIOR)

Jacket concealment

The jacket shown here is one of many styles used with the F21 by Soviet intelligence services. A faceplate attached to the F21 carries a false button that covers the lens. The camera is suspended inside the lining, while the false button protrudes through a hole in the front of the jacket. When the remote shutter release—held in a pocket—is gently squeezed, the center of the false button opens briefly to allow a photograph to be taken.



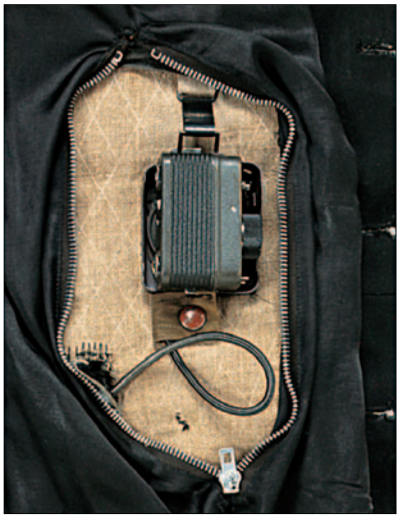
POSITION OF F21 CONCEALMENT



F21 CAMERA WITH FALSE BUTTON FACEPLATE

NORMAL BUTTON

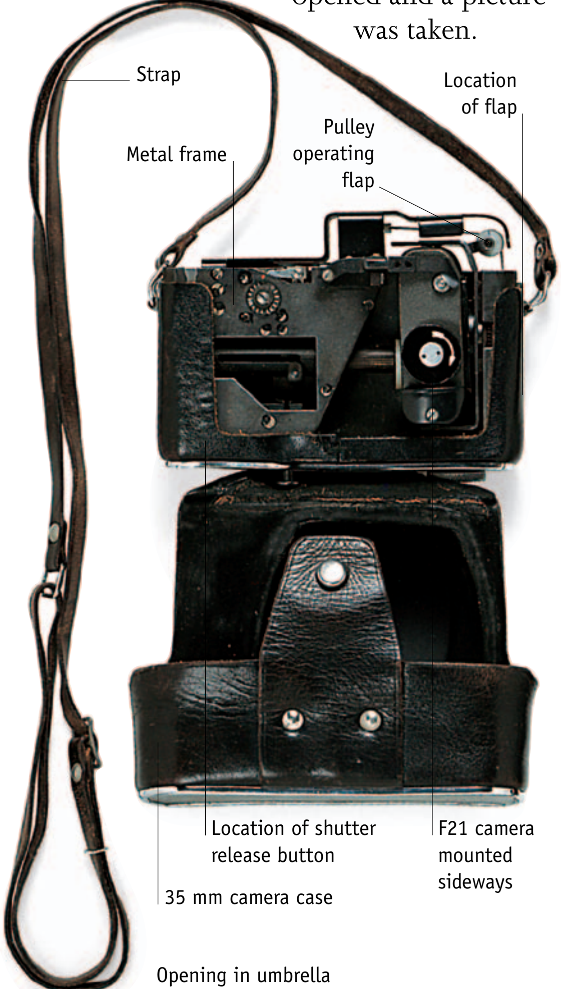
ALTERNATIVE FACING FOR FALSE BUTTON



INSIDE VIEW OF F21 CONCEALMENT

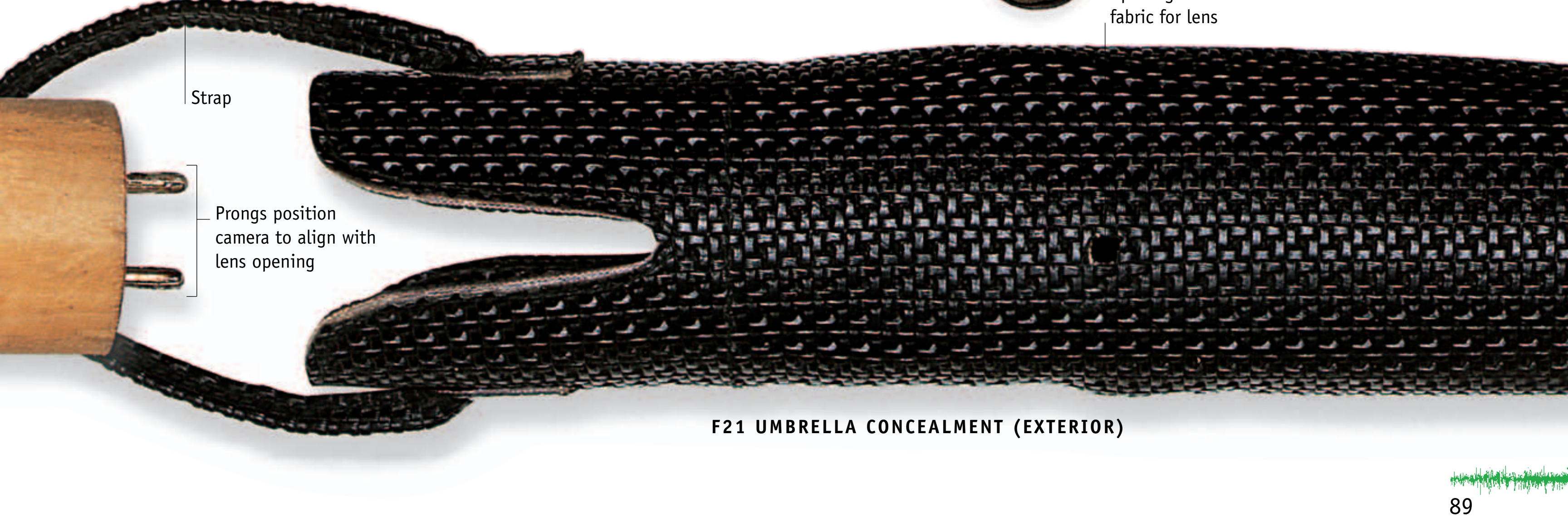
Camera case concealment

A spy would wear this camera case around the neck as though the camera was not being used. But inside, an F21 was mounted sideways to take pictures at right angles to the front of the case. As the spy pressed a button, a flap opened and a picture was taken.



Umbrella concealment

It was possible for a spy to take pictures through a tiny hole in an inconspicuous object such as an ordinary telescopic umbrella without attracting any attention. The F21 camera was mounted in a shaped wooden frame that fitted inside the umbrella, with the camera lens aligned with a hole in the umbrella cover. A spy would carry the umbrella in his hand and take a photograph by pressing the shutter release through the umbrella fabric.


Opening in umbrella fabric for lens
Strap
Prongs position camera to align with lens opening

F21 UMBRELLA CONCEALMENT (EXTERIOR)

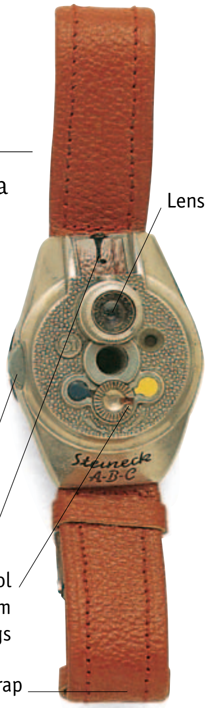
Subminiature cameras I

SUBMINIATURE CAMERAS are a class of pocket-sized cameras that use small film sizes, often 16mm or 9.5mm. They are useful for gathering photographic intelligence, and many are built into an outer casing that disguises the camera as a different object. To ensure that the disguise is effective, certain features of normal cameras, like the viewfinder, may be omitted. Spies may need a considerable amount of training to use subminiature cameras because pictures have to be taken surreptitiously, and often under very difficult circumstances. Intelligence agencies sometimes have subminiature cameras specially made for their own use. On other occasions they use models that are available commercially and are suitable for espionage photography.

WORLD WAR II FRENCH MATCHBOX CAMERA

Wristwatch camera

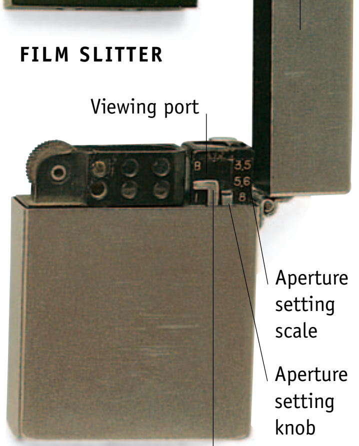
The Steineck ABC camera was made to resemble a wristwatch. It uses a circular piece of film with six exposures. Pictures can be taken while pretending to check the time.


Lens
Shutter release
Right-angle viewfinder
Aperture setting control with bright (yellow) and dim (blue) light settings
Wrist strap

Cigarette lighter camera

Designed in Japan in 1951, the Echo 8 cigarette lighter camera was once the smallest commercially available camera in the world. It was housed inside a working cigarette lighter. This concealment made it ideal for use in social or business settings, where a cigarette lighter would not attract attention. To use the camera, the spy just needed to flip up the top and light a cigarette while aiming the camera at the subject.

FILM SLITTER

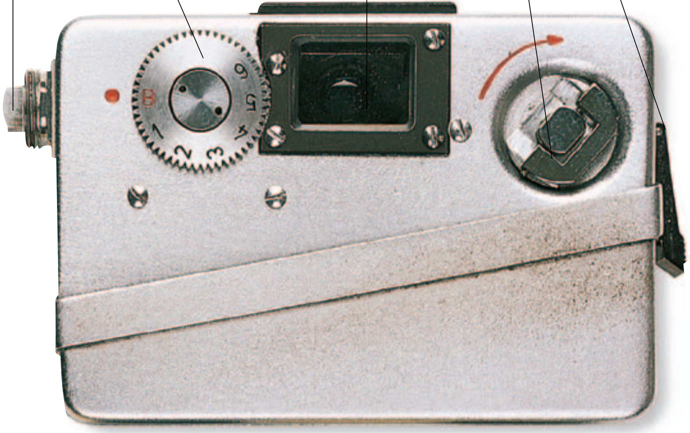


CIGARETTE LIGHTER CAMERA

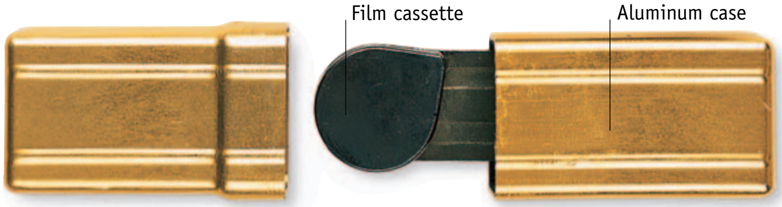
How the camera was used
This picture is from a contemporary instruction manual. The lens, shown as a dot, has been made more clearly visible for instruction purposes.

Milox TI-246 camera

The Milox camera was first produced in 1968 at the Meopta camera works in Prerov, which is now in the Czech Republic, and used for surveillance photography. The unique optical design of this thin camera allowed it to be used in a variety of concealments, such as a small handbag.



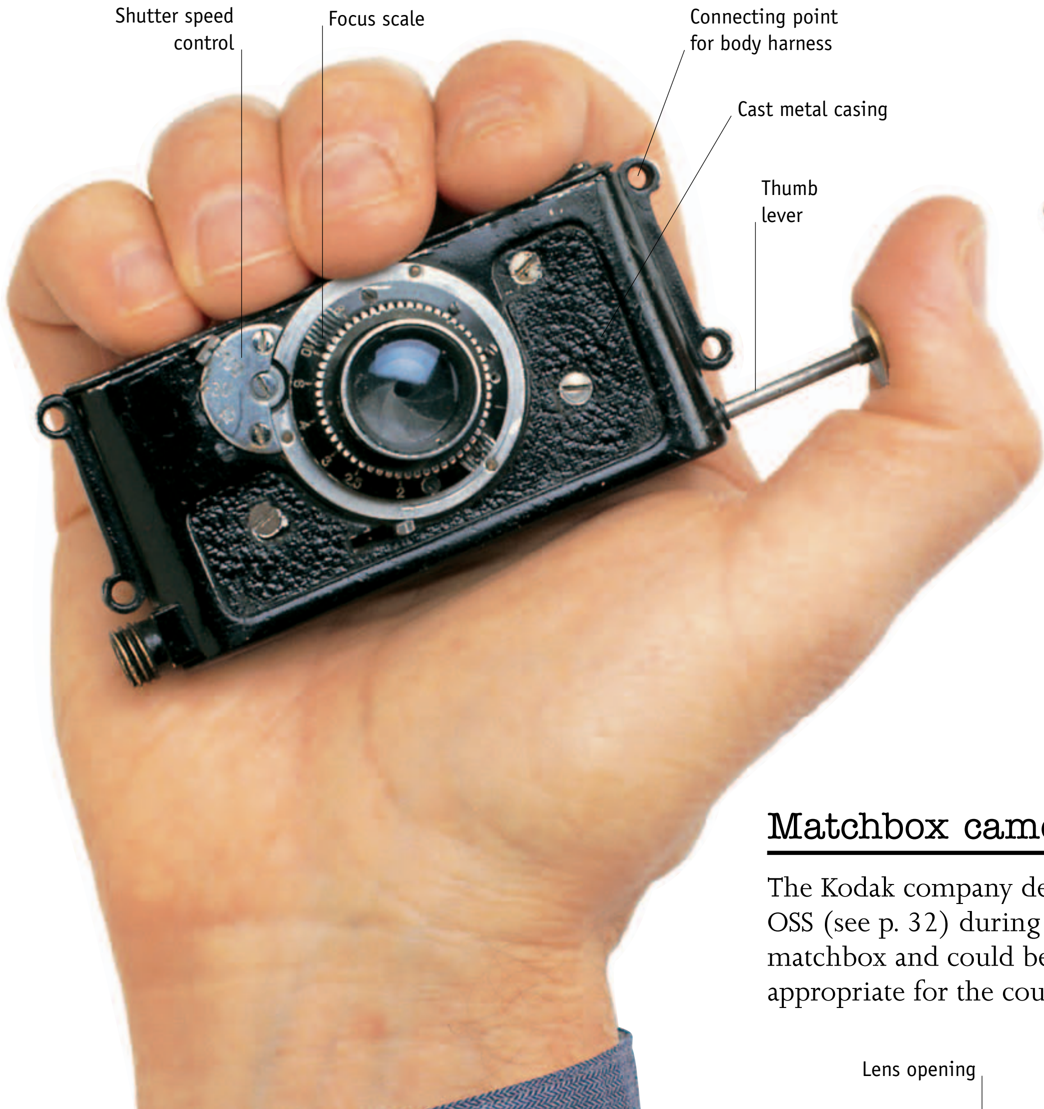
CAMERA



FILM CASSETTE IN CASE

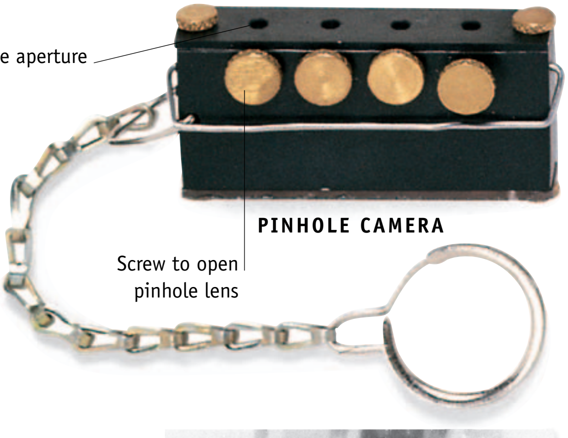
Ajax-8 surveillance camera

This KGB surveillance camera was used from 1949 up until the 1980s. It was designed to be aimed instinctively while concealed in the hand. It could also be worn flat against the body in a body harness, enabling photographs to be taken through a fake button or brooch. The shutter is released and the film is advanced when the thumb lever is pressed.



Pinhole camera

This tiny KGB camera (shown actual size) from the 1980s utilizes a 19th-century photographic principle: each of its four chambers has a pinhole aperture for a lens, making it possible to photograph close-up and distant objects without focusing.



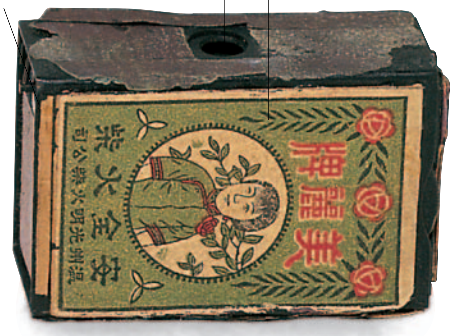
PINHOLE CAMERA

KGB TEST PHOTOGRAPH TAKEN WITH A PINHOLE CAMERA

Matchbox camera

The Kodak company developed this 16mm camera for use by the OSS (see p. 32) during World War II. It was made in the shape of a matchbox and could be camouflaged by adding a matchbox label appropriate for the country in which it was to be used.

CAMERA

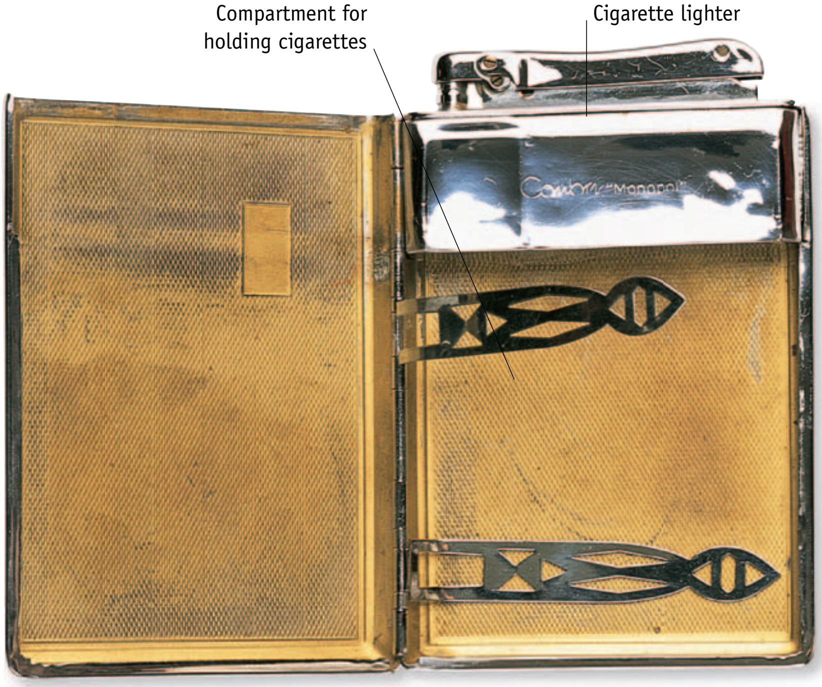


CAMERA WITH MATCHBOX LABEL

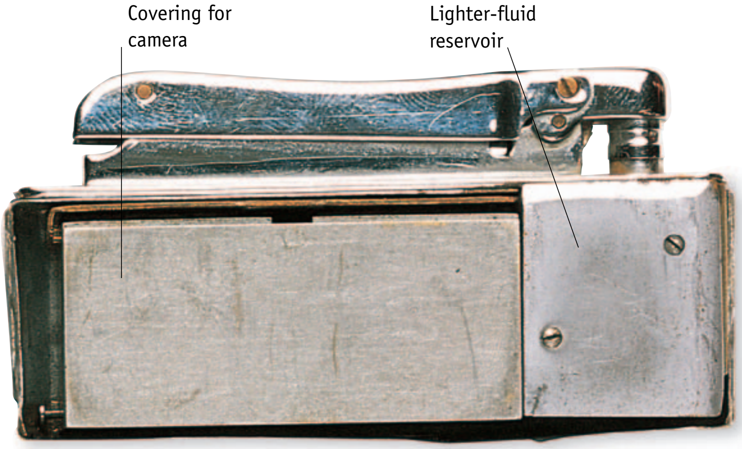
Subminiature cameras II

Cigarette-case-and-lighter camera

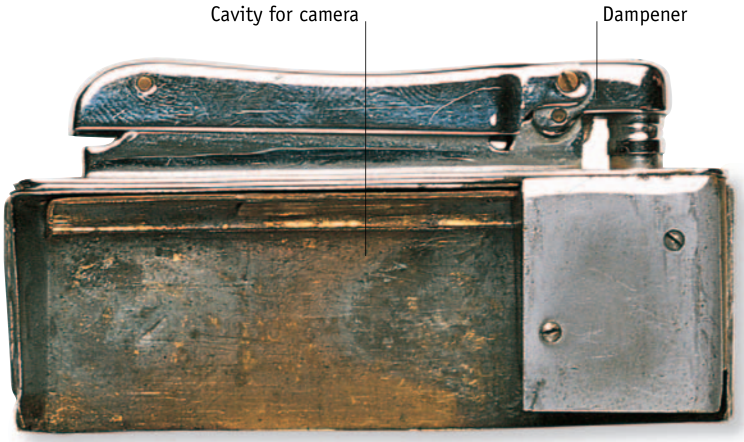
A German document camera from the 1950s and 1960s is concealed here inside a European-style combination cigarette case and lighter. The small camera uses a Minox-format cassette. When hidden in the lighter, the camera could be carried through a security checkpoint without being detected. Specialized cameras in concealments such this were made in small numbers exclusively for intelligence services.



CIGARETTE HOLDER AND LIGHTER



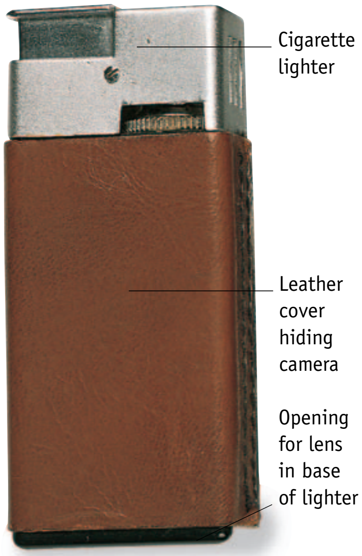
CAMERA CONCEALED IN LIGHTER

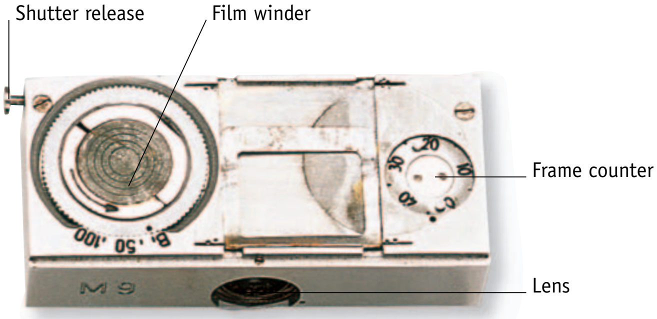


LIGHTER WITHOUT CAMERA

Svouk lighter camera

Produced in the 1970s, this precision working cigarette-lighter camera had its own special 6mm film. The camera was used for photographing documents through a pinhole opening in its base. The camera was one of three in the Svouk series, which were designed by the KGB's 11th Optical Laboratory in Moscow.


Cigarette lighter
Leather cover hiding camera
Opening for lens in base of lighter

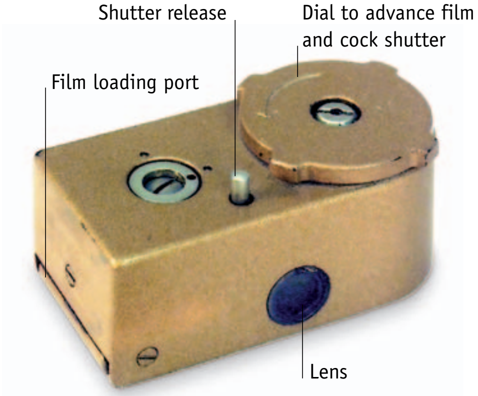


CAMERA

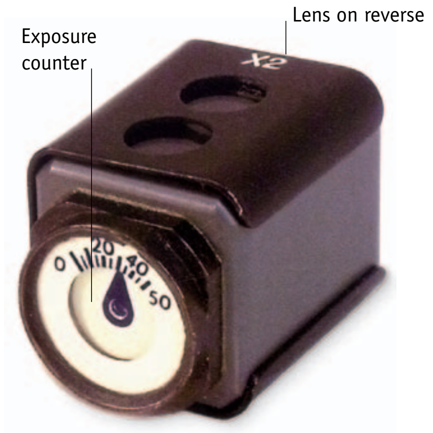
COVERING FOR CAMERA

CIA subminiature cameras

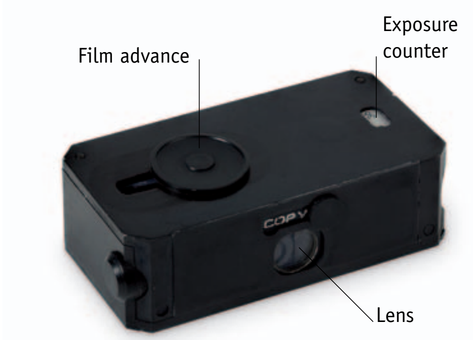
After the arrest of CIA mole Oleg Penkovsky in Moscow in 1962 (see p. 106), the CIA realized its agents did not have the specialized equipment that they needed in the Soviet Union. Available subminiature cameras had been designed decades earlier—and not for secretly photographing documents. The first subminiature cameras made by the CIA, in the 1960s and 1970s, still used the Minox film format, but were smaller and easier to conceal.



DCD-1 (1965)



WRAL (1970)

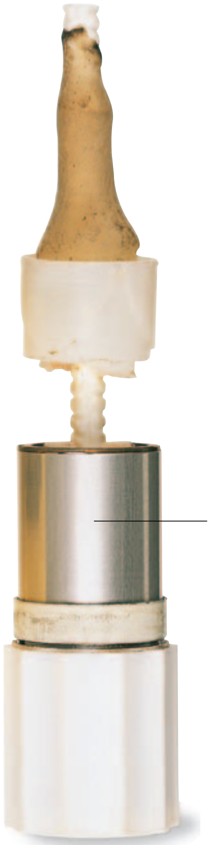


MOLLY (1971)

Zvouk glue-stick camera

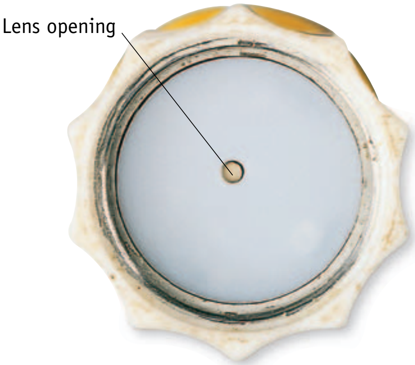
This KGB glue stick (which is now dried out) conceals a Zvouk copy camera in its base. Photographs were taken by lifting the camera 12½ in (30 cm) above a document and, while holding the stick's base, rotating the body a quarter-turn. The camera could photograph 30 documents onto a cassette loaded with black-and-white 6mm film.

GLUE STICK

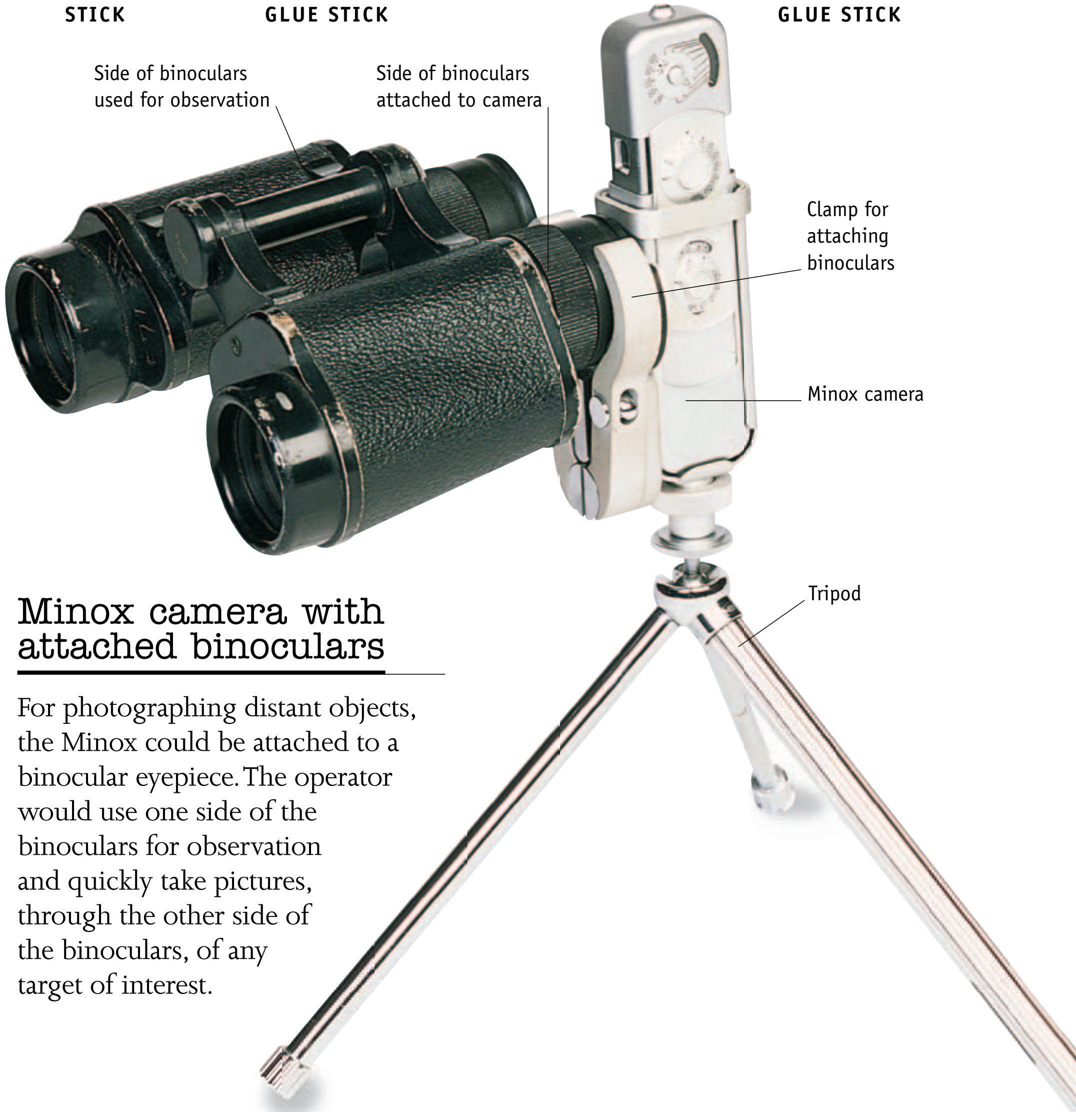


CAMERA IN GLUE STICK

FILM CASSETTE



BASE OF GLUE STICK


Side of binoculars used for observation
Side of binoculars attached to camera
Clamp for attaching binoculars
Minox camera
Tripod

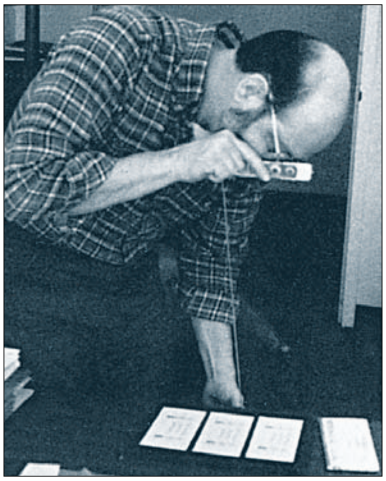
Minox camera with attached binoculars

For photographing distant objects, the Minox could be attached to a binocular eyepiece. The operator would use one side of the binoculars for observation and quickly take pictures, through the other side of the binoculars, of any target of interest.

Minox camera

EARLY FILM CASSETTE CASE

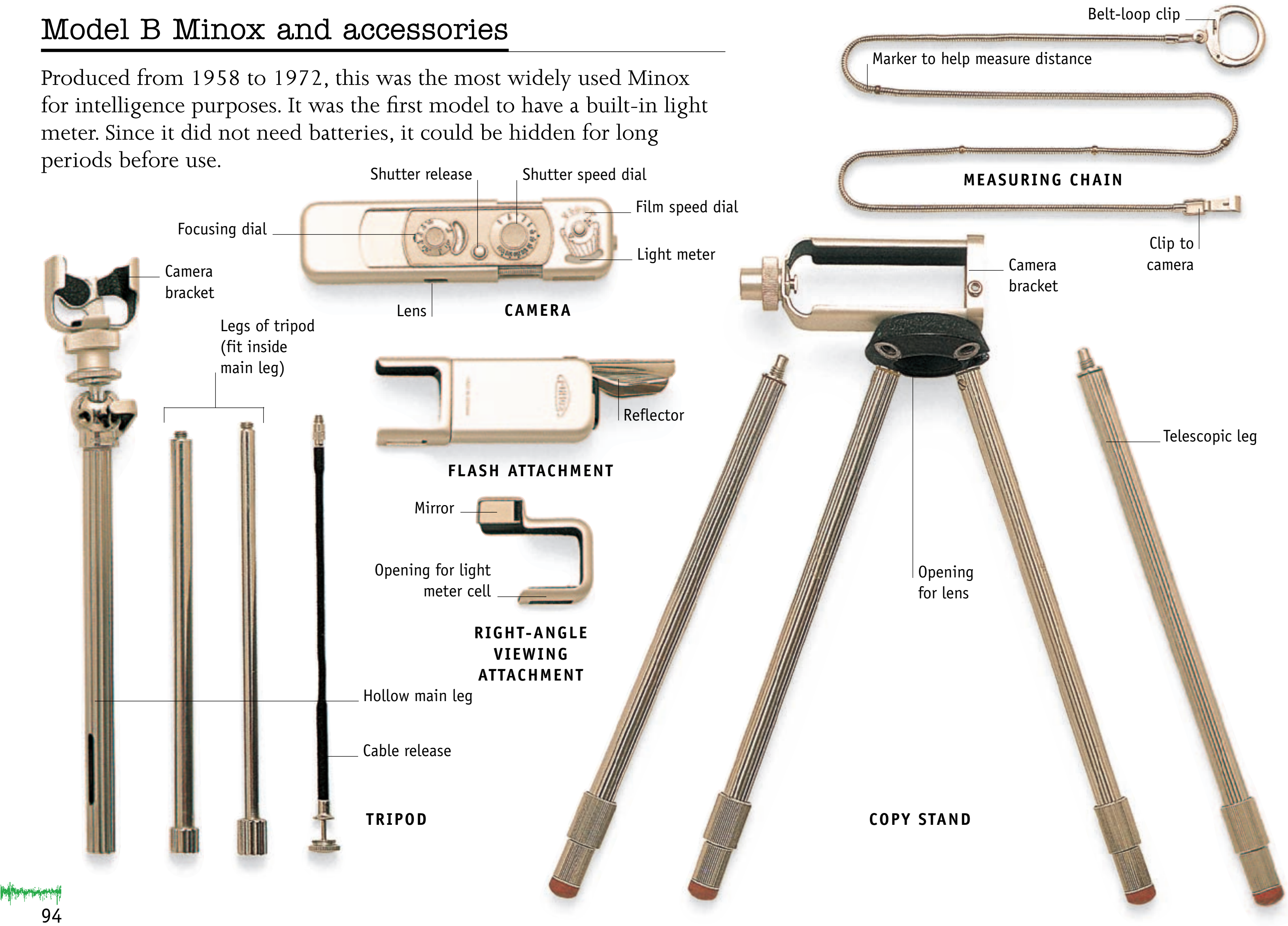
THE MINOX SUBMINIATURE CAMERA was for years the world's most widely used spy camera. It was originally manufactured—in Latvia, in 1938—as a commercial camera, but intelligence agencies soon realized that its small size, precision, and flexibility made it ideal for clandestine photography. It is suitable both for general use and for close-up work, such as taking photographs of documents, and can take 50 pictures without reloading. The more advanced models produced after World War II were equipped with very high resolution lenses that, when used with better-quality film, allowed a tremendous amount of detail to be obtained from the tiny negatives. And with its many accessories, the Minox could be adapted for a wide range of intelligence uses. The CIA moved away from it in the 1970s, but the Russians carried on using it until the late 1990s.



Demonstrating the Minox
American KGB spy John Walker (see p. 54), following his arrest, shows how he used his Minox C camera with its measuring chain.

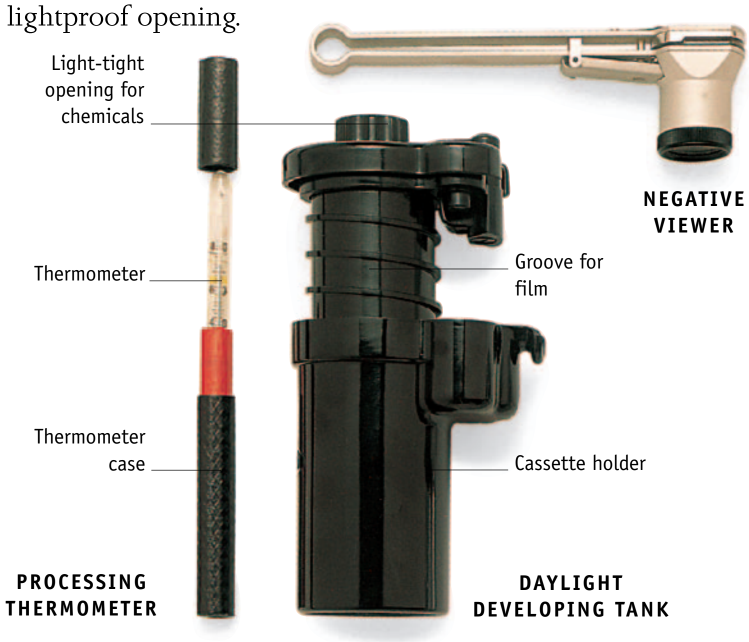
Model B Minox and accessories

Produced from 1958 to 1972, this was the most widely used Minox for intelligence purposes. It was the first model to have a built-in light meter. Since it did not need batteries, it could be hidden for long periods before use.



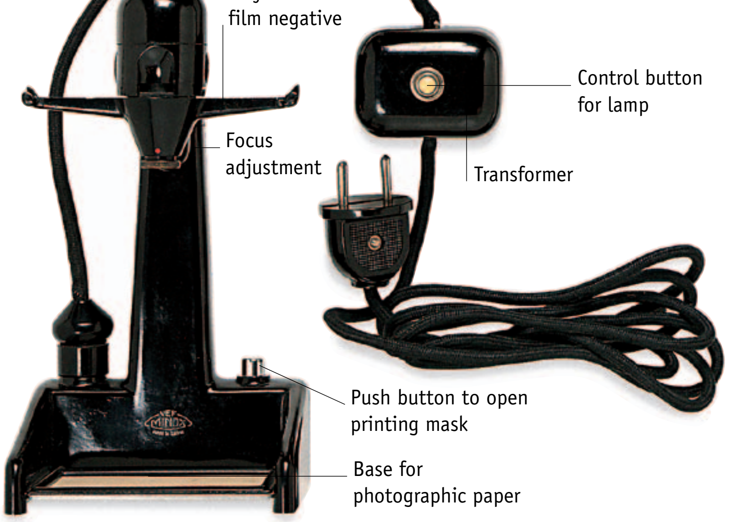
Daylight developing kit

With Minox's miniature developing tank, spies could process their film in full daylight. The tank is the size of a small soda can and uses tiny quantities of chemicals, poured in through a lightproof opening.



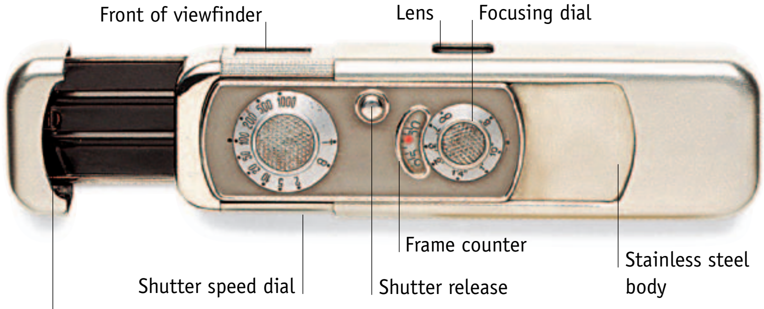
Riga Minox enlarger

Early Minox enlargers were designed to produce small prints from the tiny negatives. Since World War II, improved enlargers have been developed, which make bigger prints from the higher resolution film now available.



Riga Minox camera

The original Minox camera was seen as a marvel of technology when it first became available. During World War II, intelligence agencies found it difficult to acquire enough Minox cameras for their espionage activities in German-occupied Europe.



TECHNICAL DATA

Lens	Minastigmat five element
Maximum aperture	f3.5
Focal length	About ⅝ in (15 mm)
Negative size	About 5⁄16 x ⅜ in (8.5 x 10 mm)
Film	Unperforated 9.5mm film; 50 exposures
Shutter speeds	½ to 1⁄1000 second
Focusing range	8 in (20 cm) to infinity
Dimensions	3⅛ x 1 1⁄16 x ⅗ in (79 x 27 x 15 mm)
Weight	4½ oz (128 g)

THE MINOX INVENTOR

Latvian engineer Walter Zapp (1905–2003) wanted to create a portable camera that would fit easily in the palm of the hand yet take high-quality pictures. In the 1930s he developed a mechanism that met these strict requirements. The first Minox camera used a 50-frame film one-quarter the size of standard 35mm film. This and later models had a reputation for extraordinary durability and reliability. KGB spy John Walker is the only agent ever known to have worn out the shutter of a Minox camera. After his arrest, the FBI ran tests and found that a Minox could take no fewer than 250,000 exposures before its shutter finally failed.

Early Minox design team
The 1937 design team that produced the first Riga Minox, with Walter Zapp in the center.

T-100 camera

DUBBED THE CAMERA THAT WON THE COLD WAR, the CIA's tiny T-100 subminiature camera was developed in the early 1970s for agent use inside the Soviet Union's most heavily guarded areas, including the KGB's own *rezidentura*, the spy base in each Soviet foreign embassy. Its design was conceived by the CIA's Office of Technical Service (OTS), which specializes in technical support for agent operations, and it had to meet seemingly impossible needs: be small enough to be easily concealed, yet take 100 distortion-free, high-resolution images of letter-size pages of text, silently, without a flash.

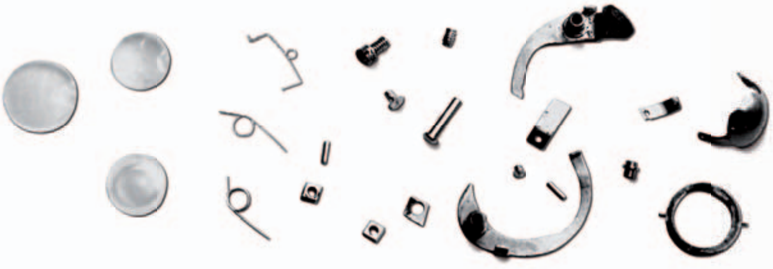
TECHNICAL DATA

First manufactured	mid-1970s
Dimensions (key fob concealment)	1½ x ⅜ in (38 x 9 mm)
Lens diameter	4 mm
Film size	⅕ x 15 in (5 x 380 mm), unperforated, 100 exposures
Negative size	4 x 4 mm
Focusing range	11 in (280 mm) fixed
Depth of field	Approximately 1 in (25 mm)
Document size	8½ x 11 in (215 x 280 mm)
Weight	Variable, according to concealment

OTS commemorative concealment
Experts in all areas of spy gadgetry, the OTS created this special concealment coin in 2001 to commemorate 50 years of support to CIA technical operations.

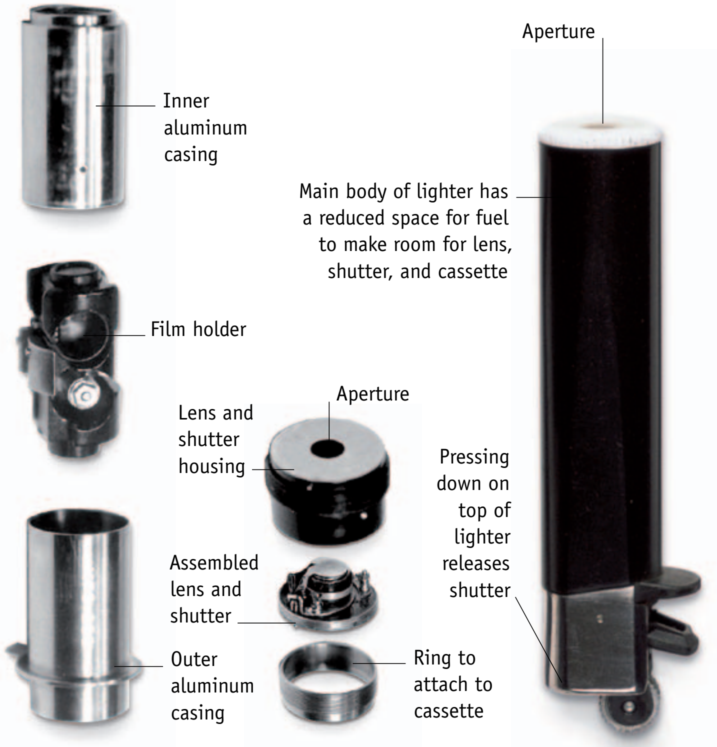
T-100 lens and shutter assembly

The T-100's minute lens was made from eight precision-ground glass elements, the smallest only slightly larger than a pinhead, stacked one on top of another. Its design was so specialized that it had no other use than covert photography. The owner of the company that made T-100 cameras for the OTS hand-assembled the numerous tiny lens and shutter components (below) for each camera with all the skill of a watchmaker.



T-100 cassettes and concealments

The OTS used ultra-thin, light, high-resolution document copy film made by Kodak for the US satellite program. In total darkness officers cut it into long, thin strips and loaded these on to holders in cassettes for supply to agents in the field. An agent had a working lighter, fountain pen (see p. 61), or key fob concealment with a lens and shutter inside—making a camera that was one sixth the size of a Minox (see p. 94).


Inner aluminum casing
Film holder
Outer aluminum casing
Lens and shutter housing
Aperture
Assembled lens and shutter
Ring to attach to cassette
Aperture
Main body of lighter has a reduced space for fuel to make room for lens, shutter, and cassette
Pressing down on top of lighter releases shutter

FILM CASSETTE ASSEMBLY

LENS AND SHUTTER

LIGHTER CONCEALMENT

EDWARD LEE HOWARD

SPY PROFILE

Howard (b.1951) joined the CIA in 1980 and trained as a case officer to conduct agent operations in Moscow. His training included a full briefing on the T-100. Just before leaving for Moscow in 1983 he was dismissed after failing a polygraph test about past drug use. Disaffected, he began supplying CIA secrets to the KGB, including all he knew about the T-100. Exposed as a spy in 1985, he fled to Moscow, where he died in 2002 after "falling" down a flight of stairs.

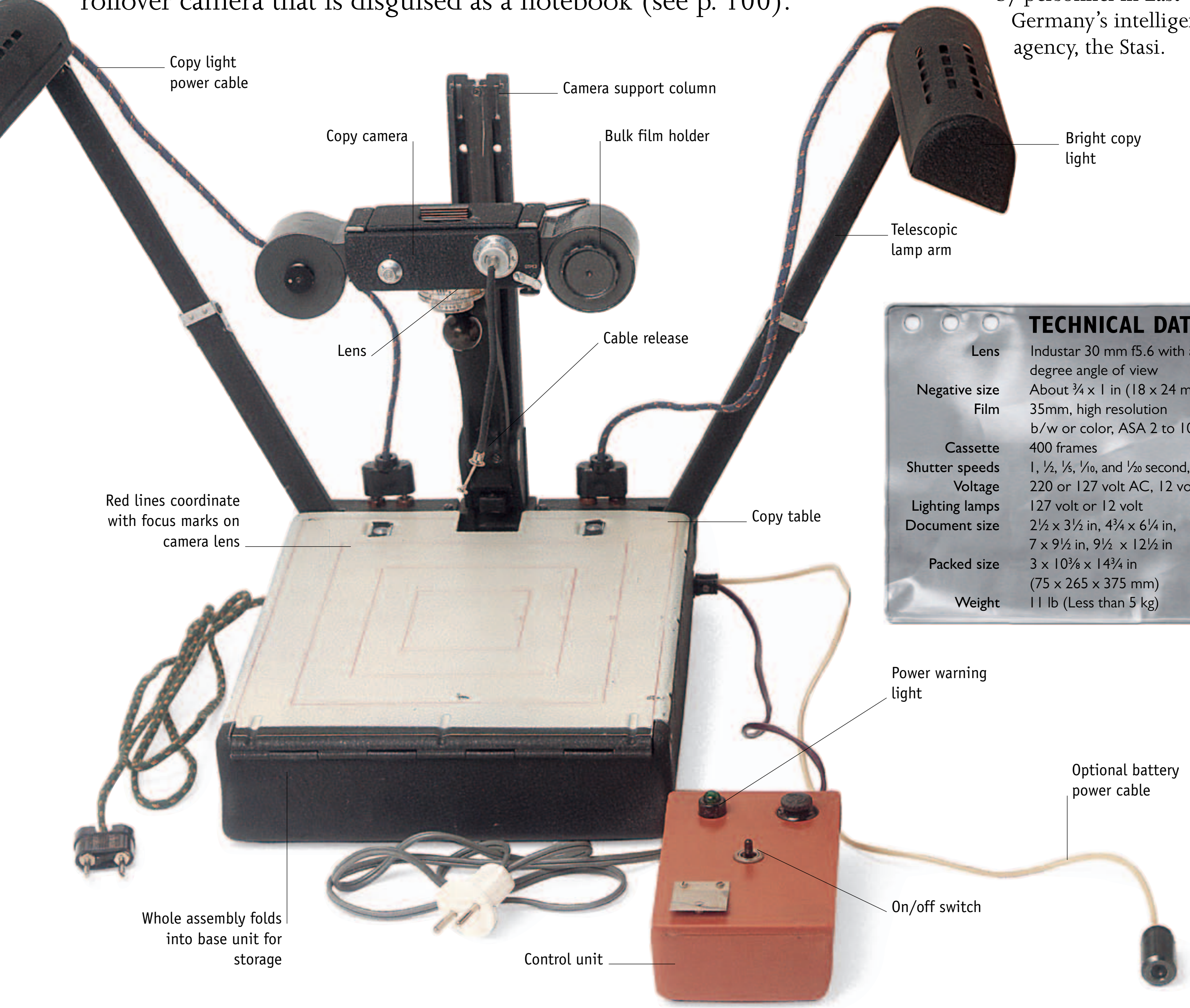
“*This page left intentionally blank.*”

Copy cameras I

SPIES OFTEN HAVE just a few moments in which to copy secret documents. They may have stolen the documents and need to replace them before the documents are missed, or they may have access to them in an office that is empty only for short periods. Normal cameras can be used for document photography but they require care and time to take good-quality pictures. Intelligence services have developed special portable copy cameras that are quick, easy, and reliable to use. Copy cameras can be either miniaturized or disguised: a fine example of the latter is the KGB rollover camera that is disguised as a notebook (see p. 100).

Yelka C-64 copy camera

This equipment was designed for the KGB and operates on a wide range of electrical voltages, including that of car batteries. It is simple to use and produces good pictures. The Yelka was built with hinges that enabled it to be folded down when not in use. The whole unit, when folded, fits inside its own base (its copy stand), which is about the size of a large book. The example shown here was used by personnel in East Germany's intelligence agency, the Stasi.



TECHNICAL DATA

Lens	Industar 30 mm f5.6 with a 50 degree angle of view
Negative size	About ¾ x 1 in (18 x 24 mm)
Film	35mm, high resolution b/w or color, ASA 2 to 100
Cassette	400 frames
Shutter speeds	1, ½, ⅕, ⅒, and 1⁄20 second, plus bulb
Voltage	220 or 127 volt AC, 12 volt DC
Lighting lamps	127 volt or 12 volt
Document size	2½ x 3½ in, 4¾ x 6¼ in, 7 x 9½ in, 9½ x 12½ in
Packed size	3 x 10⅜ x 14¾ in (75 x 265 x 375 mm)
Weight	11 lb (Less than 5 kg)

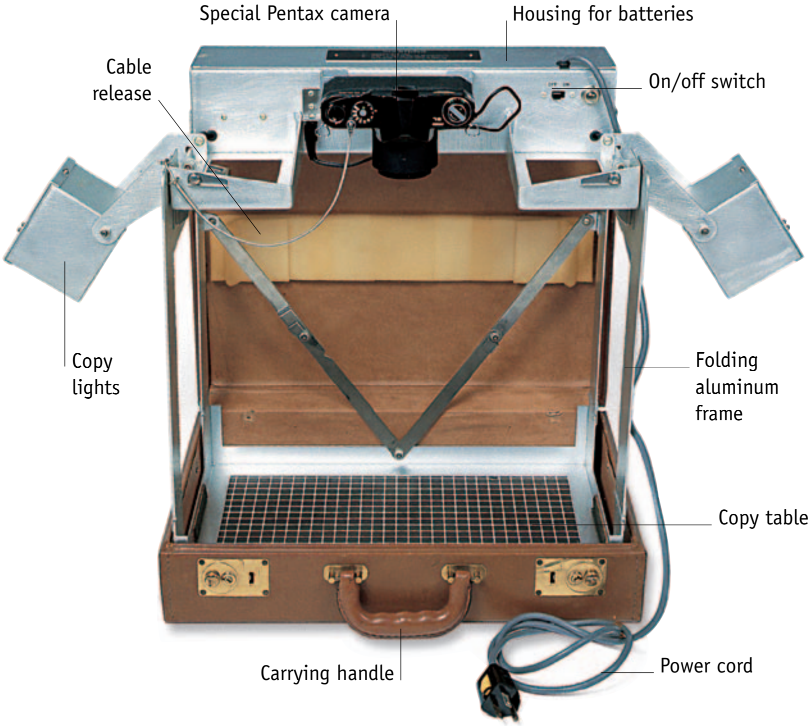
DAS MINISTERIUM FÜR STAATSSICHERHEIT

East Germany's State Security Ministry was usually known as the Stasi – short for its official German title (above). In effectiveness, it was second only to the KGB among Soviet bloc intelligence organizations. The Stasi's principal responsibility was to monitor the activities of East Germany's own citizens. After the collapse of East Germany in 1989, the German public was astonished to learn the extent of surveillance that had been going on in their midst.

Stasi lapel pin
Stasi officers watching a public meeting or demonstration wore lapel pins to identify themselves to each other and to informers. This Stasi pin, shown twice real size, has a revolving disk that can display four different identifying colors.

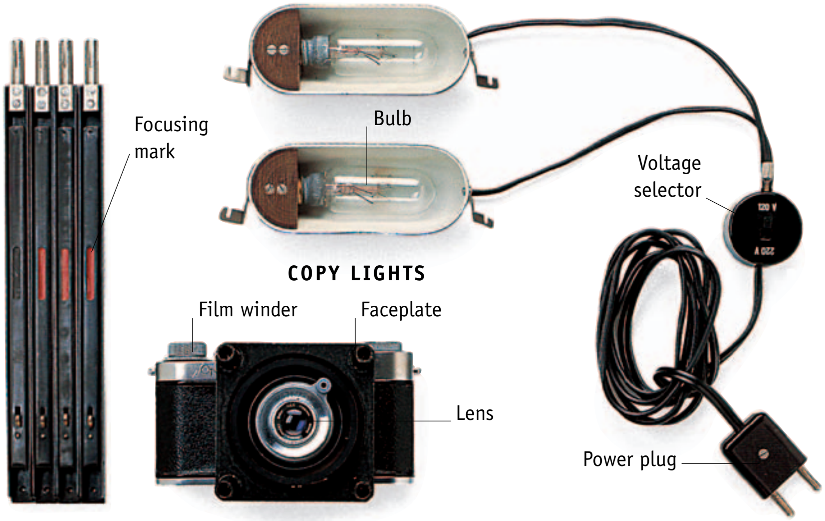
Attaché case copy camera

An attaché case forms the concealment for this American copy camera. When the case is opened, the copy lights fold out into position and operate with either electricity or batteries. The modified fixed-focus 35mm camera uses nylon gears for silent operation. This type of attaché case copy camera has been used by a variety of American intelligence organizations.



Copy camera kit

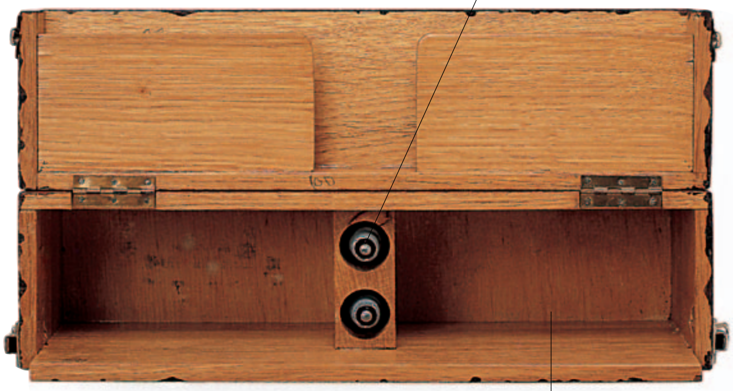
The components of this copy camera kit, designed for the Czech intelligence service (known by its Czech initials StB), could be quickly assembled from the small case in which they were usually carried. Colored marks on the legs correspond to focus settings on the camera.



COPY LIGHTS

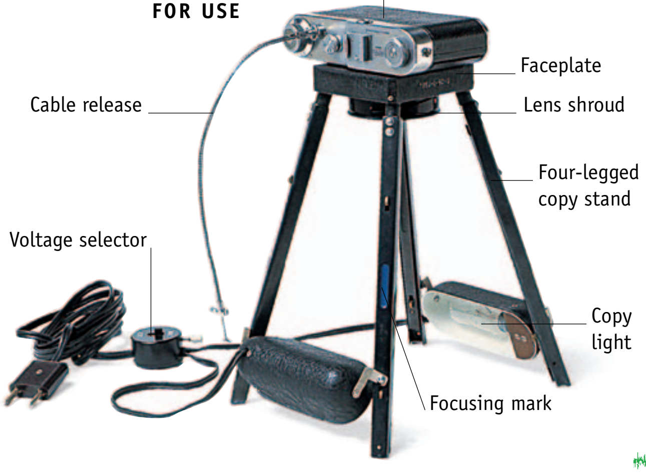
LEGS OF STAND

MEOPTA COPY CAMERA



EMPTY CASE FOR CAMERA KIT

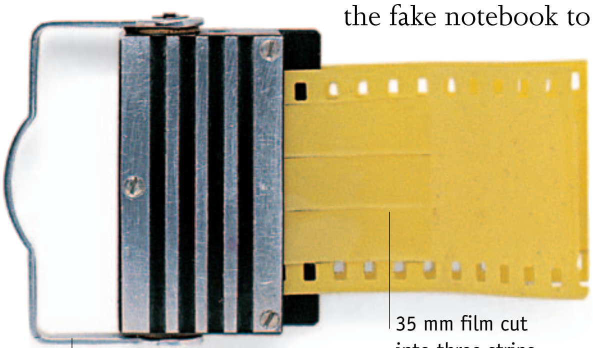
CAMERA SET UP FOR USE



Copy cameras II

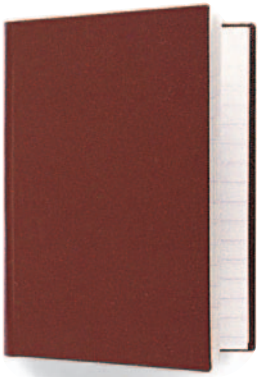
ALYCHA KGB rollover camera

This rollover or brush camera can copy up to 40 pages before it needs reloading. The camera is concealed in a fake notebook resembling a real one that the spy carries and uses regularly. To use the camera, the spy folds back the cover of the fake notebook to reveal a lens in the inner spine. Tiny wheels in the spine activate the camera mechanism and its built-in light source as the spine is rolled over a document.


Handle is raised to allow film to be fed into the slitter
35 mm film cut into three strips

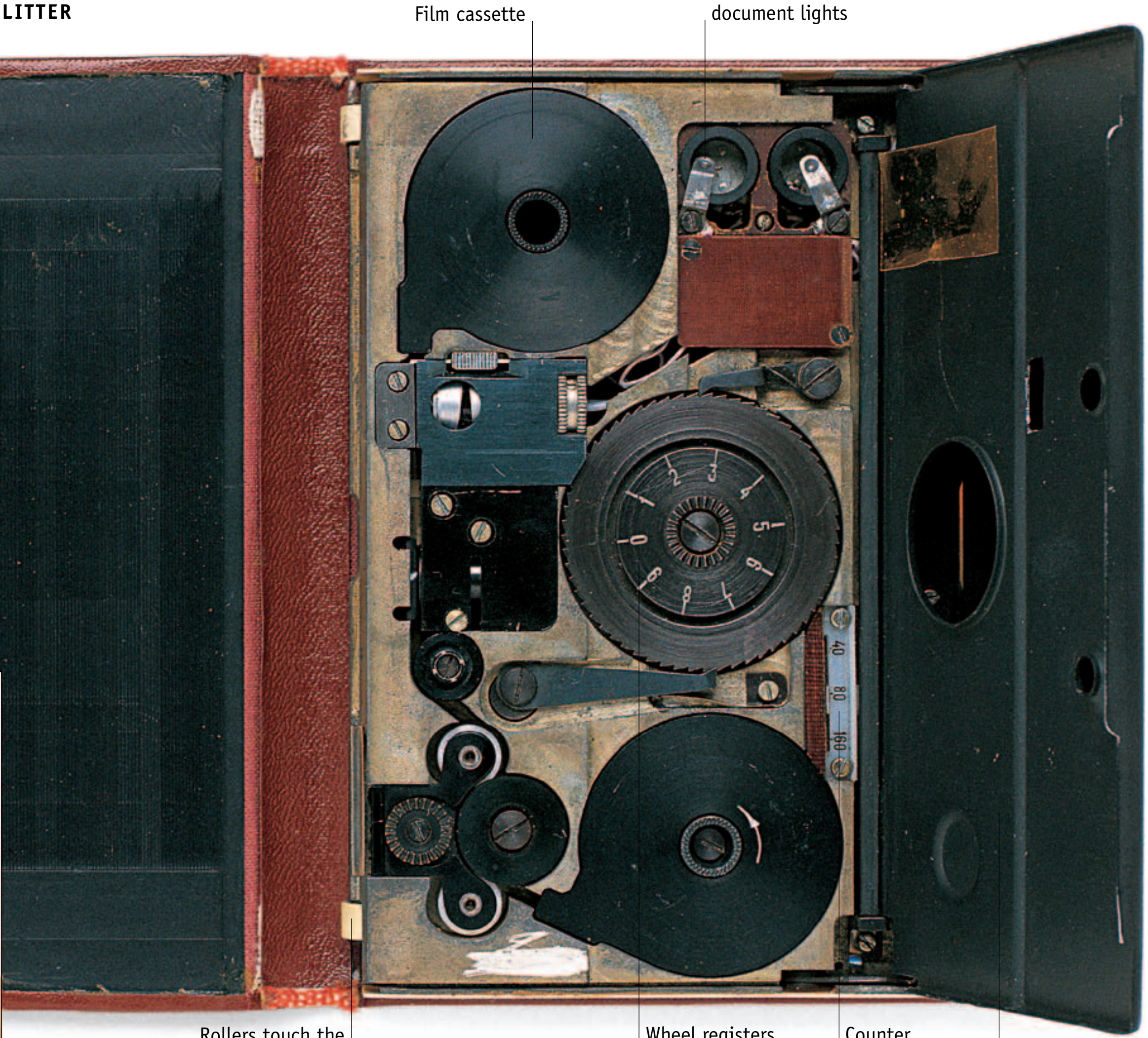
FILM SLITTER

Film slitter
The slitter cuts standard 35mm film into three strips of the correct width for use in the cassette of the rollover camera.

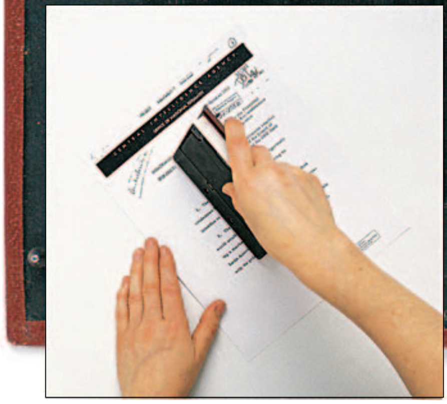


REAL NOTEBOOK

ROLLOVER CAMERA DISGUISED AS NOTEBOOK


Film cassette
Batteries for document lights
Rollers touch the document
Wheel registers film position
Counter
Hinged cover
40
80
160

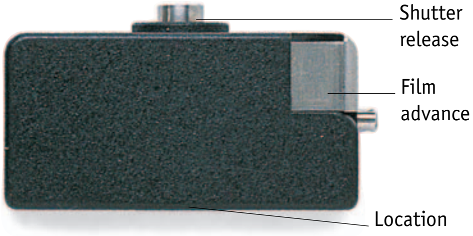
MECHANISM OF THE ROLLOVER CAMERA



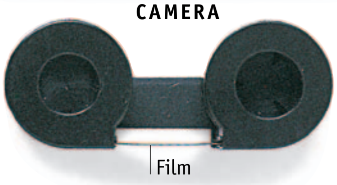
Rollover photography
The KGB camera being rolled over a document to copy it. The camera can cross the page in any direction.

ZODCHI KGB document camera

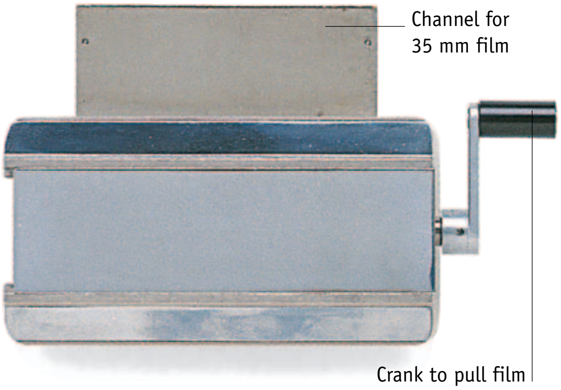
Shown actual size, this small camera was intended for use in facilities where strict security is maintained. It has no viewfinder and few external controls—just a shutter release and film advance. A film slitter cuts standard 35mm film down to a width of 9.5 mm for use in a Minox (see p. 94) cassette.



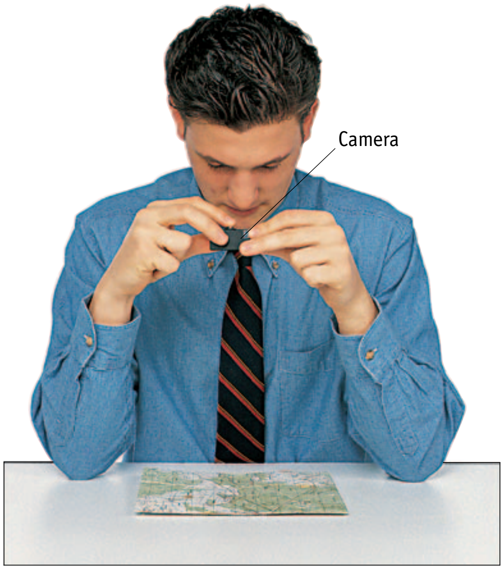
CAMERA



FILM CASSETTE



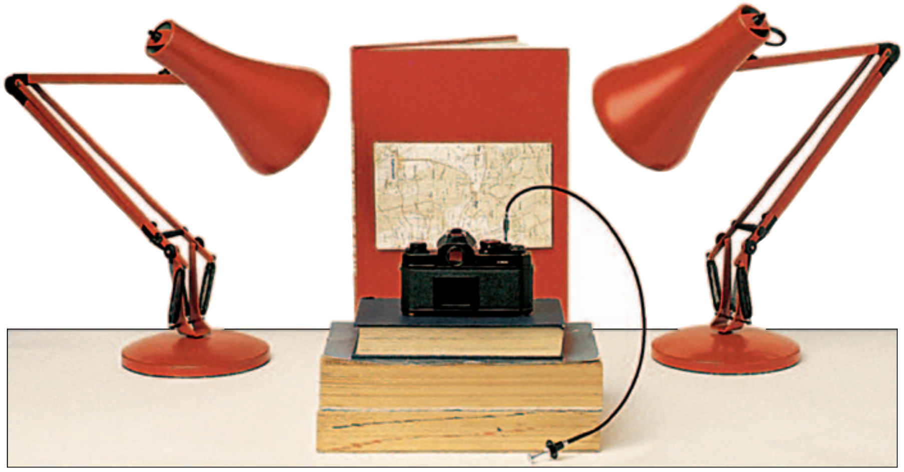
FILM SLITTER



Using the document camera
The camera has a fixed focus, so in order to take clear photographs it must be held as shown, at a specific distance from the document. A constant light should be directed on the document.

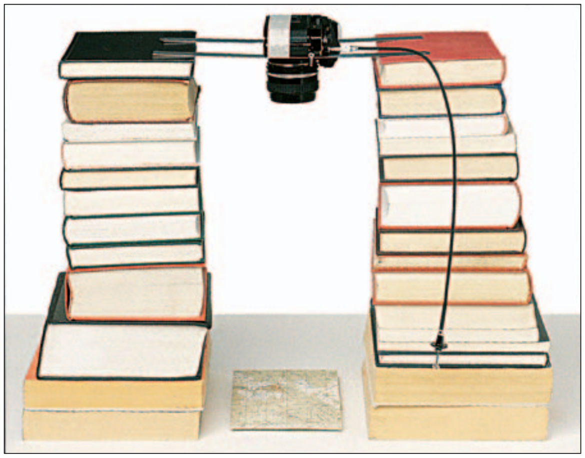
Improvised copy techniques

Agents are trained to improvise copy setups so that they can obtain good copies even in circumstances in which time or equipment are limited. Because they consist of ordinary office equipment, these setups do not attract suspicion when dismantled.

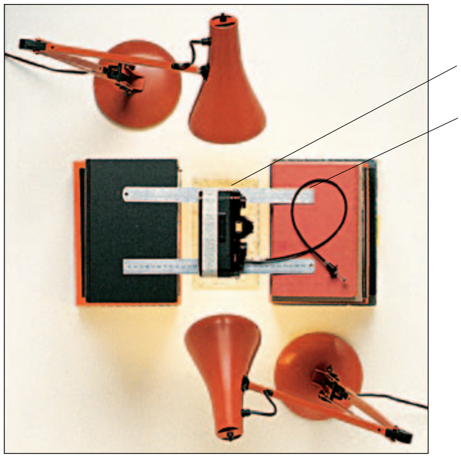


SIMPLE COPY SET-UP

Simple copy technique
This technique was developed by Victor Ostrovsky (see p. 80) for Mossad. The document, taped to a book, is stood in front of the camera, which is stuck to another book with chewing gum. Desk lamps are used for illumination. A remote shutter release is used to avoid shaking the camera.



HIGH-VOLUME COPYING: SIDE VIEW



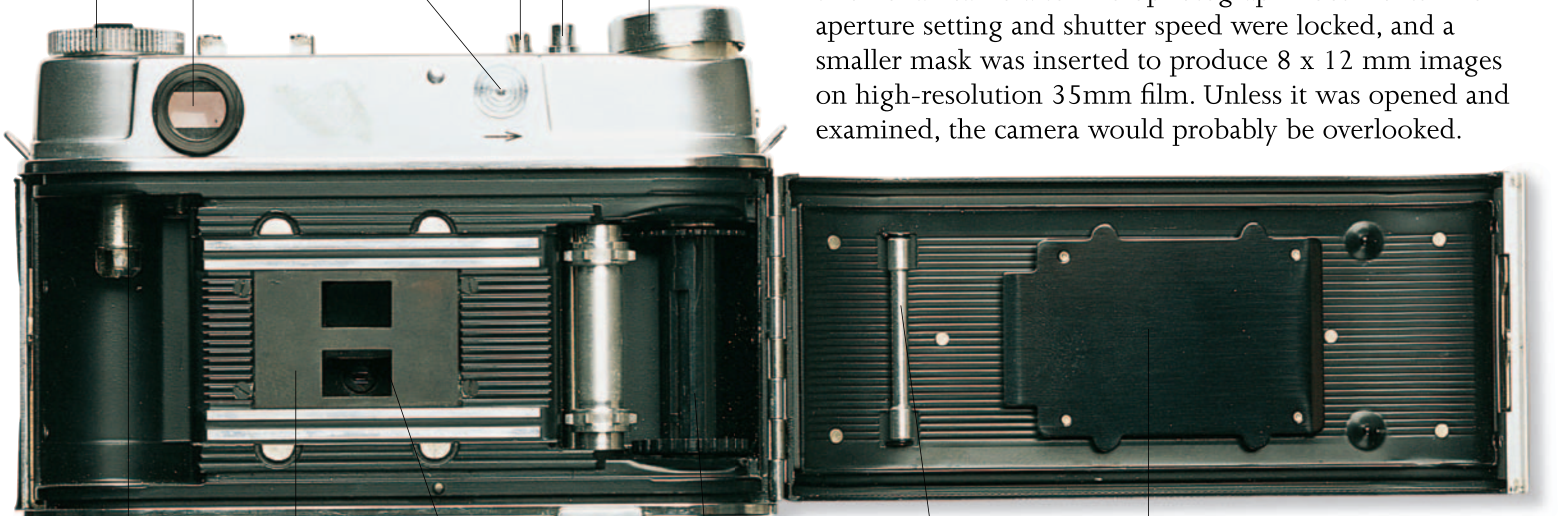
TOP VIEW

High-volume copying
Large quantities of documents can be copied quickly with this technique because once the equipment is set up, each document can be rapidly placed in the correct position and photographed. A standard 35mm camera is used, along with books, adhesive tape, rulers, and desk lamps. With practice, the best combination of exposure time, focus, and lighting can be established. The setup is then exactly reproduced for each copying session.

Copy cameras III

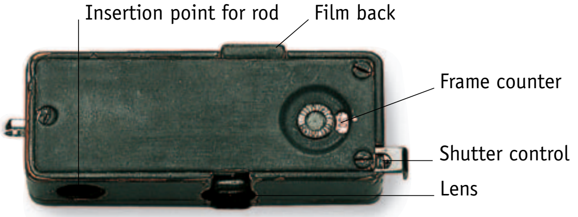
Modified Kodak Retina IIIS camera

The technical service of the HVA (see p. 56) modified this Kodak camera to microphotograph documents. The aperture setting and shutter speed were locked, and a smaller mask was inserted to produce 8 x 12 mm images on high-resolution 35mm film. Unless it was opened and examined, the camera would probably be overlooked.

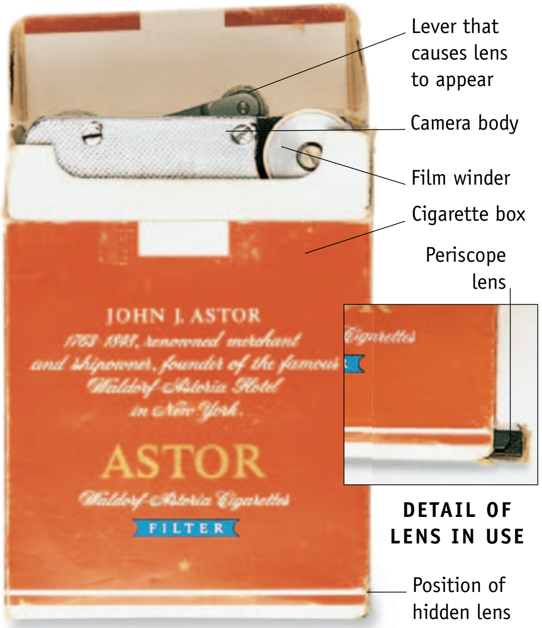


Granitnick-1 rolling copy camera

Masked in a cigarette box, this KGB camera, which was made in 1965, could photograph up to 40 pages of documents as it rolled across them. The small lens appeared when the lever was placed on the document.



ROLLING COPY CAMERA

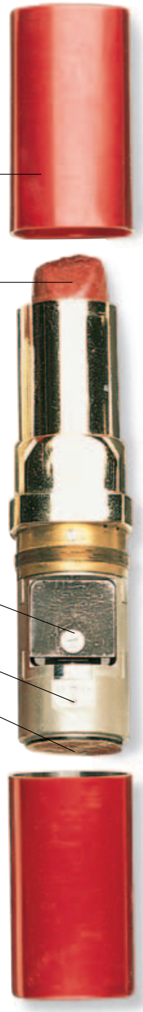

Lever that causes lens to appear
Camera body
Film winder
Cigarette box
Periscope lens
JOHN J. ASTOR
1763-1848, renowned merchant and shipowner, founder of the famous Waldorf-Astoria Hotel in New York.
ASTOR
Waldorf-Astoria Cigarettes
FILTER
Cigarettes
DETAIL OF LENS IN USE
Position of hidden lens

ROLLING COPY CAMERA

ROD

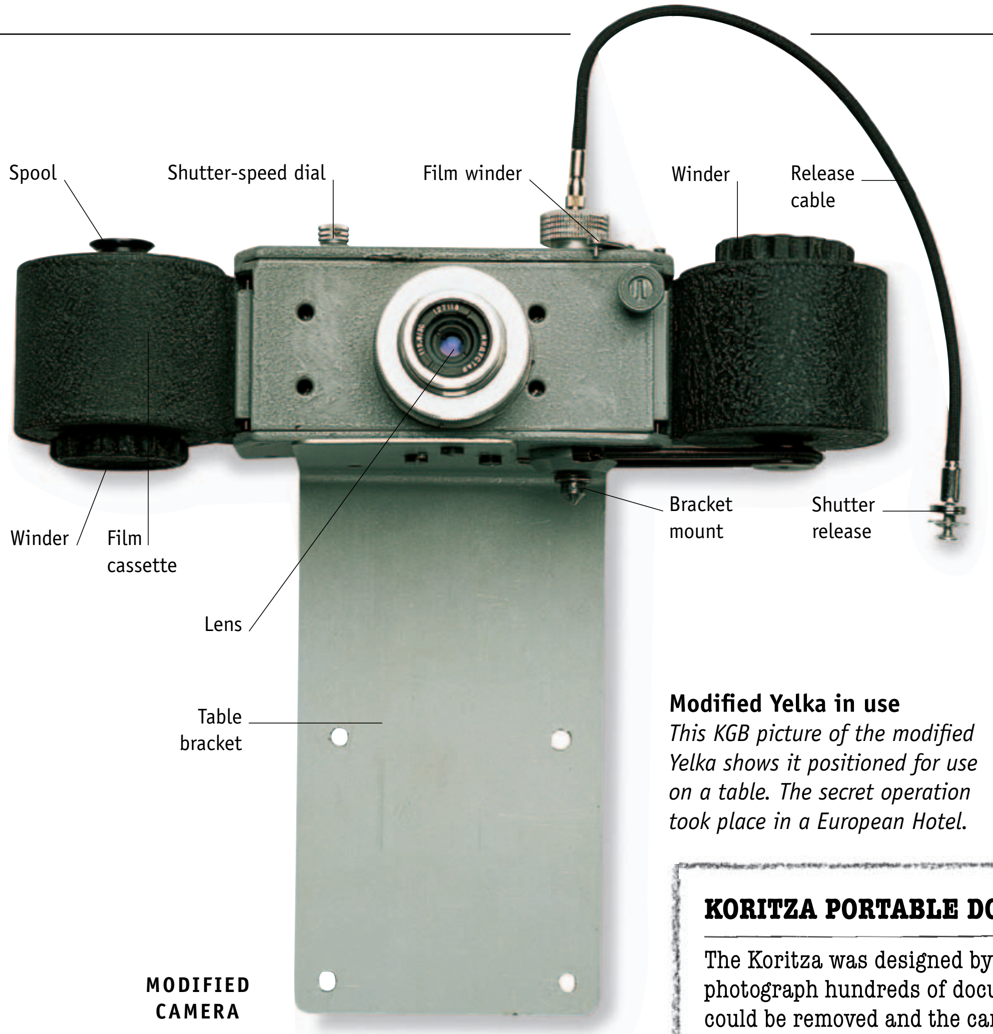
Rolling camera prototype

In 1961, the KGB designed a prototype rolling camera with a Minox film cassette for the rapid photographing of a document. The rod positions the camera the correct distance above the paper, and a propeller inside the camera advances the film as the wheel moves across the document.



Zvouk lipstick camera

The KGB designed this small lipstick camera in the 1970s, especially for female agents. The camera could photograph up to 30 documents using special 6mm film cassettes. The agent was also issued with an identical lipstick tube for daily use.



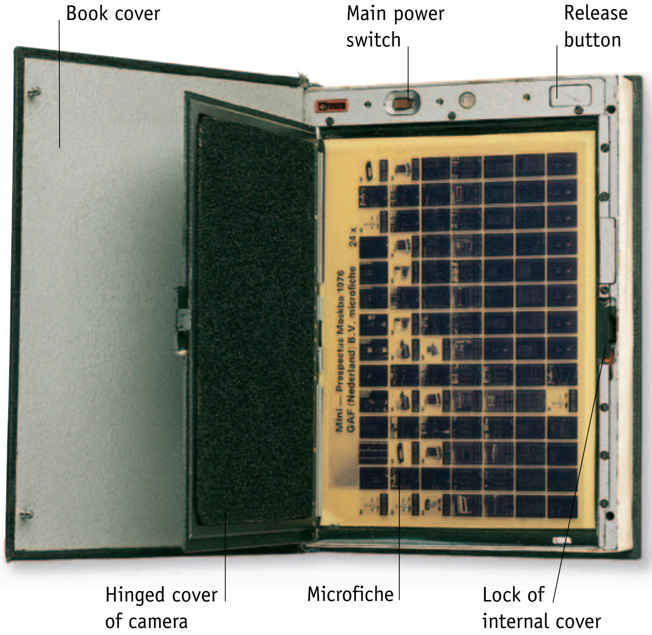
Modified Yelka camera

The Illegals Directorate of the KGB had this Yelka copy camera modified for covert use in an airport hotel, using only ambient room light. The bracket allowed the camera to be mounted on a bedside table in order to photograph documents placed on the floor.

Modified Yelka in use
This KGB picture of the modified Yelka shows it positioned for use on a table. The secret operation took place in a European Hotel.

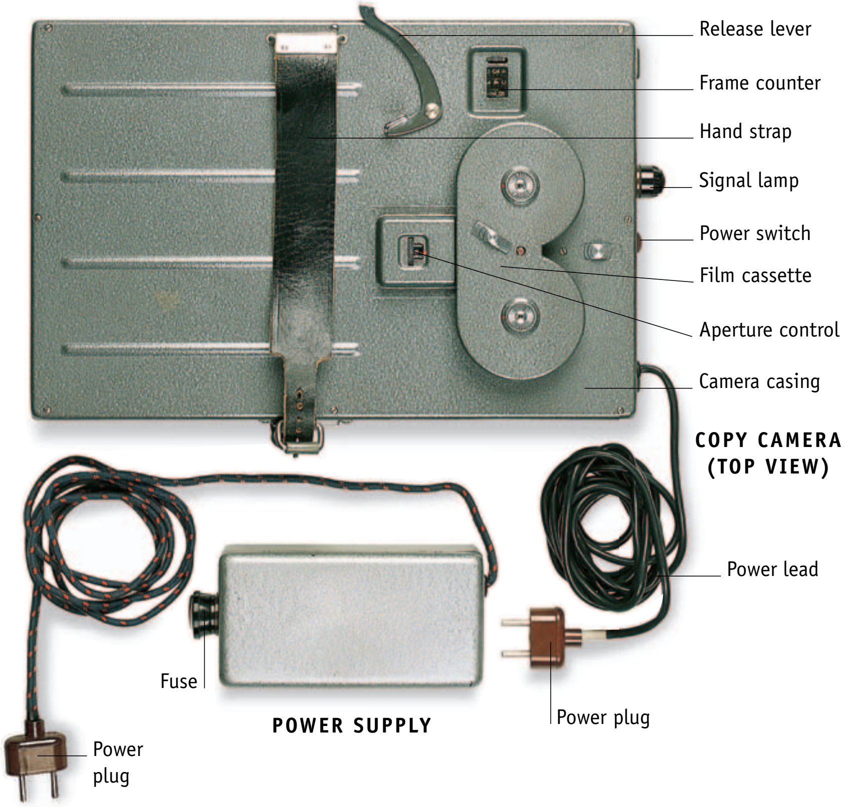
Zachiyt microfiche copier

The KGB produced the Zachiyt in the 1970s to covertly copy the increasing number of microfiches being used to store scientific, technical, and military information. The copier was disguised as a book and could make up to 35 copies without recharging.

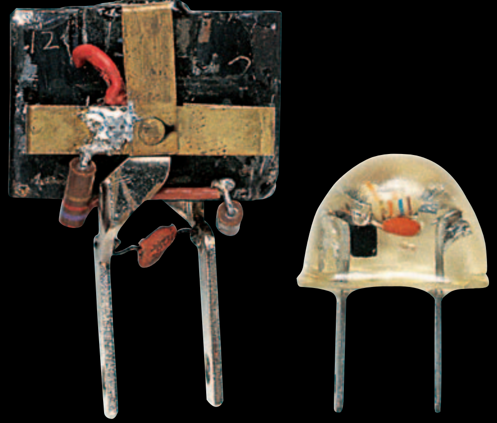


KORITZA PORTABLE DOCUMENT COPY CAMERA

The Koritza was designed by the KGB as a portable copy machine to photograph hundreds of documents onto 35mm film. The bottom of the copier could be removed and the camera used to photograph a map or image mounted on the wall. It was manually operated but required external power to operate its internal lights. An adaptor allowed it to be used inside a car.



SECRET OPERATIONS



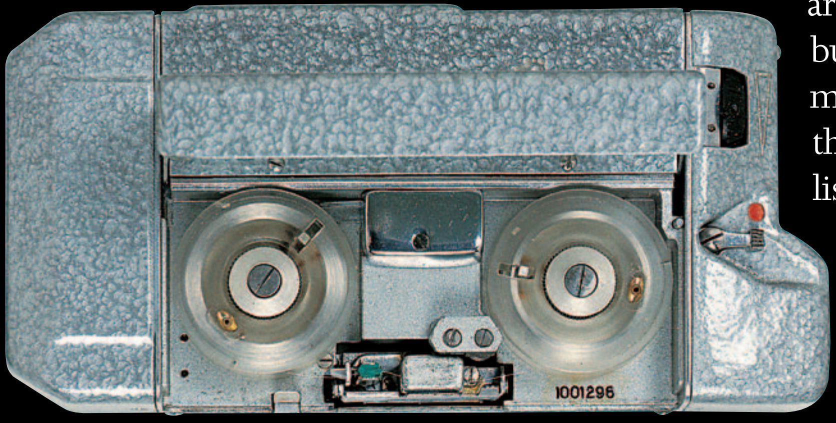
CIA bugs and plugs
Items of electrical equipment, such as plugs, make good hiding places for listening devices and infrared receivers. They draw their power from the electrical socket and can work for years if not detected.

THE CENTRAL TASK of an intelligence agency is to obtain secret information, but this is only one of a range of secret operations that are vital to it. Others include communications, countersurveillance, sabotage, and escape and evasion (avoiding capture or recapture by the enemy). For all these activities, the large intelligence agencies train skilled personnel and develop special techniques and equipment. The KGB had a Directorate called the OTU (Operational Technical Department), and now the SVR has the same. The CIA counterpart is the Office of Technical Service (OTS). In Israel, Mossad employs technical experts known as *marats* for the same purpose.

Miniature monocular
This KGB monocular, held between the fingertips when used, is small enough to be stored inside a 35mm film canister.

WATCHING AND LISTENING

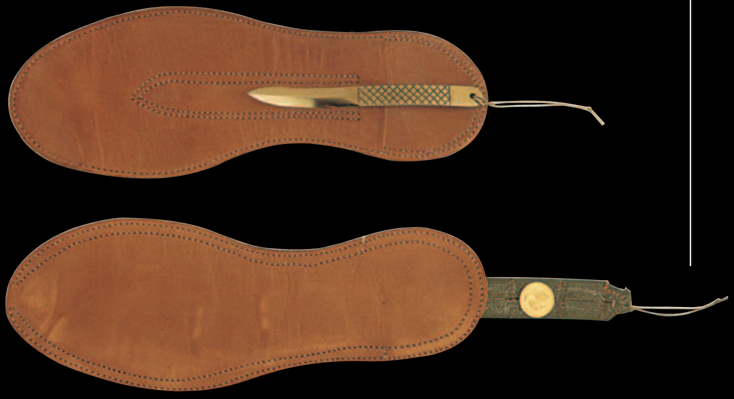
A major role for the technical experts in an intelligence agency is to provide the means of carrying out surveillance. Photographic and video cameras may be employed to monitor the activities of foreign agents. A number of notable spies have been caught as a result of visual surveillance operations. Audio surveillance, too, can yield much valuable intelligence. Specialists are trained to place listening devices—known as bugs—in locations where secret conversations or meetings may take place. In certain circumstances the listening devices are linked by wire to a nearby listening post. Alternatively, the bug may be coupled with a transmitter, which sends the sound in the form of a radio signal. The signals are picked up by special receivers, some of which incorporate a recording device. Another branch of audio surveillance entails taking the listening device personally to where it is needed. Microphones and recording devices that can be hidden in an agent's clothing have been developed for this purpose.



Wire recording device
The KGB Mezon recording device is sufficiently compact to be hidden in the clothing and activated by a control switch in the pocket. The device uses thin wire instead of tape to store its recordings.

Commercial lockpicking tools

The type of lock found in the target location will determine which of the many different tools are selected for use.



SOE concealed blades

Special concealments were devised for escape aids. Here, leather inner soles provide hiding places for a blade and five gold coins.

GAINING ENTRY

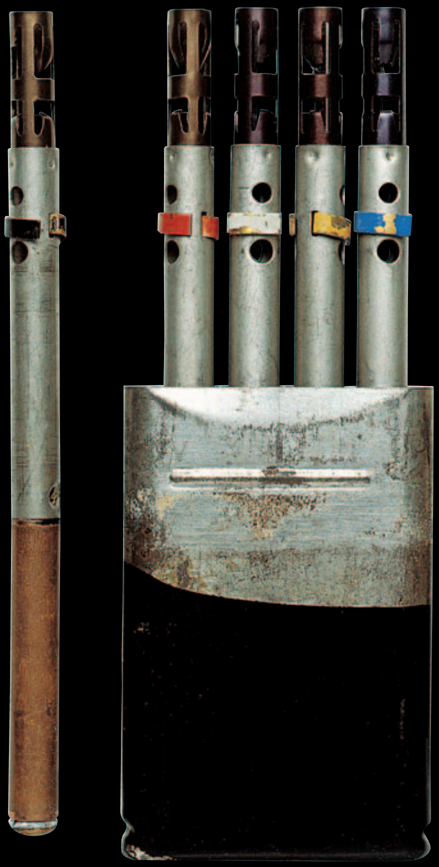
In order to plant a listening device or gain access to secret material, it may be necessary to make a surreptitious entry. The value of whatever intelligence is gained will be reduced if the targets suspect a breach of security.

The first step in carrying out a surreptitious entry is reconnaissance. One or more visits must be made to the target location. Using specialized equipment, it is even possible to see under doors and through keyholes. A key will be needed, and the best way is to "borrow" a key that can be copied and then returned. If this cannot be done, a lock will have to be picked, and this again is a specialized skill.

WARTIME OPERATIONS

In wartime, personnel sent to operate behind enemy lines are equipped and trained to escape from, or evade capture by, the enemy. During World War II, many concealments were devised for escape aids, such as the maps and compasses that were issued to aircrew flying missions over enemy territory.

World War II also led to increased development of tools and techniques for sabotage behind enemy lines. Many forms of explosive device were produced. Some were disguised as coal or animal droppings. Some had delay devices, such as pencil fuses, facilitating controlled detonation. Enemy ships in harbor were attacked using special small boats and canoes, and limpet mines were attached magnetically to the hulls. Sabotage is not merely profitable in terms of the destruction it causes, but also due to the large numbers of troops the enemy is forced to divert to guard transportation, communications, and industrial installations.



OSS pencil fuses

These devices were used by saboteurs during World War II to delay the detonation of explosives. Delays gave the saboteurs enough time to escape in safety (see p. 127).

Visual surveillance I

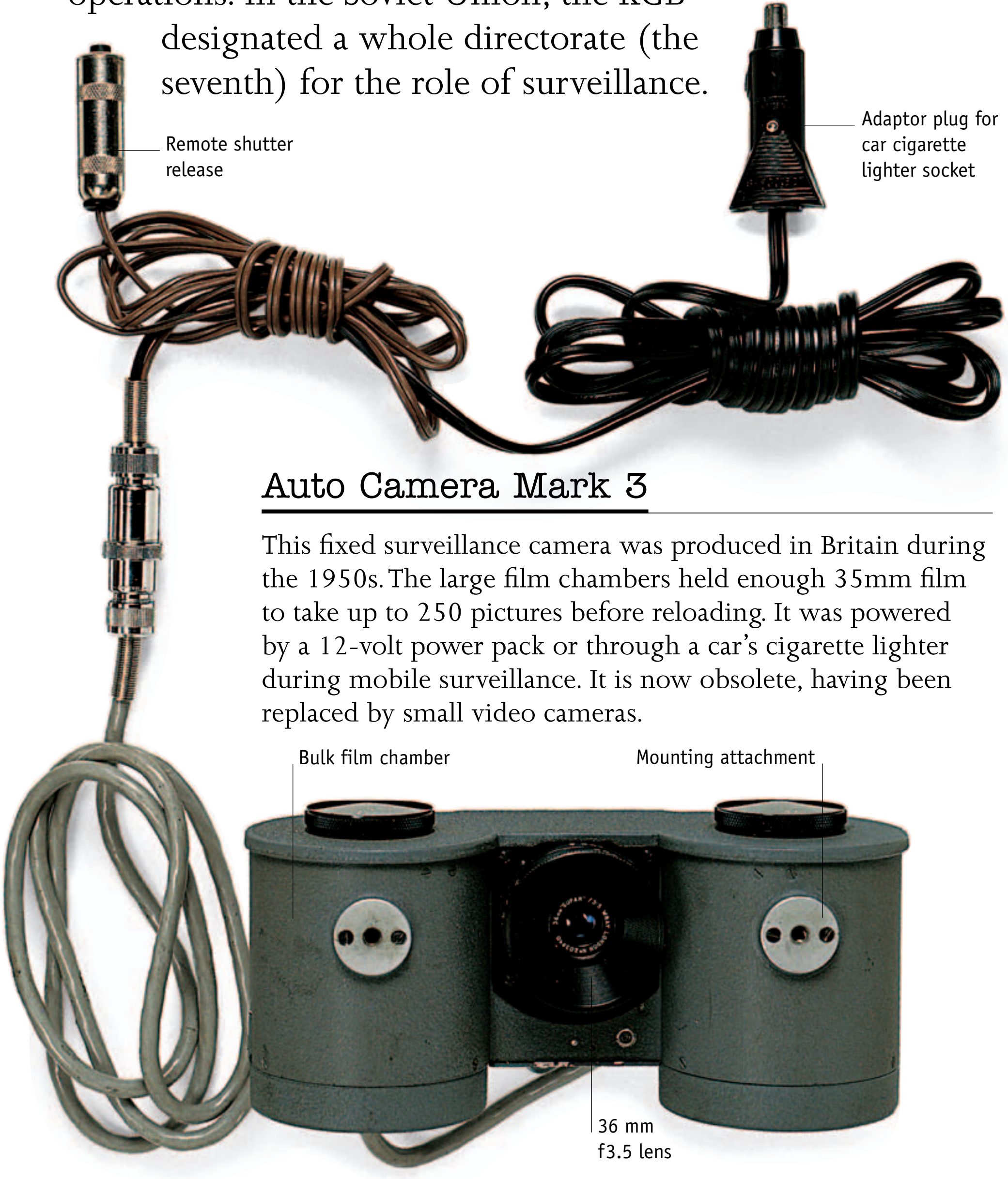
VISUAL SURVEILLANCE is the art of watching without being detected. Intelligence agencies train and employ special teams to perform this role, using such equipment as handheld optical devices (including night vision equipment) and film and video cameras. Cameras may be set up for long-term surveillance, or miniaturized for concealment on the spy's person. In American and British agencies, visual surveillance experts are called watchers; their talents are employed in internal security and counterintelligence operations. In the Soviet Union, the KGB designated a whole directorate (the seventh) for the role of surveillance.

OLEG PENKOVSKY

SPY PROFILE

An officer in Soviet military intelligence, Oleg Penkovsky (1919–63) was active as a mole at the height of the Cold War. During 1961 and 1962 he passed information to the CIA and MI6 (see p.217) about the military capabilities and the intentions of the Soviet Union. Eventually, the Soviets arrested Penkovsky, probably as a result of visual and photographic surveillance carried out by the KGB. He was executed after a show trial.

Photographic evidence
In this KGB surveillance photograph, Penkovsky, working as a mole for the West in Moscow, enters a building used as a dead drop site (see p. 170).

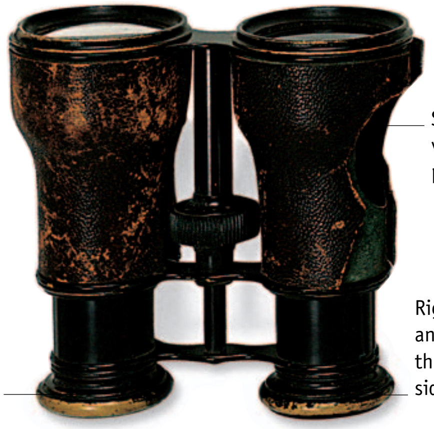


Auto Camera Mark 3

This fixed surveillance camera was produced in Britain during the 1950s. The large film chambers held enough 35mm film to take up to 250 pictures before reloading. It was powered by a 12-volt power pack or through a car's cigarette lighter during mobile surveillance. It is now obsolete, having been replaced by small video cameras.

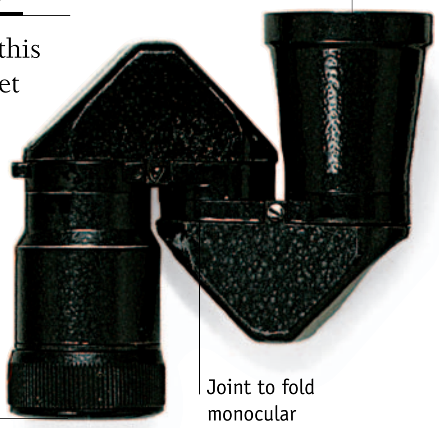
Surveillance binoculars

Made in France in the 19th century, this pair of binoculars has an angled mirror inside one of its telescopes. This enabled the user to pretend to look straight ahead, while covertly looking to the right. The other telescope gave a normal view.



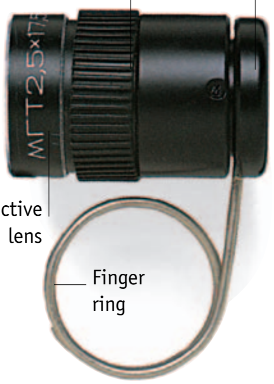
Folding monocular

Members of the KGB used this folding monocular for secret visual surveillance. The monocular was jointed so that it could be unfolded (as shown here) and held in the fist for surreptitious surveillance without attracting attention.



Miniature monocular

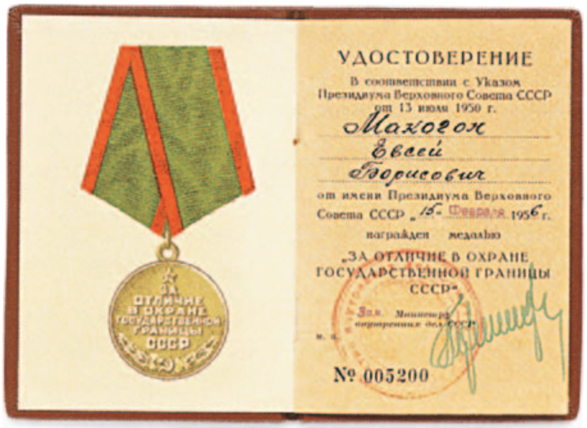
Shown here at its actual size, this monocular was so small that its KGB users were able to conceal it in an empty 35mm film container. The monocular had a magnification of 2.5 times. The finger ring enabled the spy to hold the instrument, when it was not in use, in one hand while not appearing to be concealing anything.



KGB BORDER GUARDS

The Border Guards of the Soviet Union formed a separate directorate within the KGB. This was a fully equipped military force, with its own artillery, armored fighting vehicles, and patrol boats. The force comprised 300,000 to 400,000 personnel at its peak. It fulfilled the dual role of keeping foreign intruders out of the Soviet Union and preventing any unauthorized exits. To help them with these duties, the Border Guards were issued with specialized visual surveillance equipment, such as the passive PN-1A night vision device (shown below left).

BORDER GUARD'S MEDAL (REVERSE)



УДОСТОВЕРЕНИЕ

В соответствии с Указом Президиума Верховного Совета СССР от 13 июля 1950 г.

Махогон

Евсей

Борисович

от имени Президиума Верховного Совета СССР „15" Февраля 1956 г.

награжден медалью

„ЗА ОТЛИЧИЕ В ОХРАНЕ ГОСУДАРСТВЕННОЙ ГРАНИЦЫ СССР"

Зам. Министра внутренних дел СССР

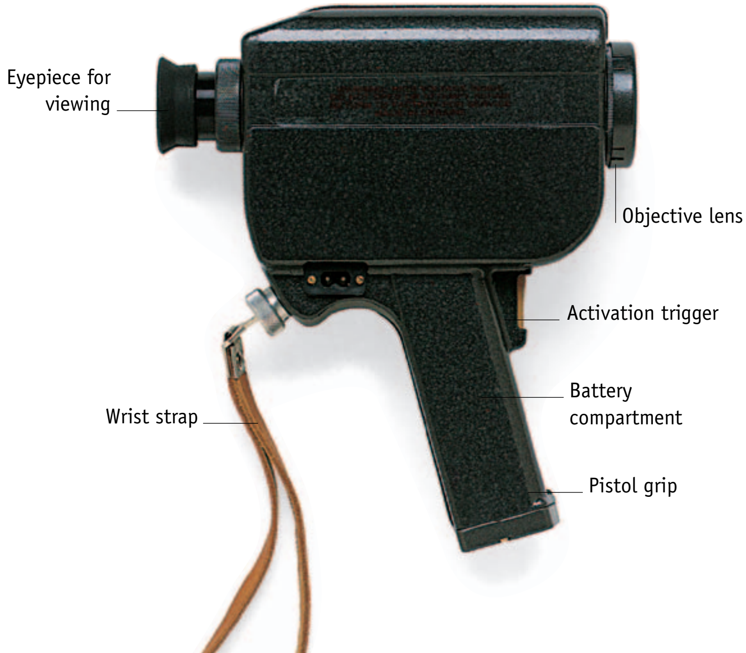
м. п.

№ 005200

FRONT OF MEDAL WITH CERTIFICATE

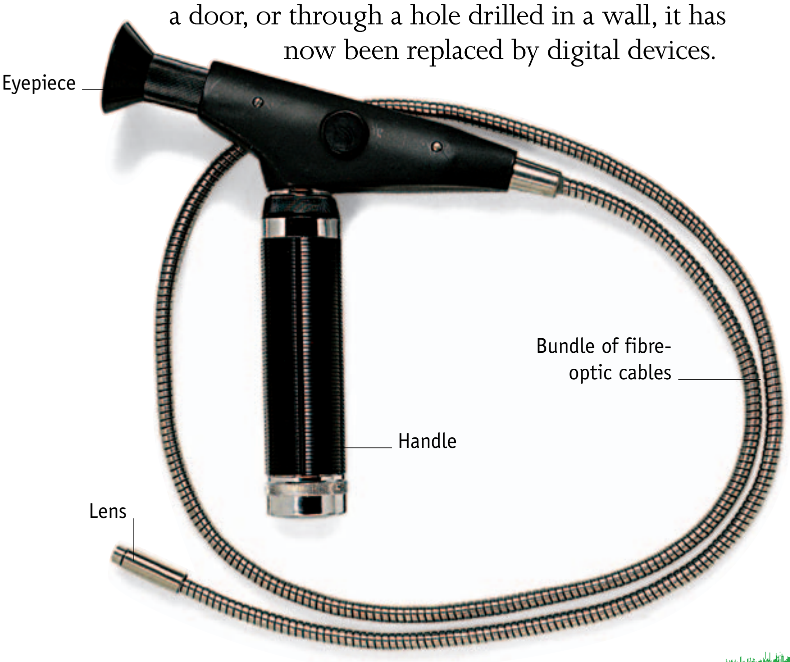
Passive PN-1A night vision device

This handheld device amplified starlight so the user could see in almost total darkness, and worked almost silently. It is now obsolete, having been replaced by a new generation of infrared night surveillance optics.



CIA fiberscope

Based on medical equipment, this fiberscope received images through 7,500 strands of fiber-optic cable. Used to look under a door, or through a hole drilled in a wall, it has now been replaced by digital devices.

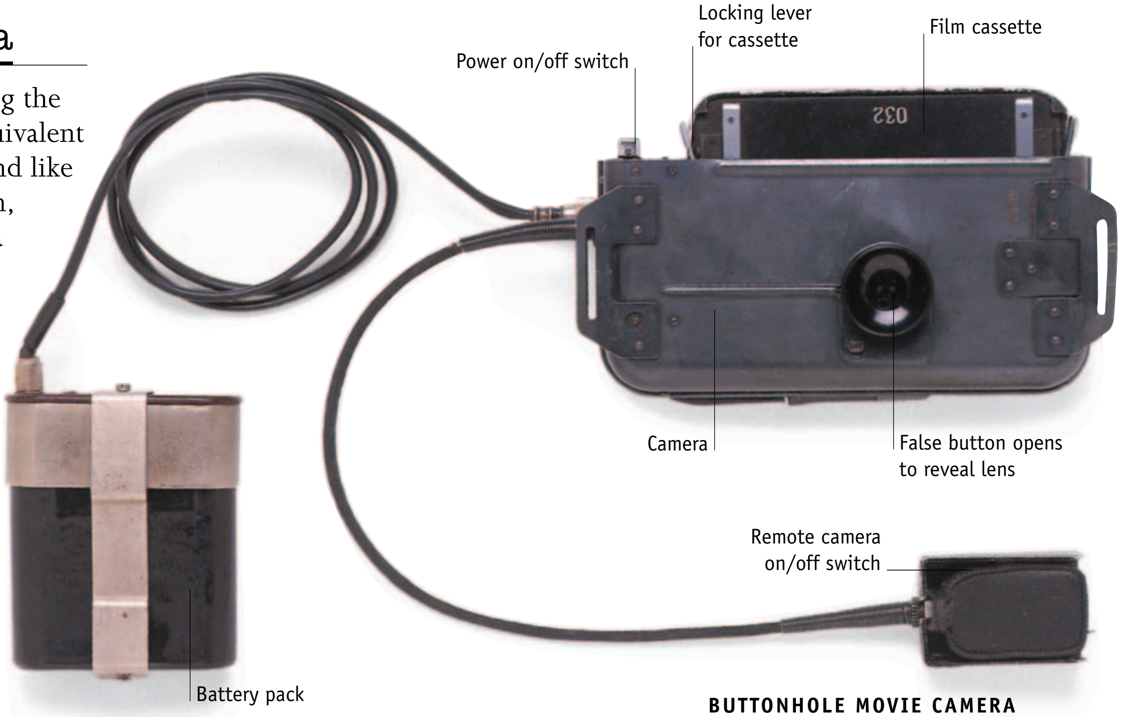


“*This page left intentionally blank.*”

Buttonhole movie camera

This device was used by the KGB during the 1960s and 1970s. It was the movie equivalent of the KGB's F21 camera (see p. 88), and like the F21 it filmed through a false button, which opened to reveal a lens. It used a film cassette that was mounted on the camera at right angles to the lens. The user turned the camera on and off with a switch hidden in a pocket. A battery pack, concealed in another pocket, powered the camera.

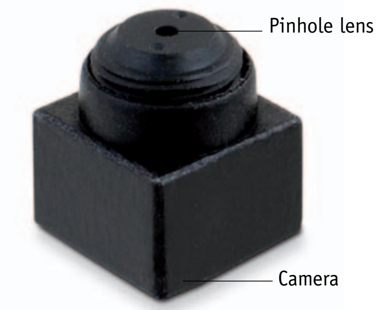
SPARE FILM CASSETTE


Power on/off switch
Locking lever for cassette
Film cassette
Camera
False button opens to reveal lens
Remote camera on/off switch
Battery pack

BUTTONHOLE MOVIE CAMERA

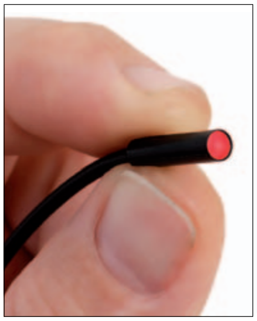
PC208 video camera

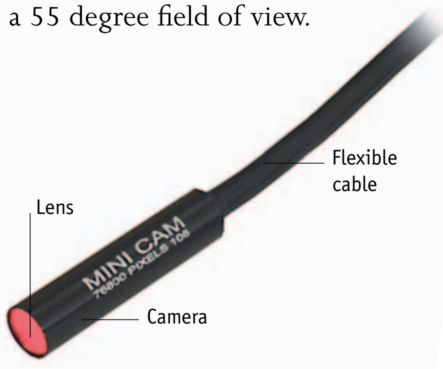
The PC208 is the world's smallest color video camera, at just ⅜ in by ⅝ in (1 cm by 1.5 cm), so it is easily concealed. Its pinhole lens has a 50 degree field of view.



PC210 video camera

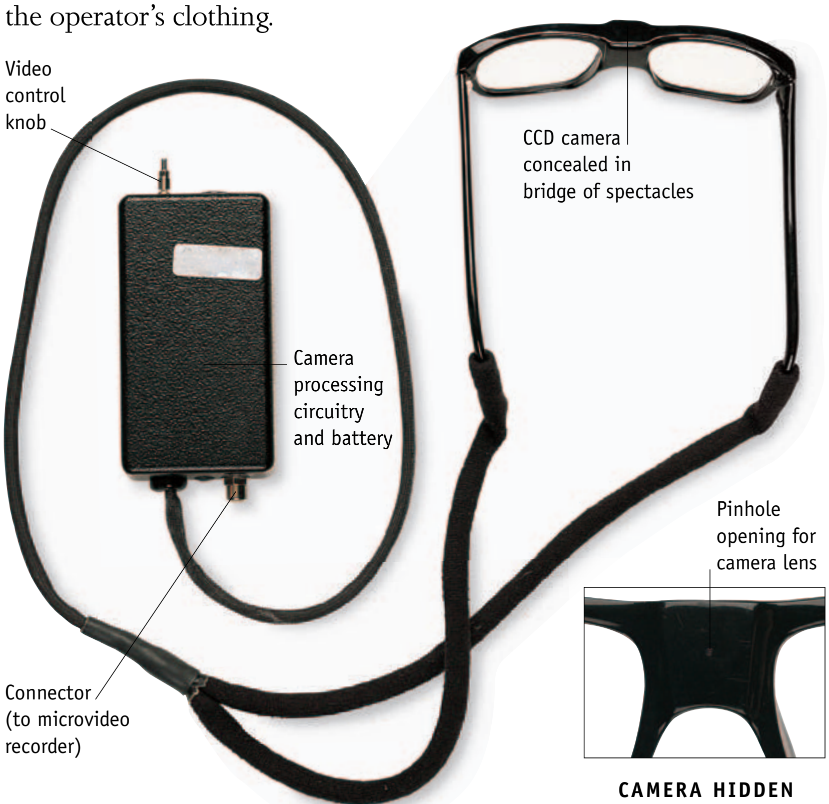
The world's slimmest color video camera—with a tip diameter of just 3/16 in (5 mm)—the flexible and unobtrusive PC210 has a 55 degree field of view.





Glasses surveillance system

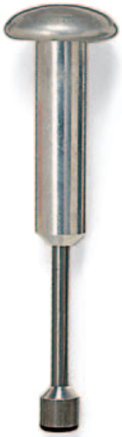
For close-contact surveillance operations, these modified glasses conceal in the bridge a CCD (charge-coupled device) camera, with a pinhole opening for the lens. Images are transmitted through cables to a processing unit and a microvideo recorder hidden in the operator's clothing.


Video control knob
CCD camera concealed in bridge of spectacles
Camera processing circuitry and battery
Pinhole opening for camera lens
Connector (to microvideo recorder)

SURVEILLANCE SYSTEM

CAMERA HIDDEN IN BRIDGE

Listening devices I

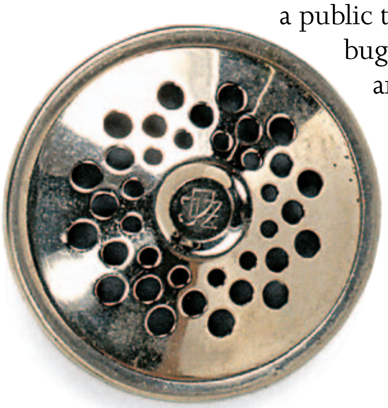


CIA SILENT HAMMER

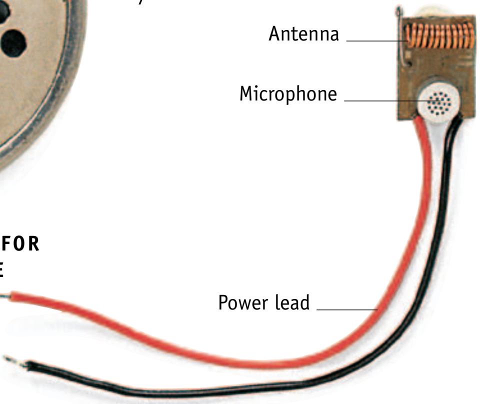
INTELLIGENCE AGENCIES make great efforts to develop devices that will enable them listen to their enemy's conversations. Tiny eavesdropping microphones are coupled with miniature amplifiers, transmitters, or tape recorders, while other devices intercept signals from telephone wires. Once created, the equipment must be planted. Specialized equipment, such as the fine-wire kit or the silent hammer, is available for installing microphone wires in walls. A transmitted signal from a listening device should be strong enough to be received at a listening post, but weak enough to make it difficult to locate using ordinary antibugging devices. Now listening devices exist that can store signals digitally and transmit them to a listening post at a predetermined time.

Miniaturized listening equipment

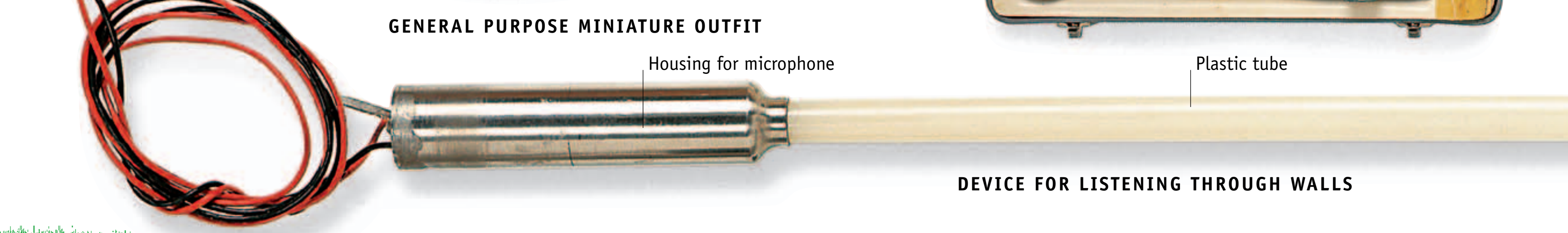
Myriad miniaturized devices have been made for spying. These CIA devices are: a bugged mouthpiece, for insertion in a public telephone; a multipurpose bug, small enough to hide almost anywhere; and a through-the-wall device, with a plastic tube that would not be discovered by metal detectors.



BUGGED MOUTHPIECE FOR PUBLIC TELEPHONE



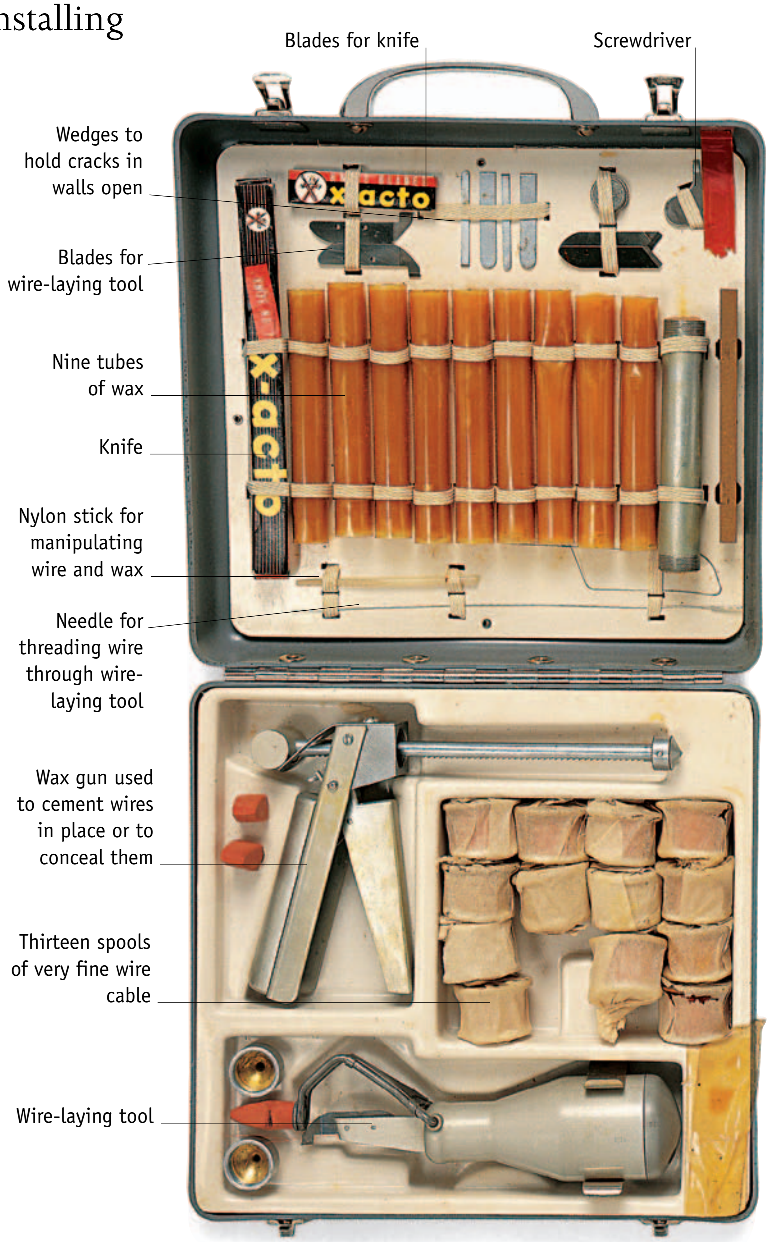
GENERAL PURPOSE MINIATURE OUTFIT



DEVICE FOR LISTENING THROUGH WALLS

Fine-wire kit

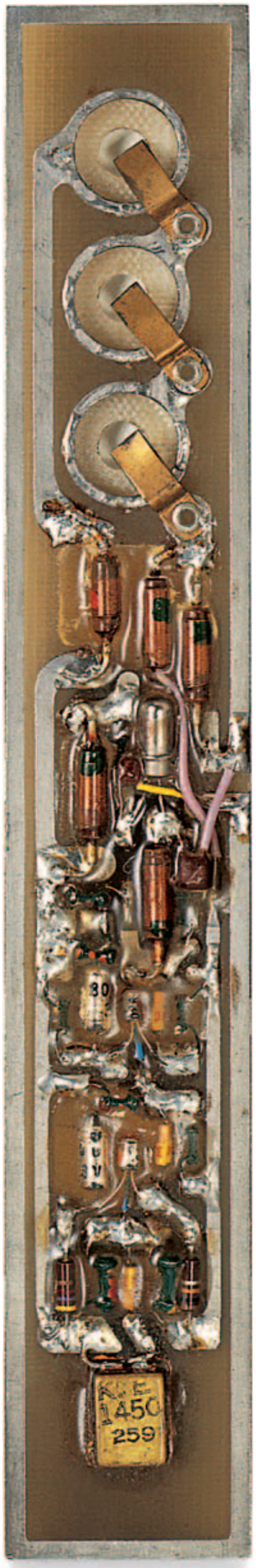
To hide the wires when installing a bug, American technicians developed this wire-laying tool and its accessories. The tool is capable of forcing fine wires or cables into soft building materials or cracks. A monitoring circuit warns if the circuit is broken during installation.



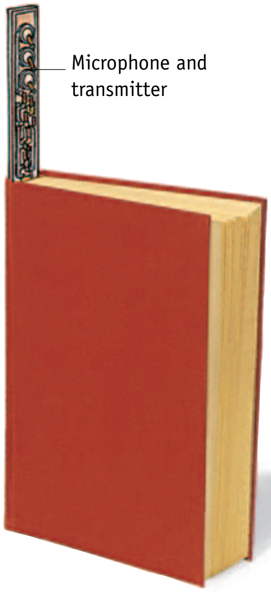
Blades for knife
Screwdriver
Wedges to hold cracks in walls open
Blades for wire-laying tool
Nine tubes of wax
Knife
Nylon stick for manipulating wire and wax
Needle for threading wire through wire-laying tool
Wax gun used to cement wires in place or to conceal them
Thirteen spools of very fine wire cable
Wire-laying tool
X-acto

Pen and book devices

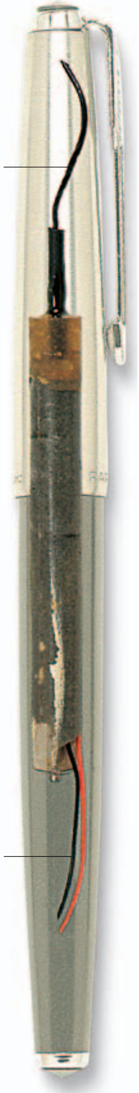
During the decades after World War II, a CIA officer who wanted to record a meeting surreptitiously might be equipped with a listening device disguised as a pen. Another ingenious CIA listening device fitted into the spine of a book, which could be placed in a room without causing suspicion. These were typical bugs of the 1960s—today's devices use digital technology and are much smaller.



MICROPHONE AND TRANSMITTER FOR BOOK SPINE



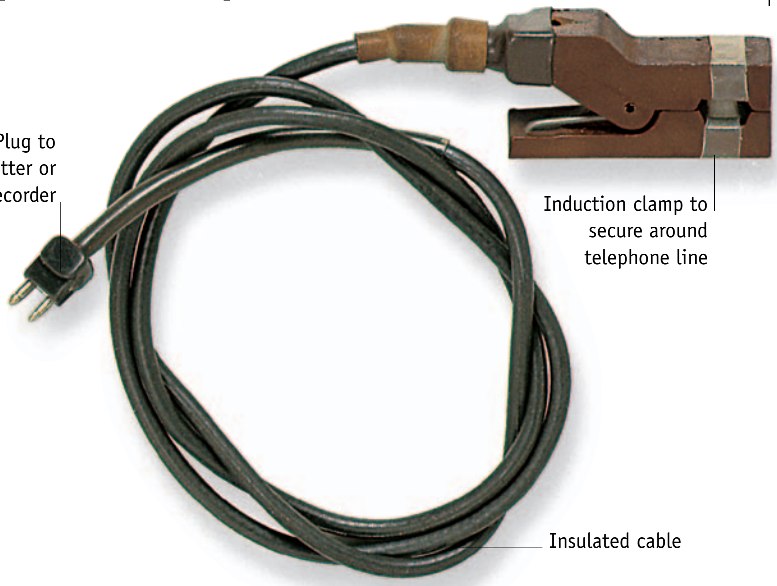
INSERTION OF TRANSMITTER INTO BOOK SPINE



MICROPHONE AND TRANSMITTER CONCEALED IN PEN

Induction telephone tap

This commercial device can be clamped onto any single-line external telephone cable and connected either to a transmitter or tape recorder. Both sides of the conversation can be received clearly. With no physical connection to the wire inside the telephone cable, the tap is difficult to detect.


Plug to transmitter or recorder
Induction clamp to secure around telephone line
Insulated cable

PETER WRIGHT

Peter Wright (1916–95) was the British Security Service's first technical officer. He joined the Security Service (MI5) in 1955, having done scientific work throughout World War II. The early years of his career were spent inventing specialized listening devices for various operations. Wright also attempted to work out how the Soviet listening devices that were found in the buildings of the Western nations worked. The Thing (see p. 112) was a Soviet listening device found in the Great Seal in the office of Spaso House, the American ambassador's residence in Moscow. Wright was the first Westerner to understand fully how it worked. Having shown an aptitude for all aspects of counterintelligence work, Wright moved to D Branch, which was responsible for counterespionage, particularly Soviet activities in Britain. He eventually went on to become an Assistant Director of MI5.

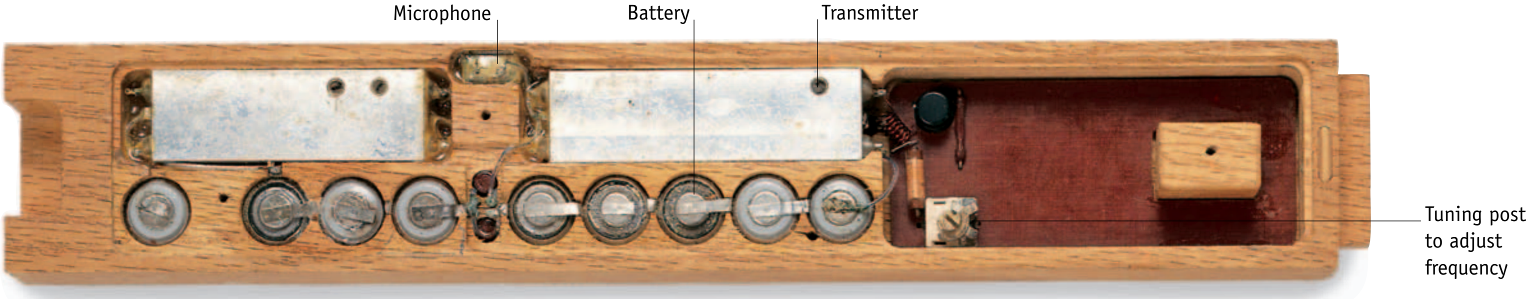
MI5's chief scientist

Despite having no formal scientific education, Peter Wright was a brilliant innovator, constantly trying to find scientific solutions to MI5's problems.

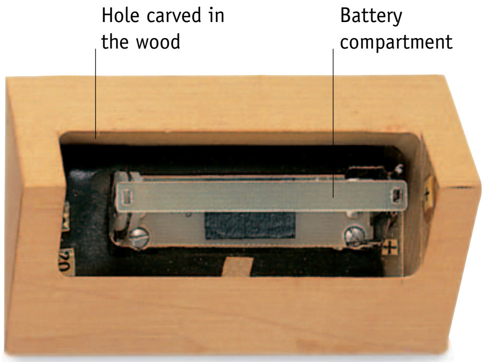
“*This page left intentionally blank.*”

Modified furniture components

Bugs can be hidden in fake furniture parts, which are then substituted for the original piece. Inside the components shown here, microphones and transmitters have been installed. One is part of a desk, modified by Czech technicians. The other is a brace that can be adapted for any wooden furniture; it was used by an American audio-surveillance team.



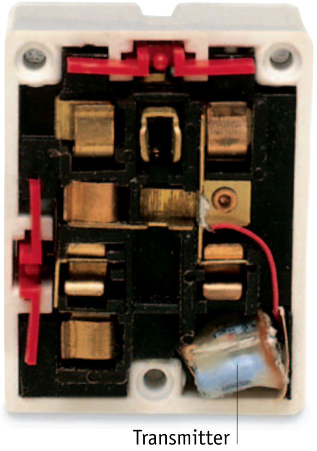
DESK COMPONENT



MULTI-PURPOSE WOODEN BRACE

Adaptor listening device

This microphone-and-transmitter set concealed in a British adaptor allows unlimited transmitting time without concern for battery drain, because its power is taken directly from the socket. A distinct disadvantage of this device is that the transmitter is permanently powered, which would enable a trained counterintelligence "sweep team" to detect it easily.

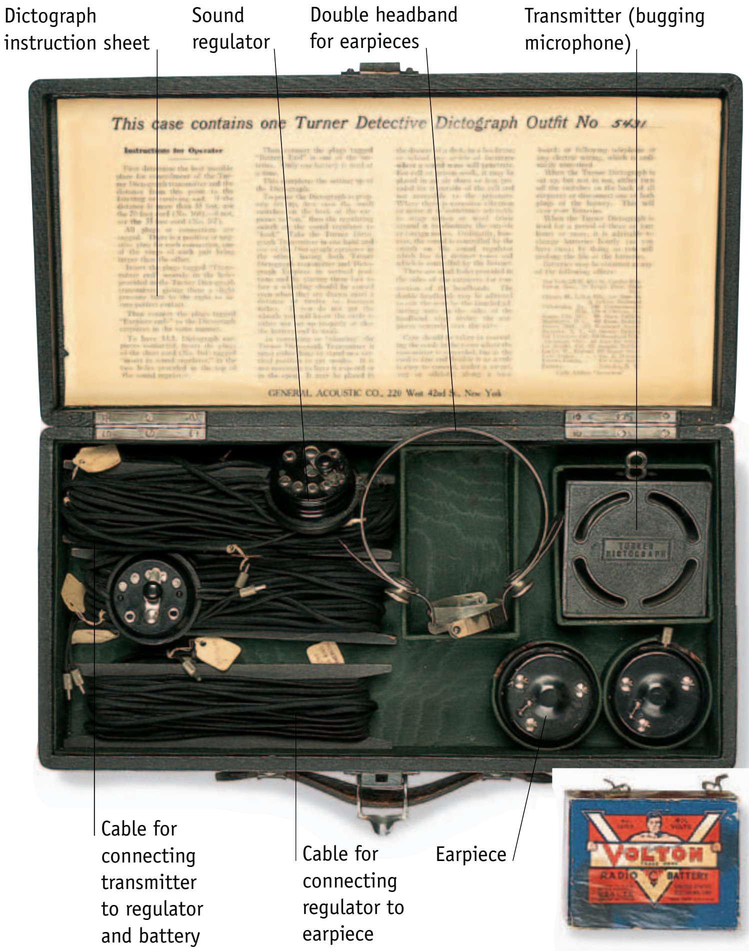


INTERIOR OF ADAPTOR

FRONT OF ADAPTOR

Turner detective dictograph outfit

This battery-driven device, used in World War I, provided the operator with a concealable transmitter, sound regulator, and earpiece for eavesdropping on suspects and conspirators up to 78 ft (24 m) away. The dictograph was the first eavesdropping apparatus to be sold commercially, and its operators were warned not to use it for blackmailing and other illegitimate purposes.


Dictograph instruction sheet
Sound regulator
Double headband for earpieces
Transmitter (bugging microphone)
This case contains one Turner Detective Dictograph Outfit No 5431
Instructions for Operator
GENERAL ACOUSTIC CO., 220 West 42nd St., New York
Cable for connecting transmitter to regulator and battery
Cable for connecting regulator to earpiece
Earpiece

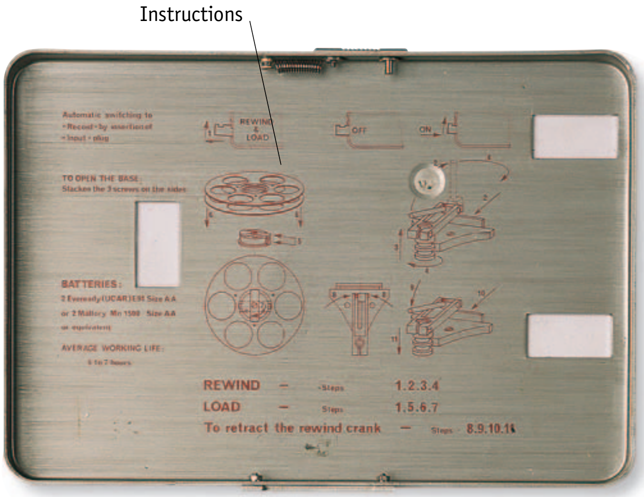
DICTOGRAPH OUTFIT

BATTERY FOR KIT

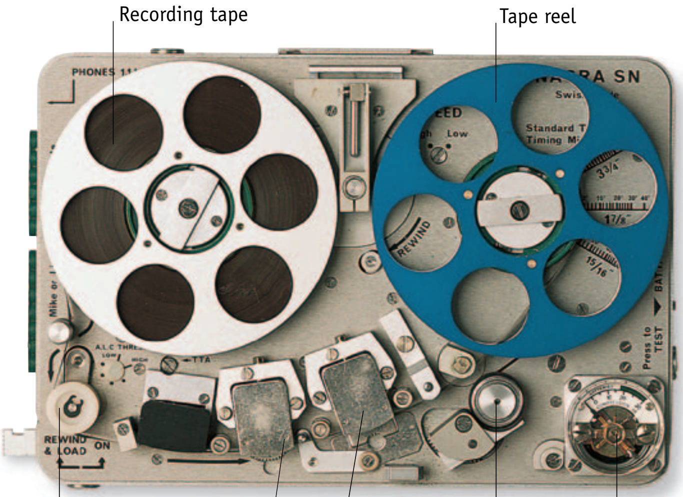
Listening devices III

Nagra SN recorder and pen

The Stasi (see p. 99) used this small reel-to-reel recorder for high-quality recordings. The recorder could be hidden in a person's clothing or concealed in a car or apartment. The agent was also supplied with two pens. One was functional and used on a daily basis so that colleagues became used to seeing it; the other looked identical but concealed a microphone. The agent would secretly switch the real pen for the microphone to record conversations.



LID WITH INSTRUCTIONS

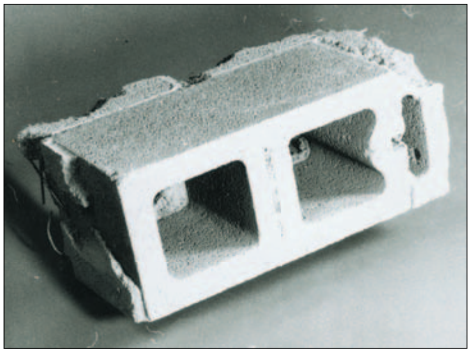


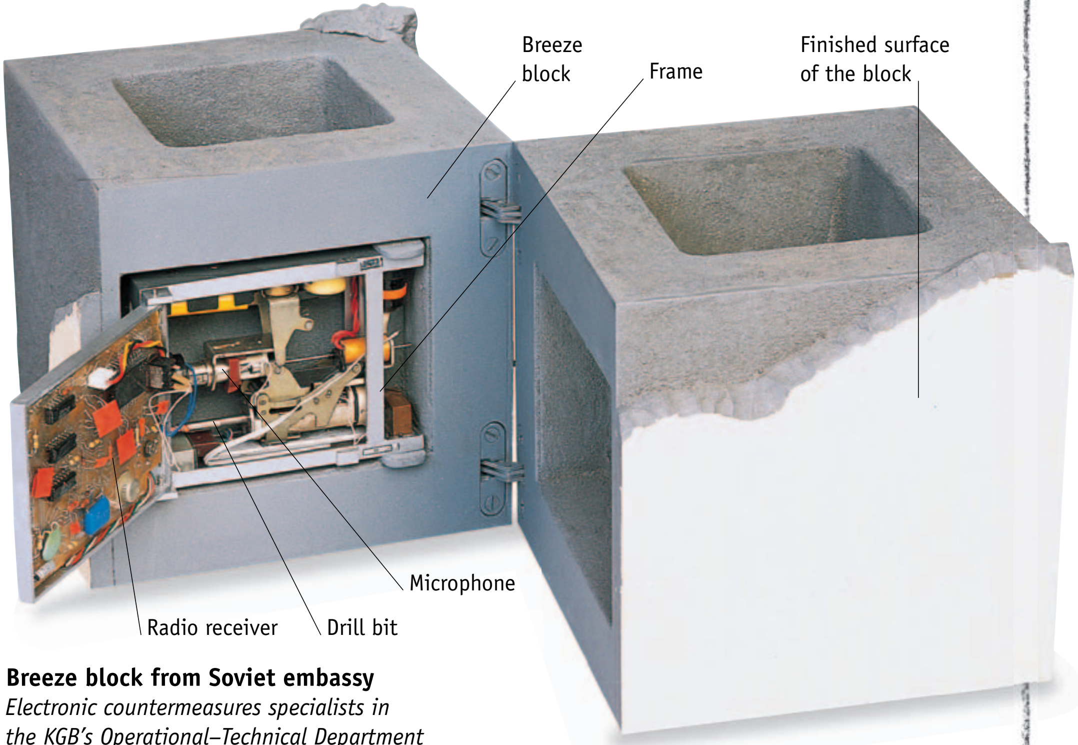
RECORDER

MICROPHONE PEN

DRILL BUG IN BREEZE BLOCK

This sophisticated eavesdropping device was planted inside the wall of a newly built Soviet embassy building in Washington, DC. The remotely controlled apparatus incorporated a drill bit that bored a hole from the inside of the block toward the surface of the wall. At intervals, a microphone was inserted into the hole, also by remote control. When it could pick up sounds, the microphone was left in place. To avoid discovery, the listening device remained dormant when first built into the wall and was afterward activated by a radio signal.



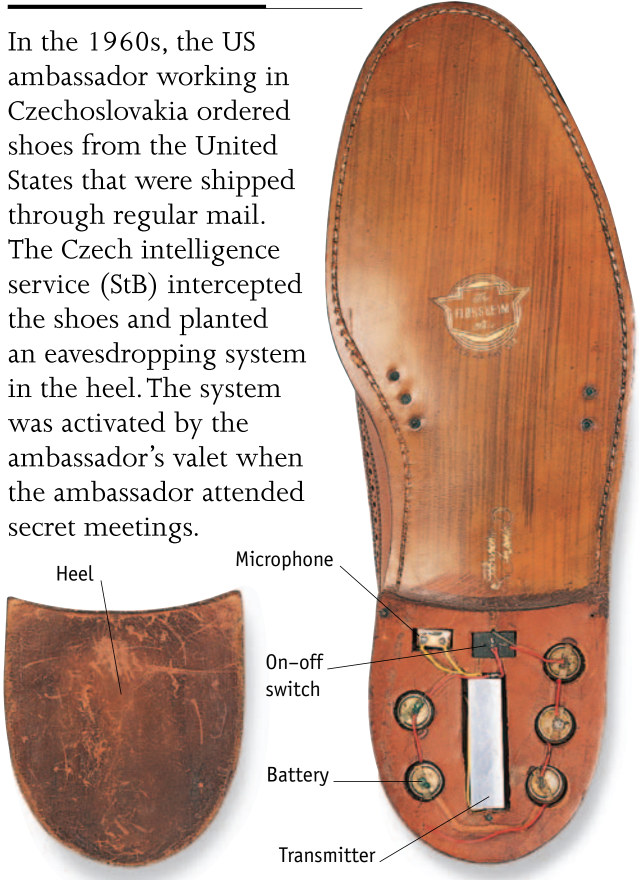


Breeze block from Soviet embassy
Electronic countermeasures specialists in the KGB's Operational–Technical Department located the drill bug in this breeze block by using a nonlinear junction detector.

MODEL OF DRILL BUG IN BREEZE BLOCK

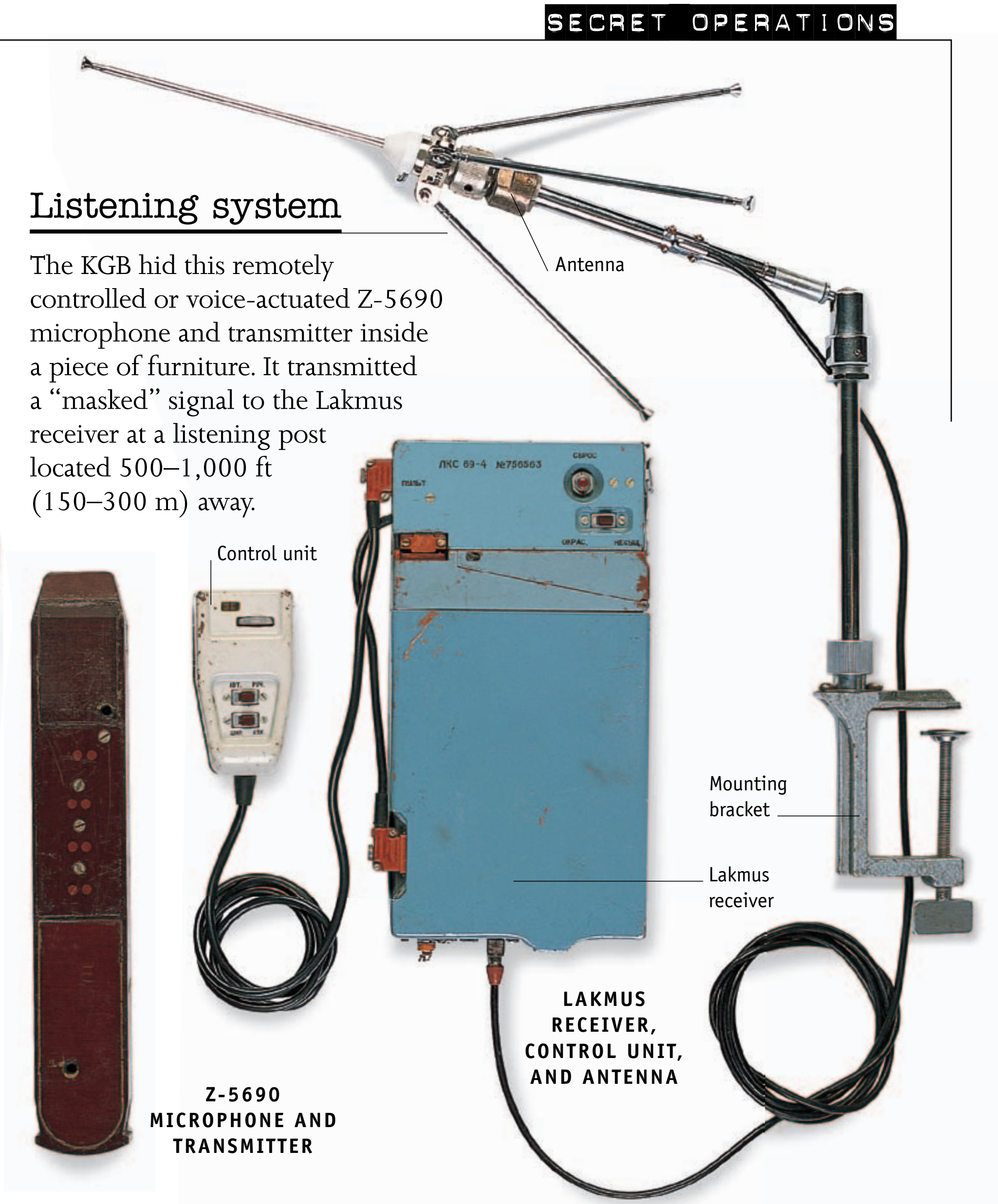
Bug in a shoe

In the 1960s, the US ambassador working in Czechoslovakia ordered shoes from the United States that were shipped through regular mail. The Czech intelligence service (StB) intercepted the shoes and planted an eavesdropping system in the heel. The system was activated by the ambassador's valet when the ambassador attended secret meetings.



Listening system

The KGB hid this remotely controlled or voice-actuated Z-5690 microphone and transmitter inside a piece of furniture. It transmitted a "masked" signal to the Lakmus receiver at a listening post located 500–1,000 ft (150–300 m) away.

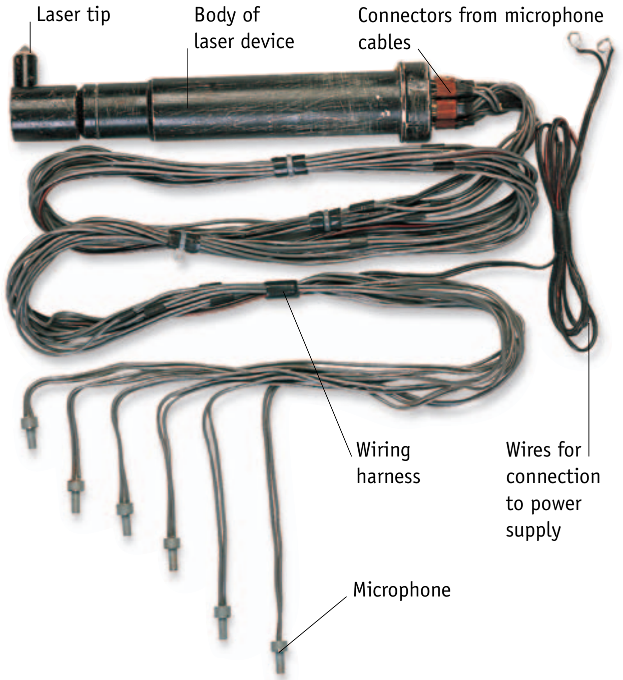


Z-5690 MICROPHONE AND TRANSMITTER

LAKMUS RECEIVER, CONTROL UNIT, AND ANTENNA

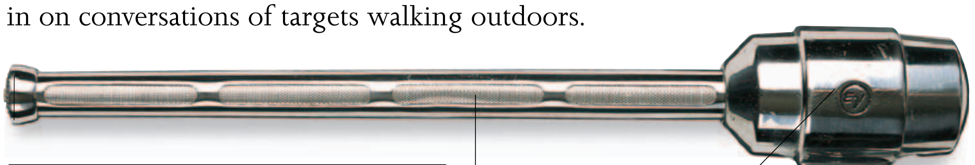
Laser listening device

This device was connected to microphones hidden in a part of a Soviet embassy building in Washington, DC. Conversations were transmitted out on the laser's light beam to avoid detection.


Laser tip
Body of laser device
Connectors from microphone cables
Wiring harness
Wires for connection to power supply
Microphone

Rifle microphone

This highly directional US rifle microphone allowed a listening post monitor to pick up the conversations of a target while excluding other conversations and background noises. The microphone would be connected to a tape recorder and was commonly used to listen in on conversations of targets walking outdoors.


Barrel channels desired sound to microphone
Microphone in casing
Handgrip
Connector (for cable to tape recorder)

Rifle microphone
In this still from a US Defense Department training film from monitor wears earphones to fine-tune the position of the microphone.

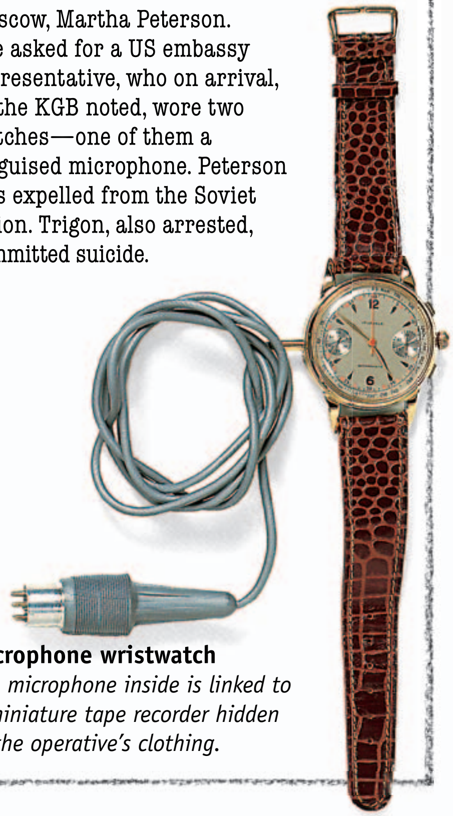
Receivers I

LISTENING IN ON AND RECORDING conversations is an important part of surveillance; its usual end product is a tape recording. Bugs (see p. 110 and p. 112) are hidden listening devices that either transmit a conversation to a listening post some distance away or are connected to a recording device. Shown here are two further categories of audio-surveillance gear. The first is the equipment used at the listening post: radio receivers, tape recorders, and other electronic hardware. The second consists of the devices carried on the person of a spy to record a conversation on the spot. These are mostly miniaturized microphones and tape recorders. The earpiece microphone shown above is a variation on this theme, designed for making recordings of telephone conversations.

EARPIECE MICROPHONE

TRIGON AND PETERSON

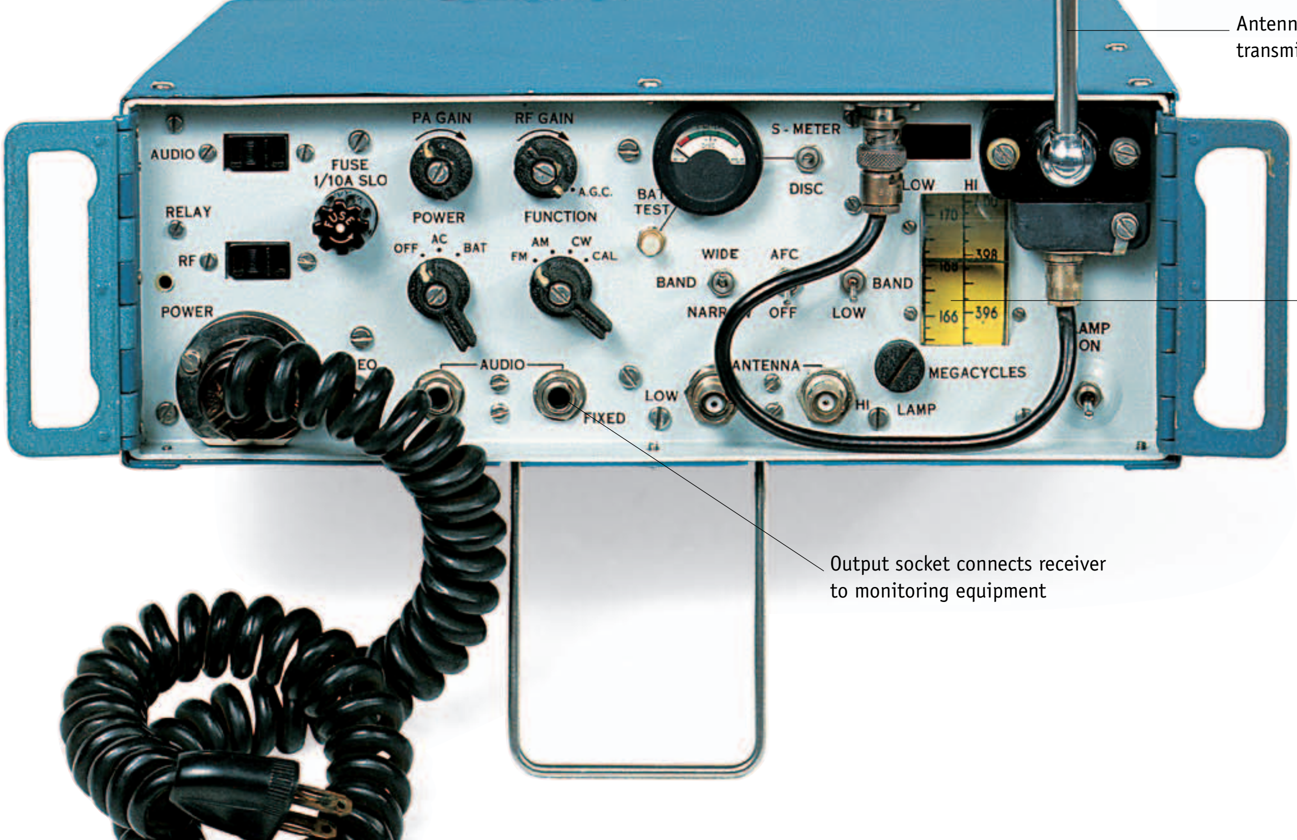
Alexsandr Ogorodnik, codenamed Trigon, was a Soviet diplomatic service secretary who supplied information to the CIA from 1974 (see p. 61). In July 1977, the KGB arrested his CIA case officer in Moscow, Martha Peterson. She asked for a US embassy representative, who on arrival, as the KGB noted, wore two watches—one of them a disguised microphone. Peterson was expelled from the Soviet Union. Trigon, also arrested, committed suicide.



Microphone wristwatch
The microphone inside is linked to a miniature tape recorder hidden in the operative's clothing.

Listening post receiver

This is a portable American-made radio receiver, designed in the 1960s. Its function was to receive signals from bugs in a target location nearby. Its output was carried by cable, either to a tape recorder or to other types of monitoring equipment.



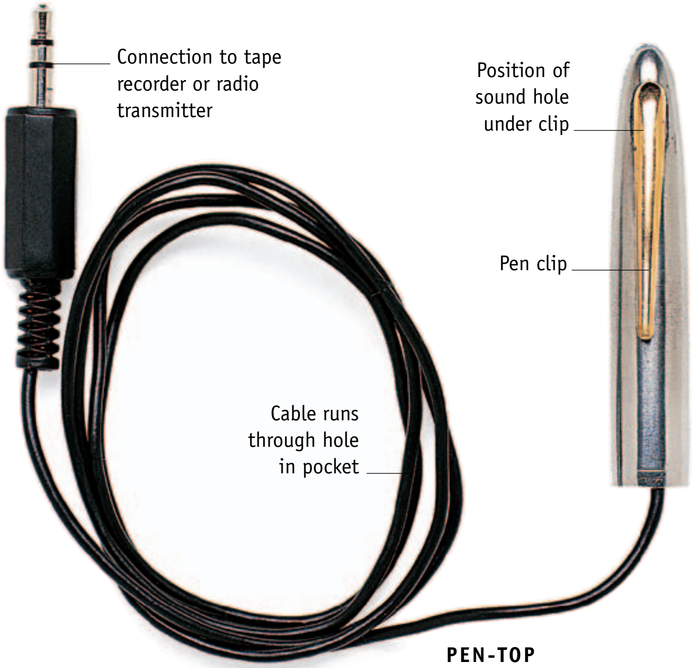
Pen with microphone

The KGB had fountain pens made that contained small microphones, allowing spies to record conversations. The signal was passed to a small tape recorder or transmitter hidden in the spy's clothing. A selection of different styles of pens was available to match the different types of cover under which spies operated.

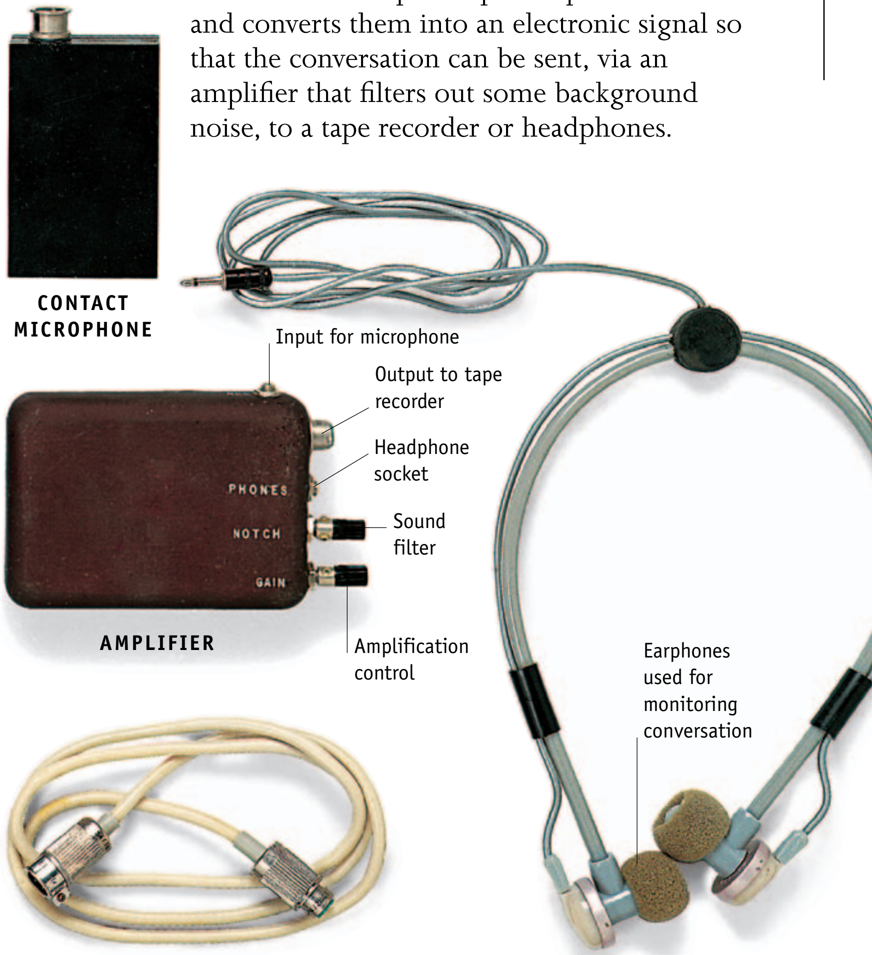
MICROPHONE IN POSITION

"Motel kit"

The contact microphone of this CIA kit is taped or glued to a wall or door and lets the user eavesdrop on a conversation in the next room. The microphone picks up sound waves and converts them into an electronic signal so that the conversation can be sent, via an amplifier that filters out some background noise, to a tape recorder or headphones.


Connection to tape recorder or radio transmitter
Position of sound hole under clip
Pen clip
Cable runs through hole in pocket

PEN-TOP MICROPHONE



CONTACT MICROPHONE

AMPLIFIER

LEAD TO TAPE RECORDER

HEADPHONES

KANG SHENG AND THE CHINESE SECRET SERVICE

During the 1920s, the fledgling Chinese Communist Party formed its own secret police force in imitation of the Soviet OGPU. The head of this organization (and its successor organization, the Social Affairs Department, or SAD) was Kang Sheng (1898–1975). Kang lived the life of a gentleman scholar and calligrapher while holding secret police and Communist Party security posts for more than 40 years. After the formation of the communist government under Mao Zedong in 1949, Kang managed to attain ever greater powers. He went on to reinforce his position by fostering the personality cult of Mao Zedong, and ensuring that Mao married Jian Qing, a former lover of Kang's. From his base in Beijing, which was known as the "Bamboo Garden", Kang monitored almost everything that happened in China. This included surveillance of members of the Communist Party itself. He used a wide variety of electronic eavesdropping devices to achieve this, and is even believed to have bugged the private office of Mao Zedong himself.

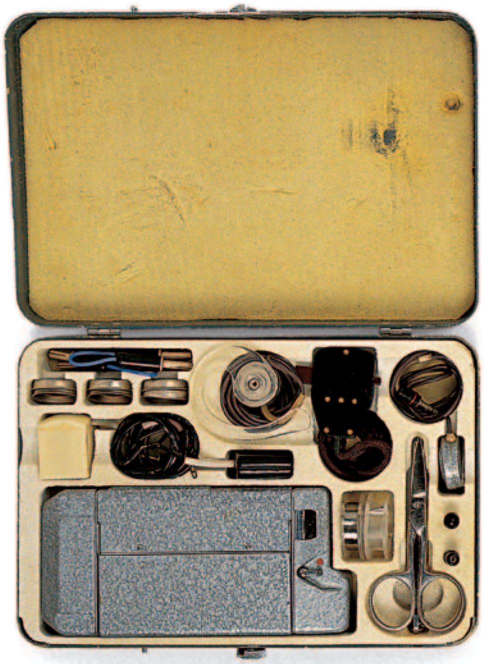
In the 1970s, when Kang was growing weak due to cancer, SAD began to extend its activities to other countries. The organization was able to earn hard currency by carrying out industrial espionage in foreign countries. SAD also helped enhance China's political influence by helping such groups as the Shining Path in Peru and the PLO in the Middle East.

KANG SHENG

Receivers II

Mezon recording device

The Mezon, which dates from the 1970s, records sound on a wire 0.05 mm in diameter instead of a tape. The KGB issued accessories adapting it for a variety of operational situations. It could be controlled by a remote switch concealed in the pocket, and included an attachment for recording telephone conversations. Screw plugs ensure the accessories will not become unplugged while in use. A shoulder harness allows the Mezon to be worn under a jacket.



COMPLETE OUTFIT IN CASE

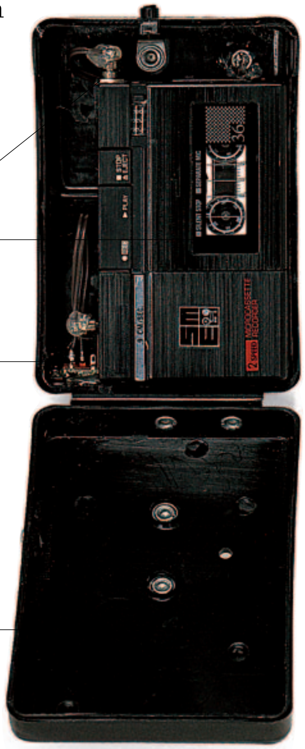
Microphone can be pinned beneath lapel to record conversations

Plug

MEZON MICROPHONE

Pager with concealed recorder

A tiny tape recorder and microphone are concealed in this American-made fake pager from the 1990s. Worn on the user's belt, the machine is operated by an on/off switch at the bottom.

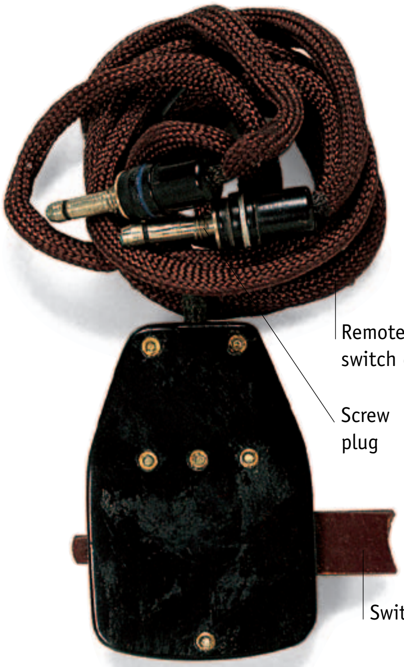


Microphone plug

Credit-card-sized tape recorder

On/off switch

Casing of fake pager opens to enable cassette to be changed

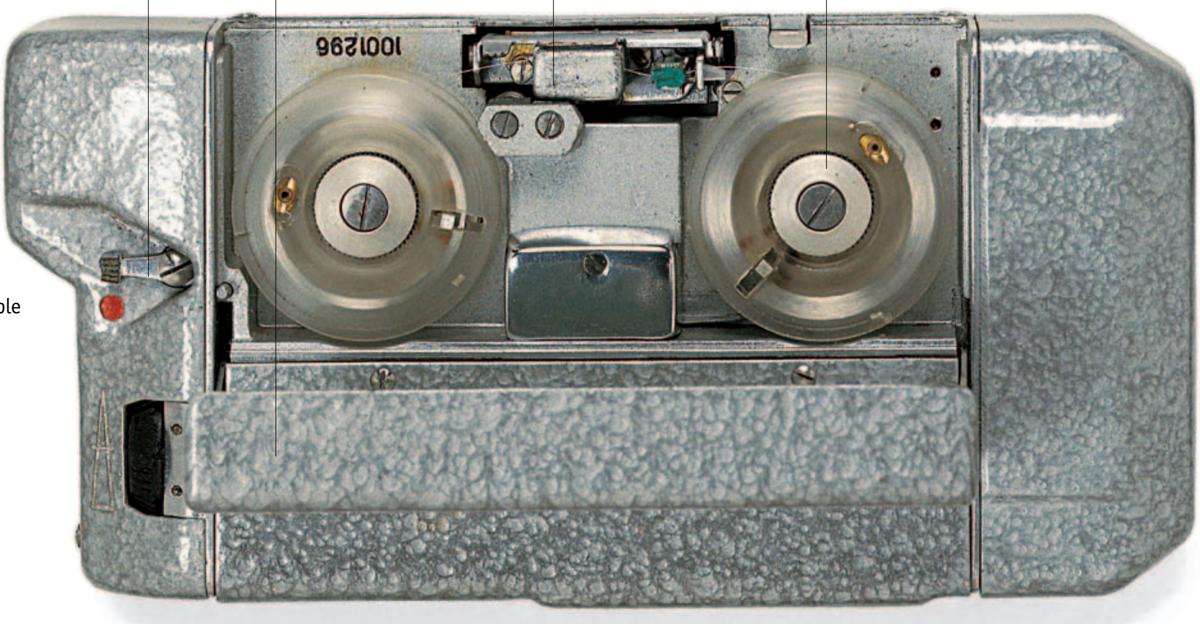


Remote switch cable

Screw plug

Switch

REMOTE ON/OFF SWITCH



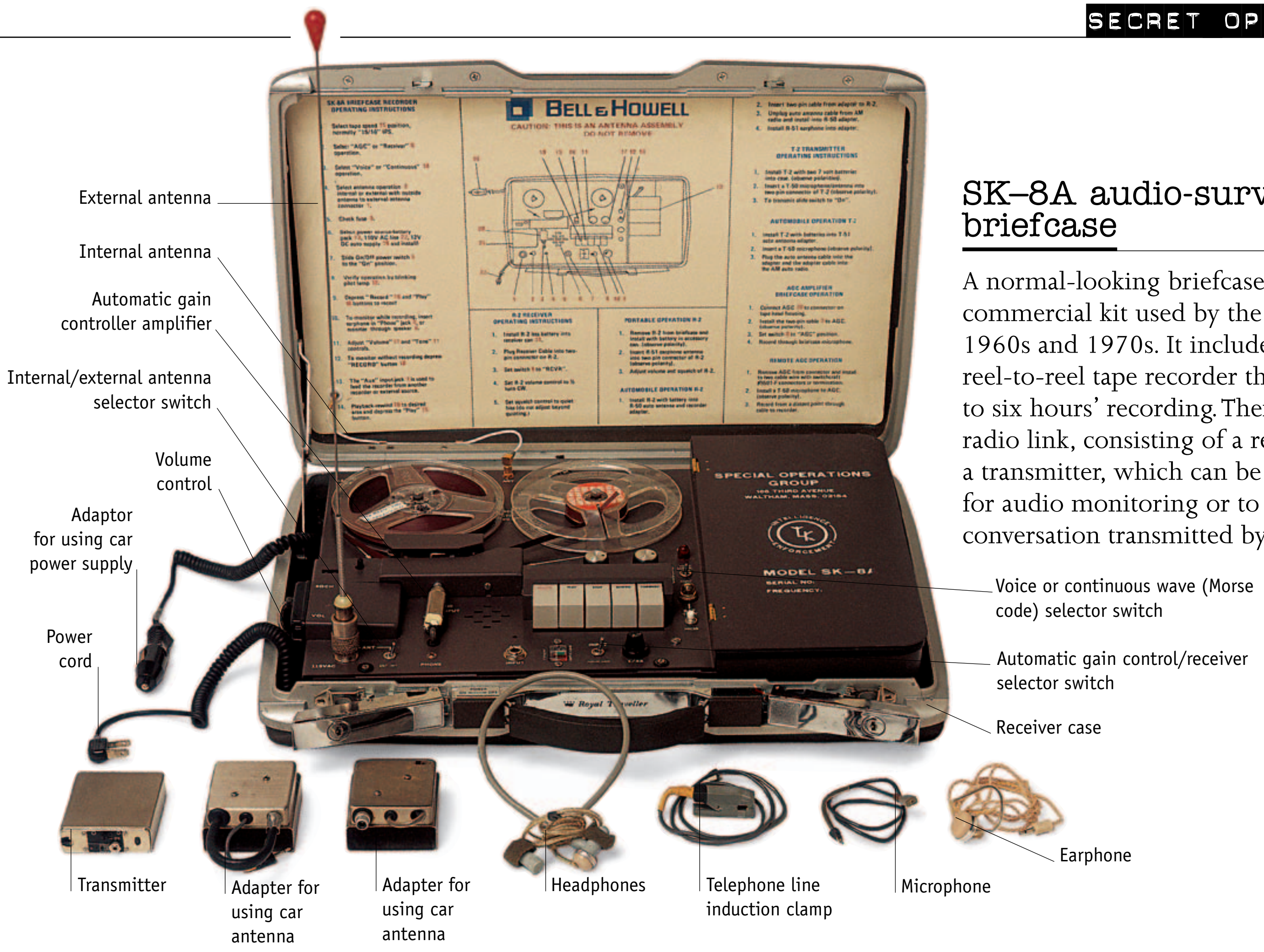
On/off lever

Lid can be closed for protection during use

Recording head

Wire spool

MEZON RECORDING DEVICE (ACTUAL SIZE)

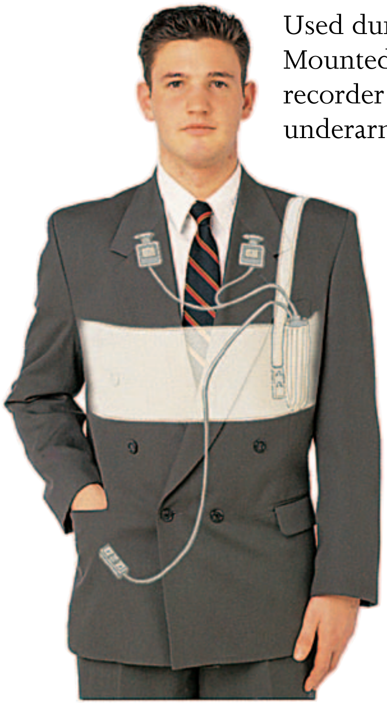

BELL & HOWELL
SPECIAL OPERATIONS GROUP
MODEL SK–8A
External antenna
Internal antenna
Automatic gain controller amplifier
Internal/external antenna selector switch
Volume control
Adaptor for using car power supply
Power cord
Voice or continuous wave (Morse code) selector switch
Automatic gain control/receiver selector switch
Receiver case
Transmitter
Adapter for using car antenna
Adapter for using car antenna
Headphones
Telephone line induction clamp
Microphone
Earphone

SK–8A audio-surveillance briefcase

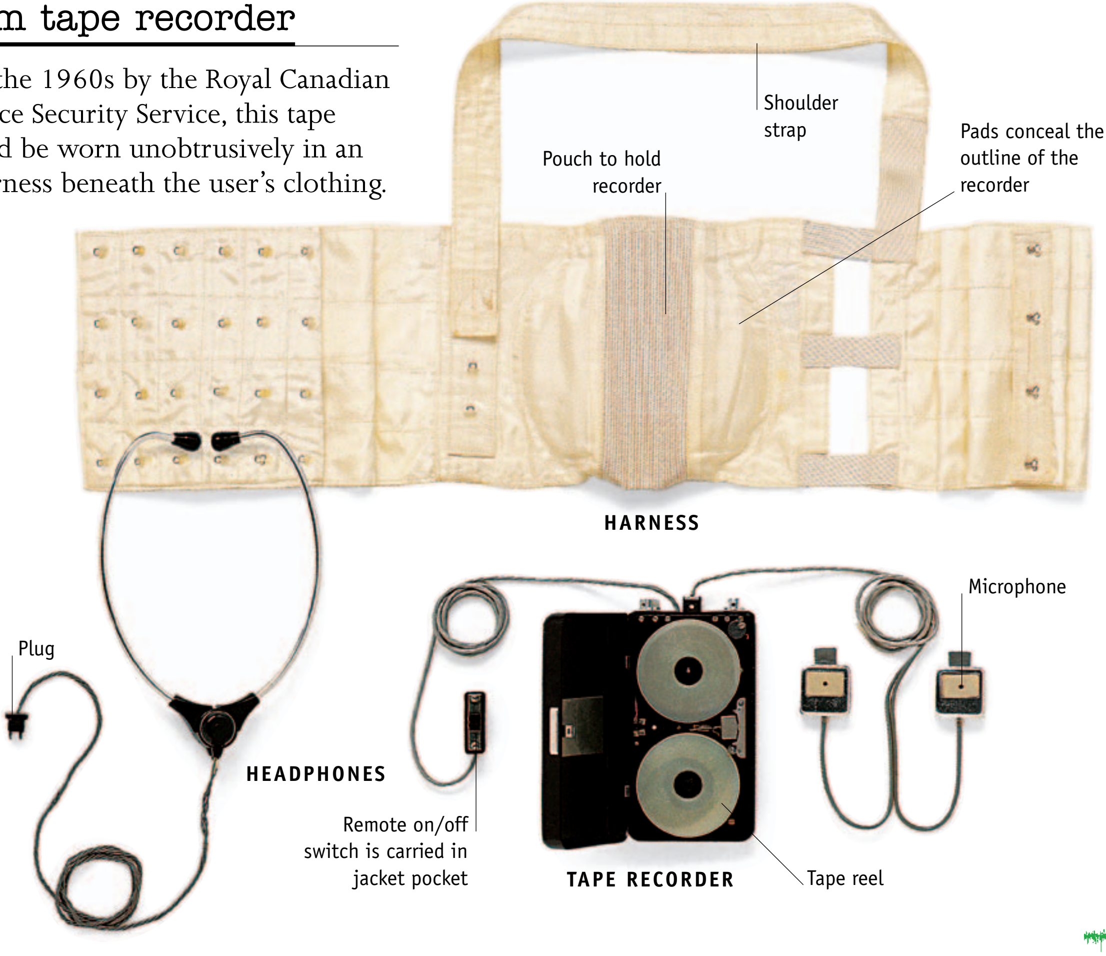
A normal-looking briefcase conceals this commercial kit used by the CIA in the 1960s and 1970s. It includes a low-speed reel-to-reel tape recorder that allows up to six hours' recording. There is also a radio link, consisting of a receiver and a transmitter, which can be used either for audio monitoring or to record a conversation transmitted by a bug.

Underarm tape recorder

Used during the 1960s by the Royal Canadian Mounted Police Security Service, this tape recorder could be worn unobtrusively in an underarm harness beneath the user's clothing.

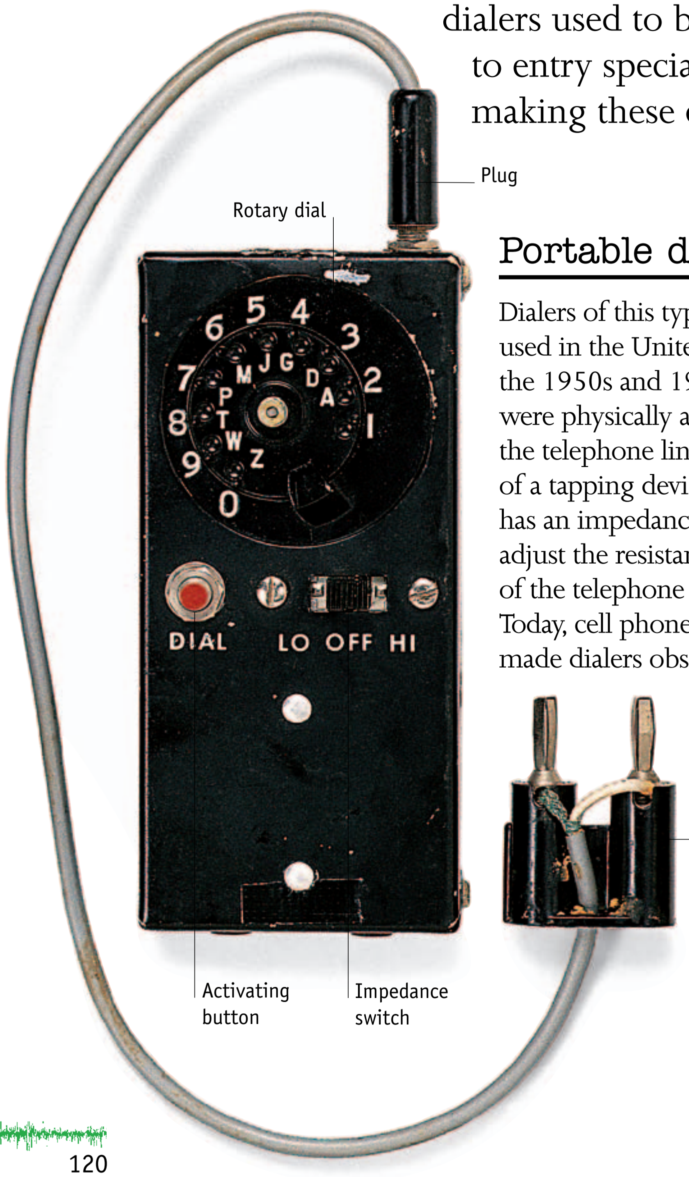


Demonstration of harness
The special harness was padded to the arm made by the tape recorder.



Surreptitious entry

INTELLIGENCE AGENCIES need personnel who can enter places secretly to gather intelligence. Such surreptitious entries require very careful planning, and are usually carried out by expert personnel using special equipment. Picking locks is avoided if possible, because it is difficult and unpredictable. It is better to steal a key and quickly duplicate it. If no key is available, it is possible to manufacture one with a special key-impression kit. Once burglar alarms have been neutralized, the final safeguard before entry is to ensure that the target location is unoccupied. One way to do this is to telephone: if anyone answers, the operation is canceled. Portable dialers used to be issued to entry specialists for making these calls.

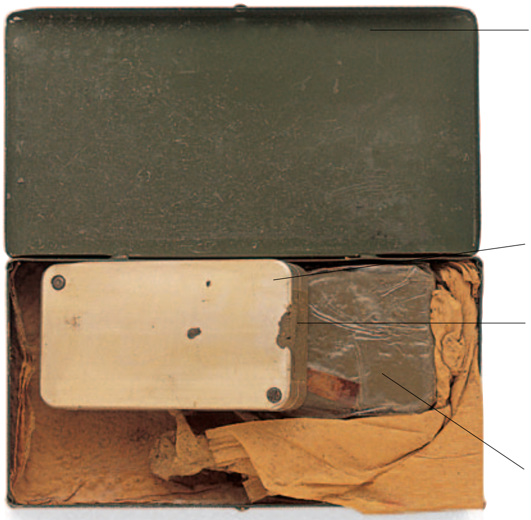


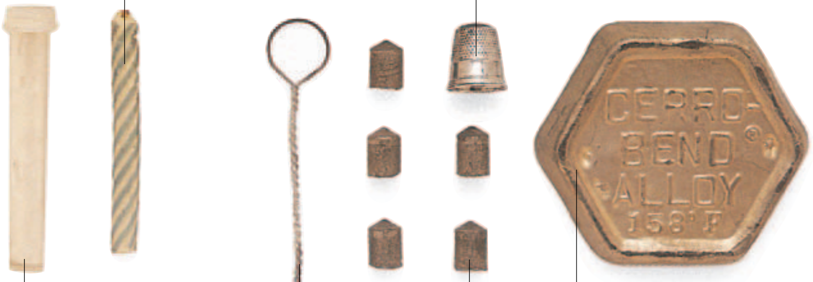
Portable dialer

Dialers of this type were used in the United States in the 1950s and 1960s. They were physically attached to the telephone line by means of a tapping device. This one has an impedance switch to adjust the resistance to that of the telephone circuit. Today, cell phones have made dialers obsolete.

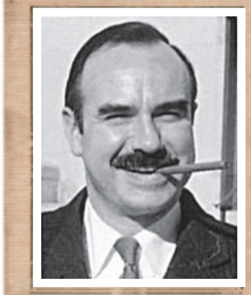
CIA key-casting kit

It may be possible to steal a key temporarily, returning it to avoid detection. Its impression is instantly taken in clay and a quick copy made, using a low-melting-point metal alloy that melts in a candle flame. A permanent copy can be cut later.


Carrying case
Aluminum mould containing modelling clay
Hole for pouring molten alloy into mould
Spare modelling clay



G. GORDON LIDDY

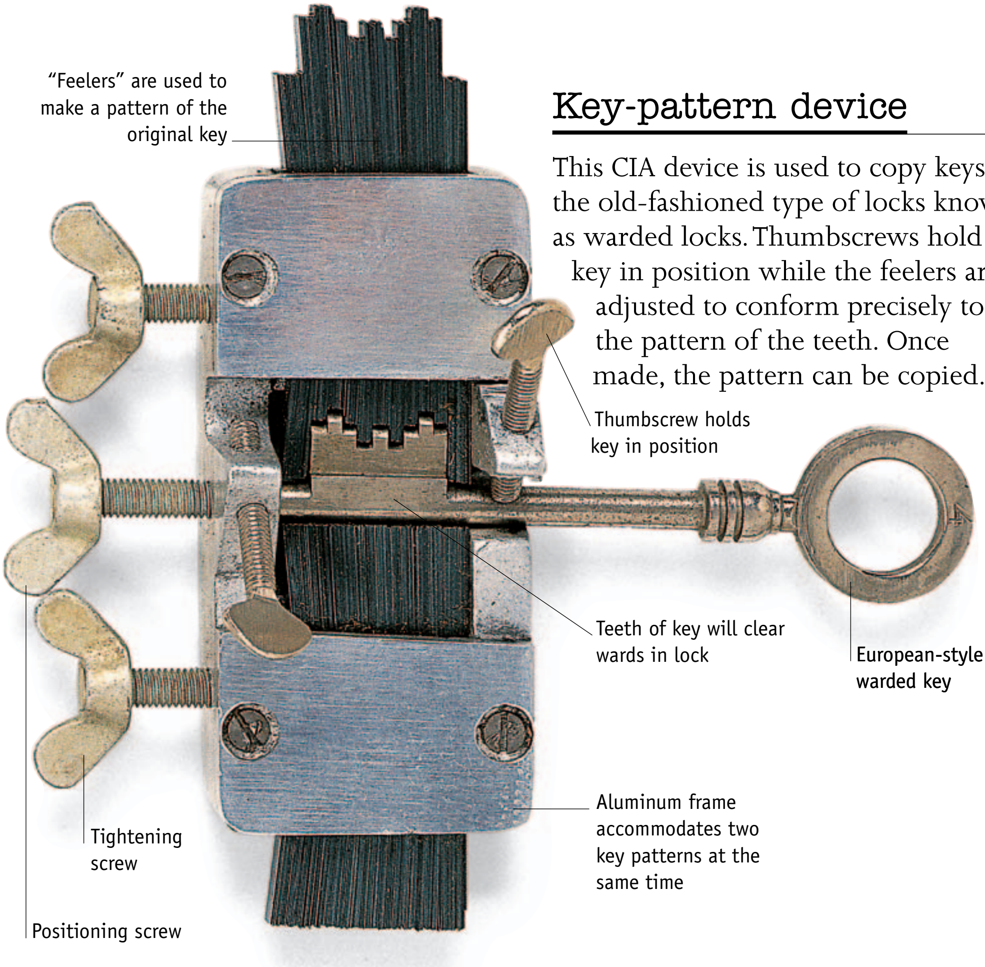


SPY PROFILE

Formerly an FBI special agent and an attorney, G. Gordon Liddy (b.1930) was one of the central figures involved in the 1972 Watergate break-in (see p. 122). In the previous year he had taken part in the surreptitious entry at the residence of the psychiatrist treating a prominent Vietnam War protester. Liddy used a Minox C camera and a measuring chain (see p. 94) to help identify the lock types and keyways at the apartment.

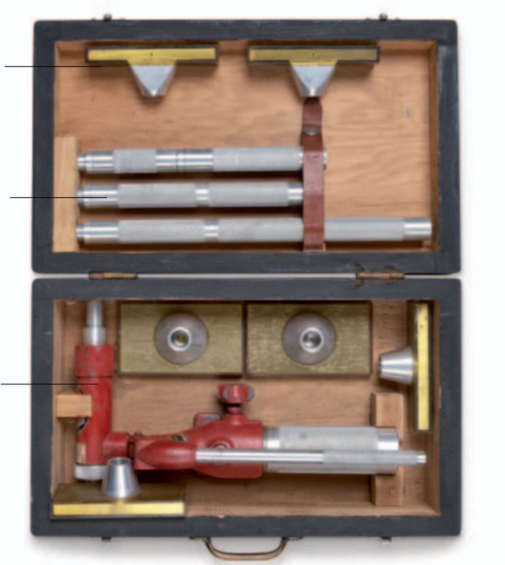
Key-pattern device

This CIA device is used to copy keys of the old-fashioned type of locks known as warded locks. Thumbscrews hold the key in position while the feelers are adjusted to conform precisely to the pattern of the teeth. Once made, the pattern can be copied.


"Feelers" are used to make a pattern of the original key
Thumbscrew holds key in position
Teeth of key will clear wards in lock
European-style warded key
Aluminum frame accommodates two key patterns at the same time
Tightening screw
Positioning screw

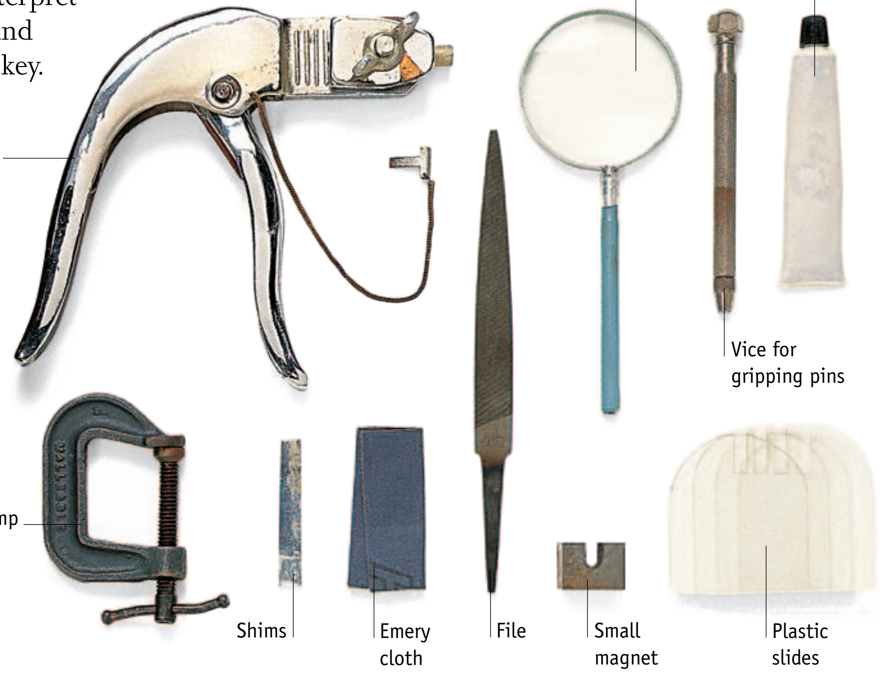
Door spreader

Most doors can be opened using a hydraulic jack to spread the sides apart enough to release the lock bolt. Burglars first used small car-jacks and extensions to bypass locking systems. MI6 improved on this and packaged all the components into a small, easily transportable kit.



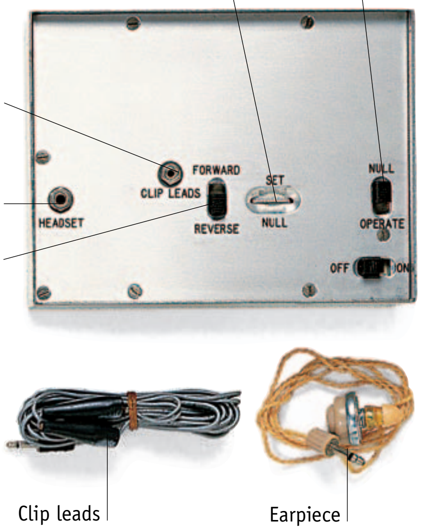
Key-impression kit

This commercial kit used by the CIA works for a variety of keys. A specially prepared impression tool inserts a key blank into the lock and picks up marks from the mechanism. An expert can interpret these marks and hand-file the key.



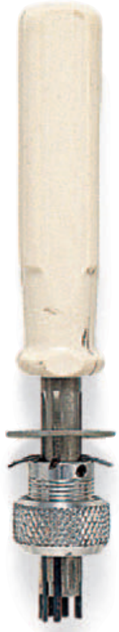
Burglar alarm evasion kit

Old alarms used a wire-borne signal; if this was broken, the alarm was raised. With this kit, CIA agents could intercept the signal, tamper with the wire, and prevent a break-in from being detected.



Lockpicks

INTELLIGENCE SERVICES OFTEN NEED to pick locks to gain access to secret material. Lockpicking devices, and kits with small tools, are available for opening most types of lock used worldwide. To open a pin-tumbler lock, a pick tool and a tension wrench are inserted and manipulated to simulate the results that would be obtained by using the key. The spy may have to try several tools before the lock will open. For faster results, a lockpicking "gun" or electric lock-opening device may be used. Lockpicking is a specialized branch of intelligence work, but it uses the same tools as commercial locksmiths.

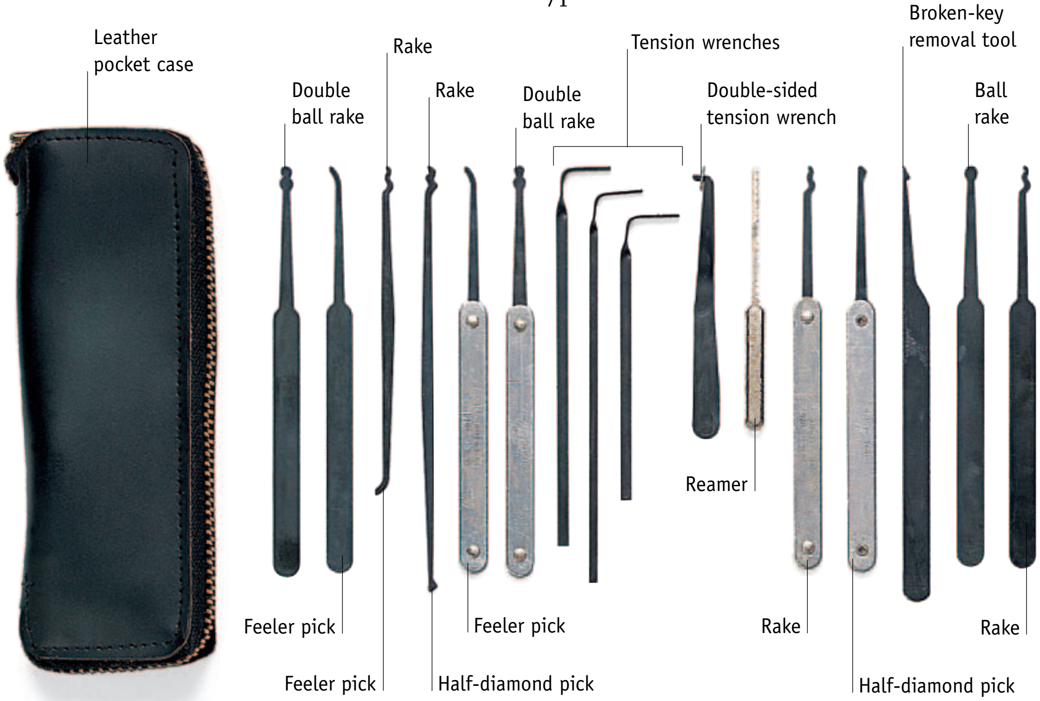


Tubular lockpick

This commercial device used by the CIA opens the type of high-security locks that use a tubular key. It is inserted and adjusted within the lock to simulate the tubular key.

Pocket lockpicking kit

This commercially available assortment of picks and tension tools used by the CIA is small enough to put in a pocket. In expert hands it opens most kinds of pin-tumbler lock—the most common type of lock in the world.



THE WATERGATE BREAK-IN

The 1972 Watergate break-in was part of an illegal plot in support of the reelection of US President Richard Nixon. The headquarters of Nixon's rival, the Democratic candidate George McGovern, were located in the Watergate office complex in Washington, DC. A White House aide, E. Howard Hunt, Jr., recruited a group of Cuban exiles to break into the building. In their first entry, the Cuban team photographed various documents and installed a number of listening devices.

A second entry was undertaken to gather more information and reposition one of the listening devices. But the burglars were inexperienced lockpickers and this entry was discovered by a night watchman—tape holding a door lock open had been left visible from the outside.

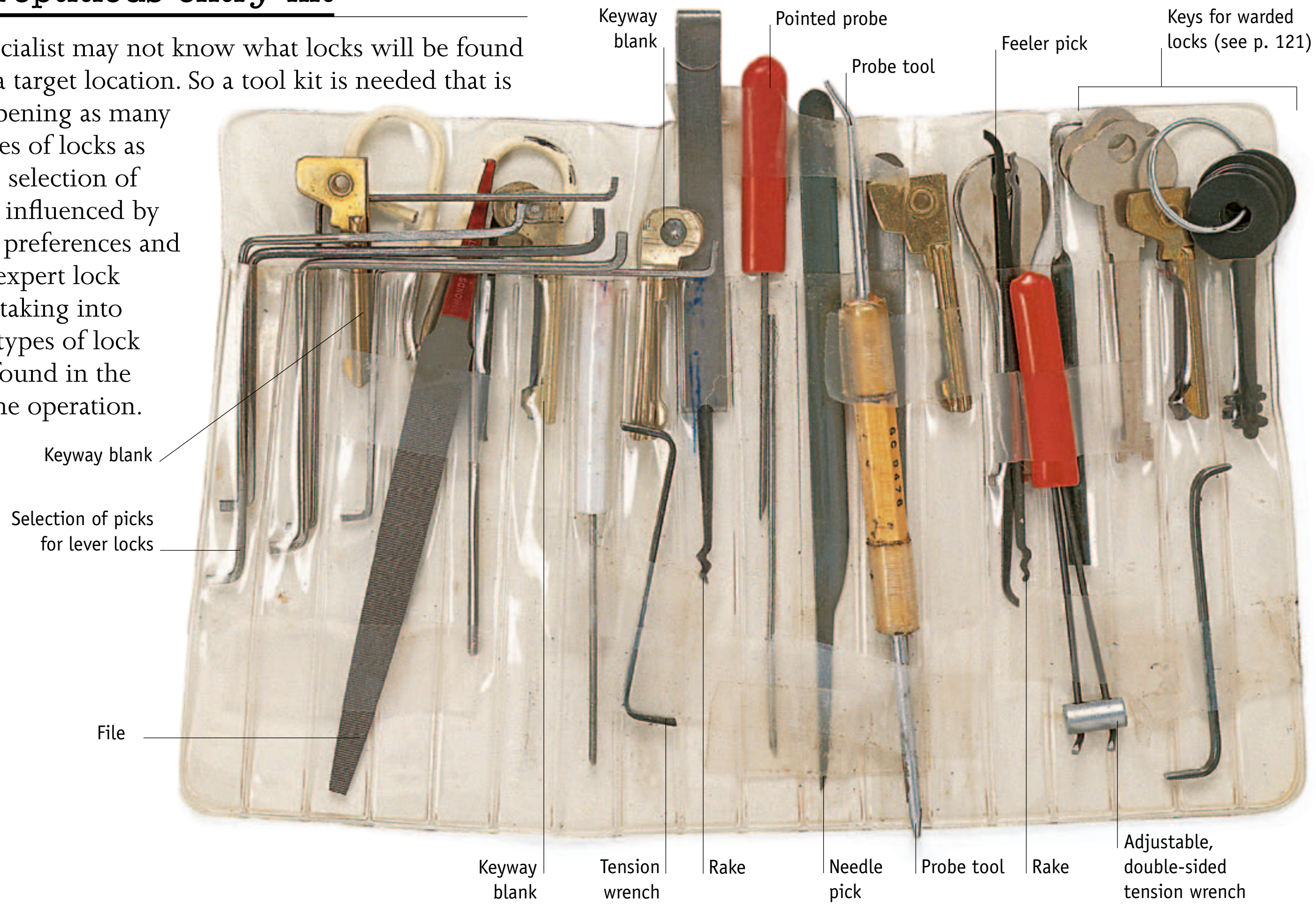
The police were called, and they arrested the Cubans. Later, the two men responsible for planning the operation, Hunt and G. Gordon Liddy (see p. 120), were also arrested, tried, and convicted. The Watergate scandal led to the resignation of President Nixon.

The Watergate burglars
The men recruited to carry out the burglary in the Watergate office complex were exiles from Fidel Castro's communist regime in Cuba.

E. Howard Hunt, Jr.
A former CIA officer, Hunt (1918–2007) recruited the Watergate entry team using his contacts in the Cuban exile community.

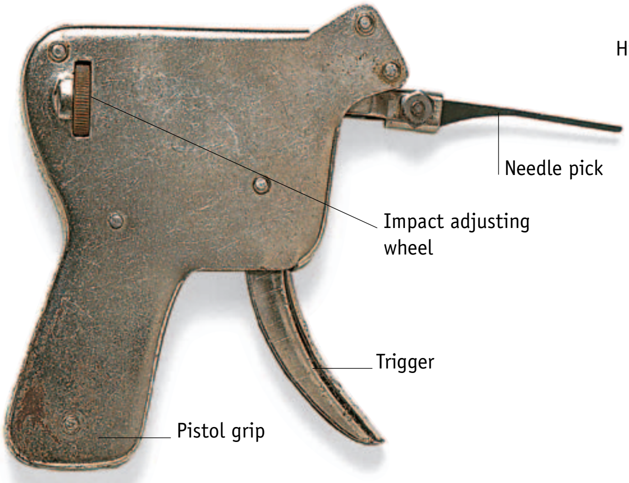
CIA surreptitious entry kit

An entry specialist may not know what locks will be found once inside a target location. So a tool kit is needed that is capable of opening as many different types of locks as possible. The selection of tools will be influenced by the personal preferences and skills of the expert lock opener, also taking into account the types of lock likely to be found in the country of the operation.



Lockpick gun

This commercial device used by the CIA opens pin-tumbler locks. Squeezing the trigger causes the pick to strike the pins that work the lock mechanism. A tension wrench is used to turn the lock cylinder when the pins are properly aligned.

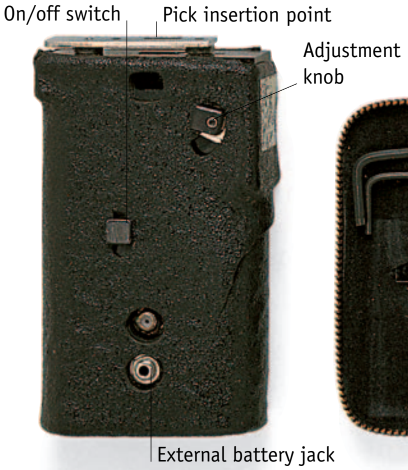


LOCKPICK GUN

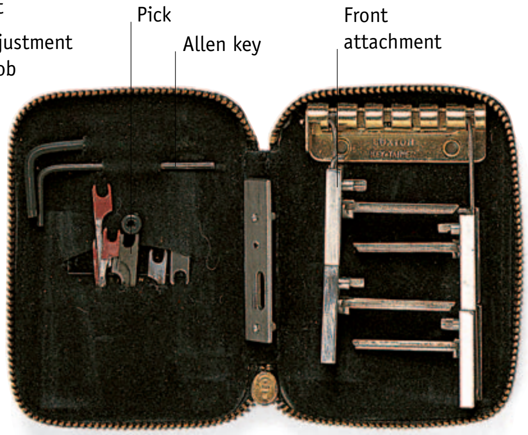
TENSION WRENCH

CIA electric lock-opening device

The user selects a pick, inserts one end in the device and the other in the lock, then switches the device on. This bounces the pins in the lock until they are aligned, so the lock opens. No additional tool is needed to turn the lock cylinder.



LOCK-OPENING DEVICE



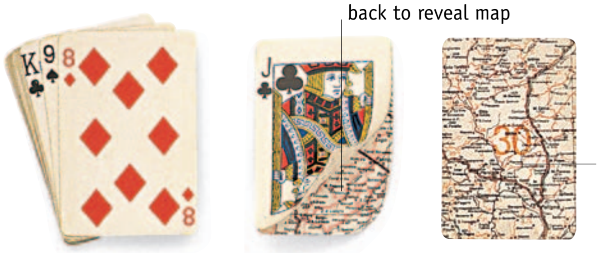
ATTACHMENTS IN CARRYING CASE

Escape and evasion

EVERYDAY ITEMS SUCH as hairbrushes made ideal concealments for World War II escape and evasion aids, including compasses and maps. They were developed to assist prisoners of war in escape attempts, and help spies and airmen operating in enemy territory evade capture. Most of the devices here were made by MI9, an office in British intelligence set up in 1940 to help prisoners of war escape (see also p. 190).

MI9 playing cards with concealed map sections

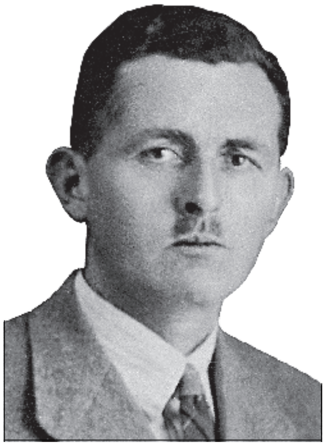
The top layer of these cards was soaked off to reveal numbered map sections. The assembled sections formed a master from which escape maps were copied.


Card surface peeled back to reveal map
Numbered map section fully revealed

THE MAN WHO WAS "Q"

Charles Fraser-Smith (1904-92) worked for British intelligence during World War II. His task was to supply the clandestine services with "Q" gadgets—named after Q-ships, the warships in World War I that had been disguised as ordinary merchant navy ships.

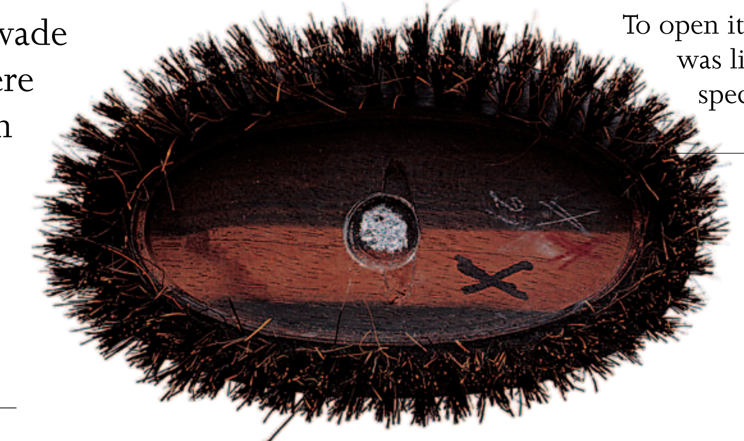
Many of his Q gadgets were concealments disguised as everyday objects. Others were items of equipment that had been miniaturized or adapted for concealment. Fraser-Smith employed over 300 companies, all of which were sworn to secrecy, to make his devices.



Charles Fraser-Smith
Fraser-Smith was the inspiration for the character "Q" in Ian Fleming's James Bond novels.

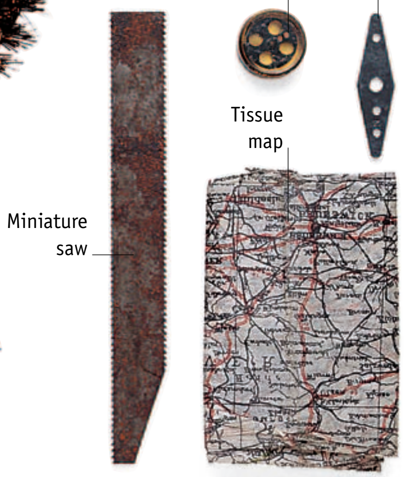
MI9 hairbrush with secret compartment

This hairbrush concealed a variety of vital escape and evasion aids. To open it, a section of the brush was lifted by pulling on a specific row of bristles.



HAIRBRUSH

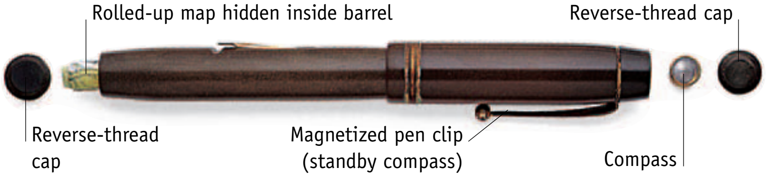
LIFTED-OUT SECTION OF HAIRBRUSH



ITEMS CONTAINED IN HAIRBRUSH

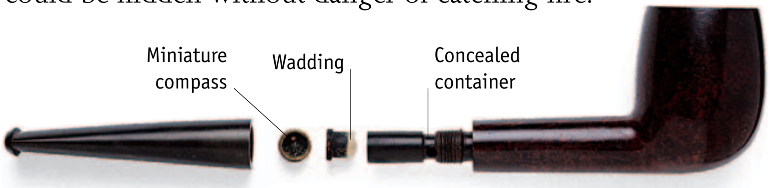
MI9 pen concealing map and compass

Secret chambers in this pen were secured with end caps attached by reverse threads. Any attempt to unscrew the caps in the normal (counterclockwise) direction merely tightened them.

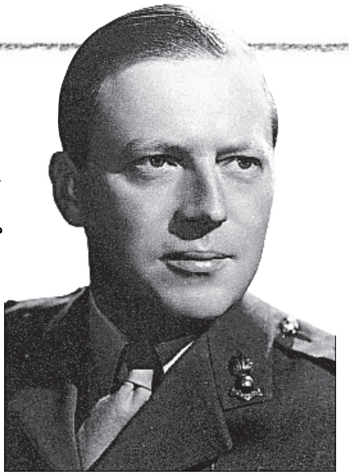

Rolled-up map hidden inside barrel
Reverse-thread cap
Reverse-thread cap
Magnetized pen clip (standby compass)
Compass

MI9 pipe with concealments

This pipe could be smoked without damaging the concealed items. The bowl had an asbestos lining inside which a map could be hidden without danger of catching fire.

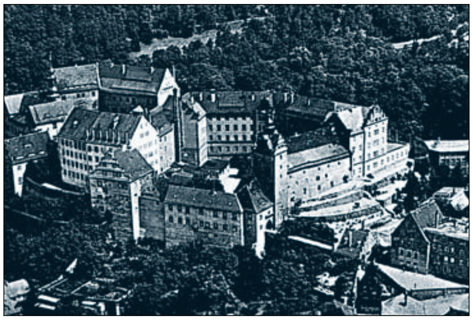


ESCAPE FROM COLDITZ CASTLE



Airey Neave (1916–17)
After his Colditz escape, Neave became an adviser on escape aids in order to assist other prisoners.

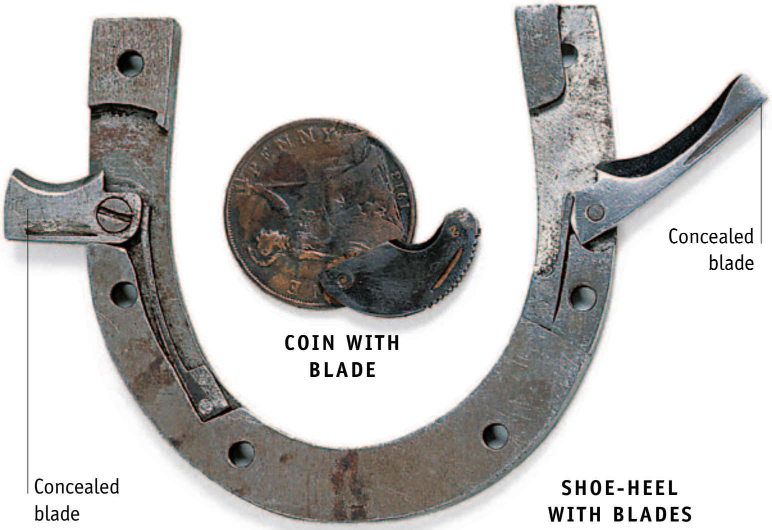
Colditz Castle, a historic fortress in eastern Germany, became a prison for high-risk Allied prisoners of war during World War II. Many of these had already escaped or tried to escape from German captivity, and by concentrating them at Colditz, the Germans unwittingly created what became known as the Colditz Escape Academy. A group of prisoners coordinated escape attempts and made, by hand, a range of items, such as clothes and forged documents, to supplement escape aids that were smuggled into Colditz from Britain. In January 1942, an escape by British Lieutenant Airey Neave and Dutch Lieutenant Toni Luteyn involved disguising themselves as German officers and Dutch workers. On his return to England, Neave became an adviser to MI9. In 1979, when a Member of Parliament, he was killed by a bomb under his car. The Irish National Liberation Army (INLA) claimed responsibility for his murder.



Colditz Castle
The Nazis wrongly thought that this forbiddding fortress was escape-proof.

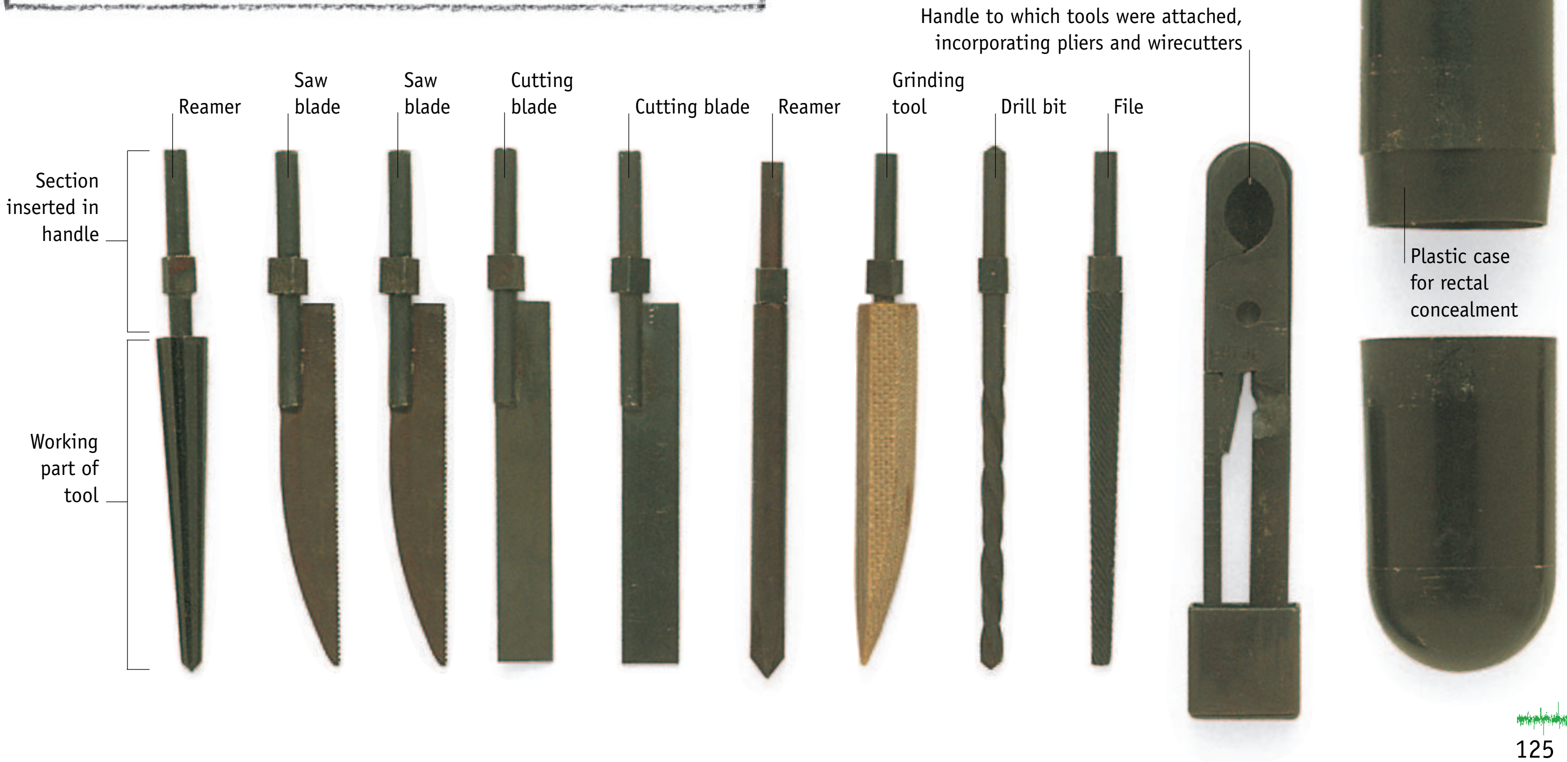
MI9 hidden blades

Small blades were hidden in objects that were unlikely to be confiscated from prisoners. A coin with a hidden blade, mixed with other pocket change, might easily be overlooked by the enemy. Shoe-heel blades could be used by prisoners whose hands were tied to their feet and behind their back.



Rectal tool kit

Escape tools and ways of concealing them continued to be needed in the years after World War II. This CIA kit from the 1960s was designed for rectal concealment if a search was anticipated.



Handle to which tools were attached, incorporating pliers and wirecutters
Reamer
Saw blade
Saw blade
Cutting blade
Cutting blade
Reamer
Grinding tool
Drill bit
File
Section inserted in handle
Working part of tool
Plastic case for rectal concealment

Sabotage I

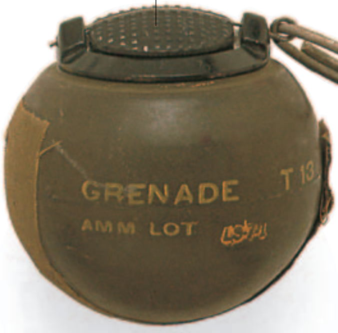
ACTS OF SABOTAGE aim to disable part of an enemy's infrastructure. Sabotage operations are usually carried out for one of two reasons: to damage the economies of potentially hostile countries during peacetime, or to disrupt an enemy's industry and communications during wartime. Wartime attacks not only cause destruction, but also force the enemy to divert troops from the front line to guard vulnerable areas. During World War II, both the SOE (see p. 30) and the OSS (see p. 32) were engaged in sabotage in cooperation with resistance groups. These operations often entailed the use of specialized explosives and fuses, such as bombs disguised as pieces of coal.

Tree spigot mortar

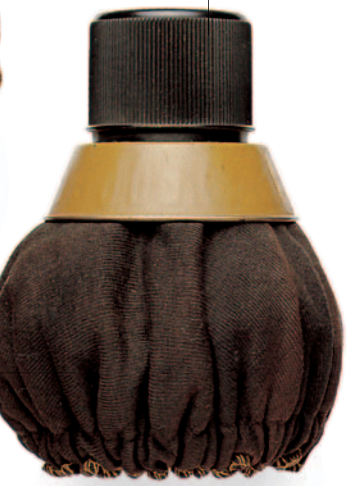
This unusual SOE device was meant for use against both vehicles and individuals. A trip wire set off the mortar, which hurled a shell filled with high explosive toward the target. The shell exploded on impact.

Grenades

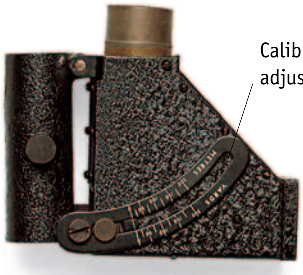
Unlike most grenades, which have time-delay fuses, these grenades explode on impact, making them effective against hard-to-hit moving targets. (The name "gammon" is a British word for ham.)



CIA BEANO GRENADE

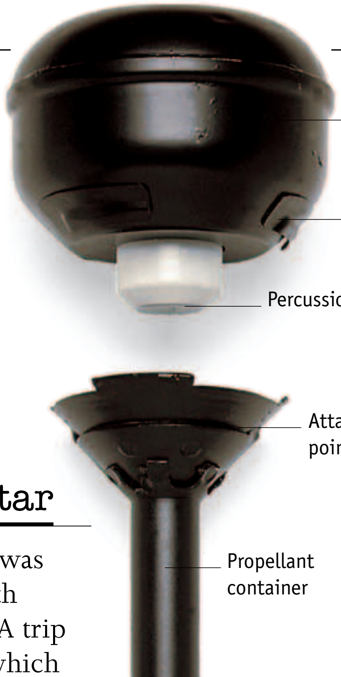


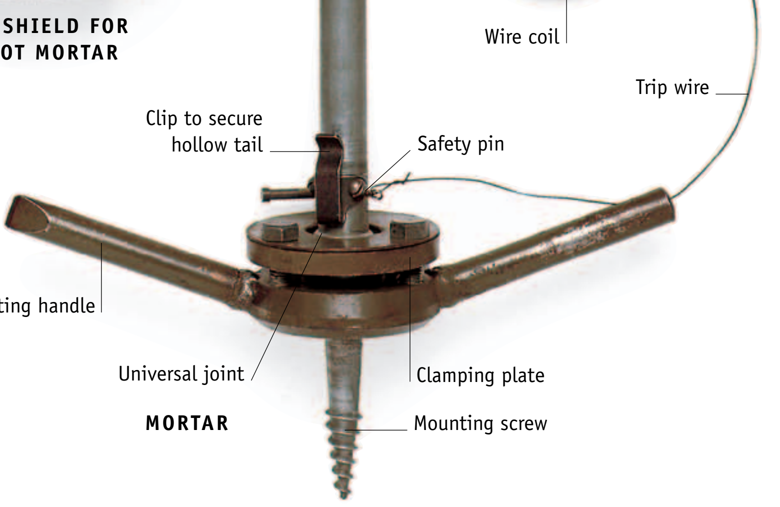
GAMMON GRENADE (BRITISH SPECIAL FORCES)



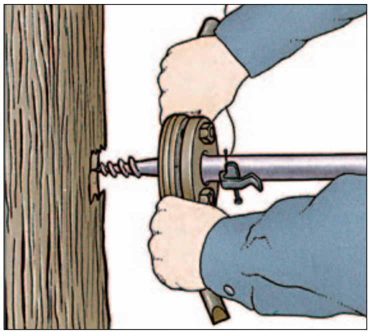
PRISMATIC SIGHT FOR SPIGOT MORTAR

RAIN SHIELD FOR SPIGOT MORTAR





MORTAR

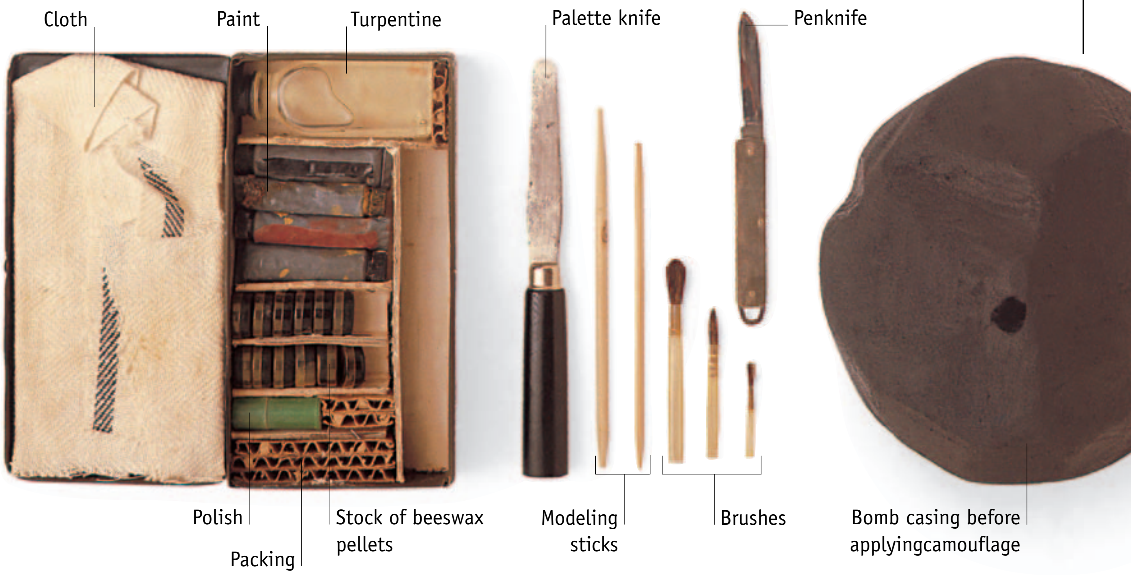


Mounting the spigot

The mortar was set up by screwing the spigot into a tree trunk, then pointing it in the direction the enemy was to approach from. The hollow tail was fitted over the spigot, and the shell was placed in a funnel at the the top of the hollow tail.

Explosive coal kit

Kits for disguising explosives as pieces of coal were issued to some OSS sabotage teams during World War II. These kits contained all that was needed to make the outer case of the bomb resemble the type of coal used in the operational area. The case was filled with explosive and placed in an enemy coal dump—these were often inadequately guarded. The bomb would detonate when burned in a locomotive's furnace or a factory boiler.



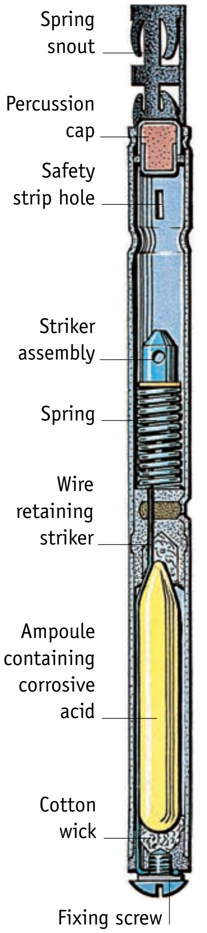
CODENAME PASTORIUS

In 1942, eight German saboteurs were put ashore from two submarines on the American coast. Their mission was codenamed Pastorius. Four landed in Florida and four in Long Island, New York. The Coast Guard spotted the New York group and alerted the FBI, who searched the beach and found explosives and fuses. One saboteur, Georg Dasch, surrendered to the FBI. He provided information that resulted in the arrest of the others. Six of the saboteurs were sentenced to death and executed. Dasch and one other were given jail sentences and sent home after the war.

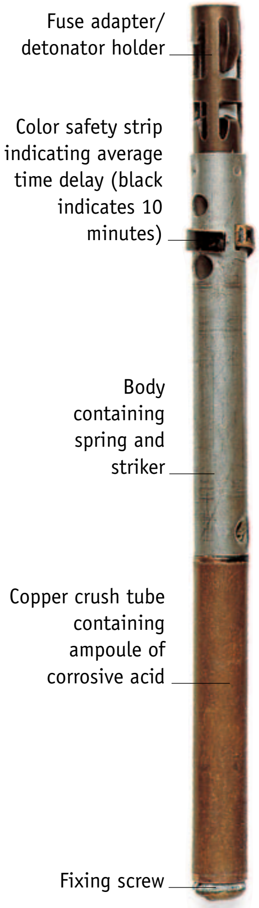
Georg Dasch (1903–92)
In order to save himself from execution, Dasch provided information that led to the arrest of his fellow saboteurs.

OSS pencil fuses

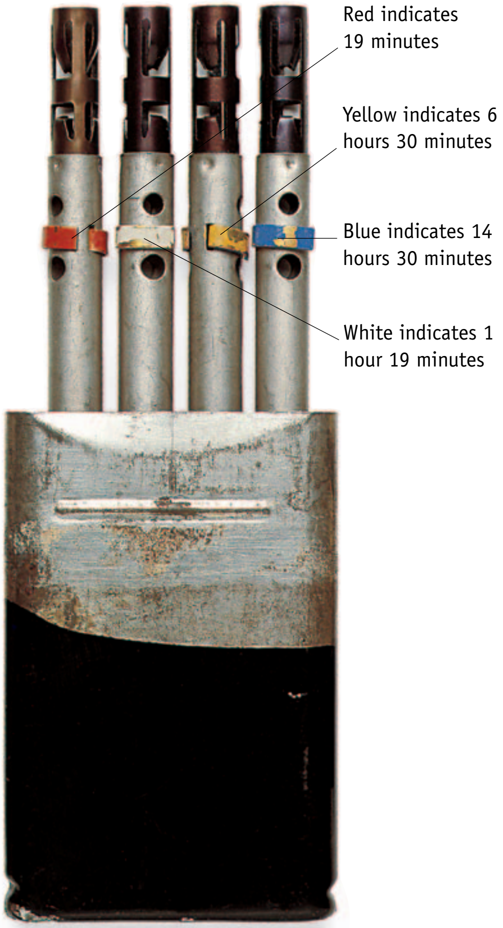
These World War II devices would detonate an explosive after a set time, giving a saboteur time to get away. The saboteur pulled off a safety strip and squeezed the appropriate point on the side of a copper crush tube, which broke an ampoule of acid inside. The acid corroded a wire to release a striker that struck a percussion cap and a detonator. Colored bands indicated the length of time delay for each fuse.



INTERNAL VIEW OF A PENCIL FUSE


Fuse adapter/ detonator holder
Color safety strip indicating average time delay (black indicates 10 minutes)
Body containing spring and striker
Copper crush tube containing ampoule of corrosive acid
Fixing screw

PENCIL FUSE


Red indicates 19 minutes
Yellow indicates 6 hours 30 minutes
Blue indicates 14 hours 30 minutes
White indicates 1 hour 19 minutes

BOX OF PENCIL FUSES

Sabotage II

Guard dog tranquillizers (CIA)

An agent can silence guard dogs by feeding them ground beef mixed with tranquillizer capsules. The animals are unharmed but may sleep for several hours. The typical dose for an average-sized dog is four capsules, but more may be necessary for particularly ferocious animals. When the agent has finished, a dose of antidote can be given to speed the dog's recovery.

TRANQUILLIZER CAPSULES

SINGLE DOSE OF ANTIDOTE

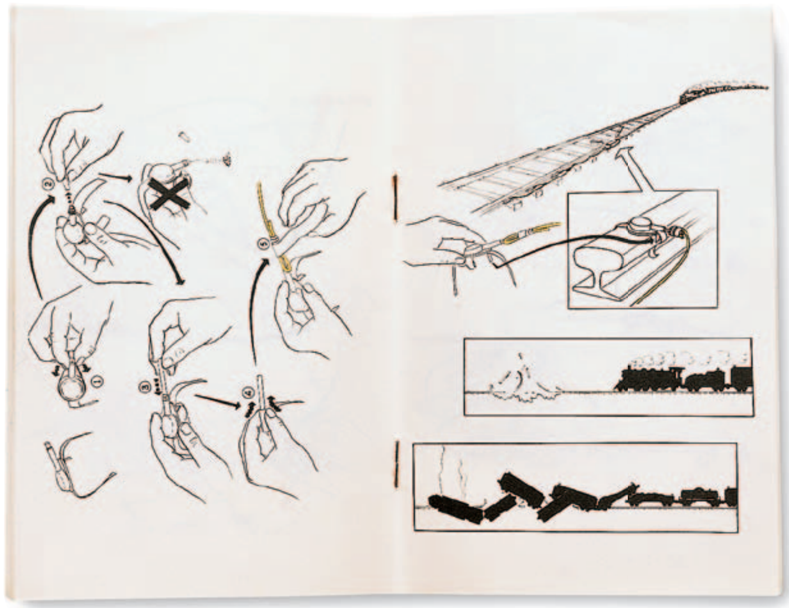
OPERATION MONGOOSE

In 1961, Attorney General Robert F. Kennedy and the White House directed the CIA to eliminate Cuban leader Fidel Castro and his government. The bold plan was code-named Operation Mongoose. Despite the Attorney General's personal involvement at all levels, the plan did not result in Castro's overthrow. Following the assassination of Robert's brother, President John F. Kennedy, in November 1963, covert operations against Castro continued for another two years before being abandoned (see p. 195).

ROBERT F. KENNEDY

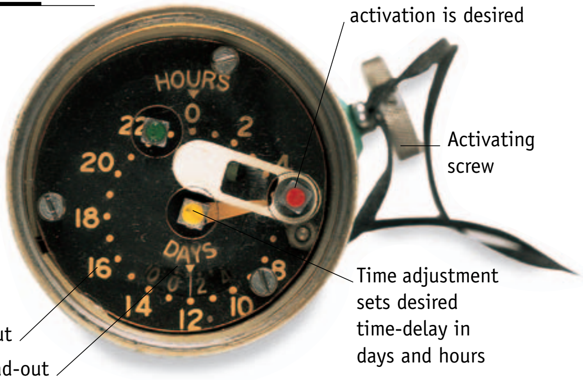
Sabotage booklet

The CIA produced pictorial sabotage booklets, to eliminate the language barrier. The pages below show how to assemble and plant a fog signal, a device used to set off a charge of high explosives for the demolition of trains. The device is activated by the wheels of the train passing over it.

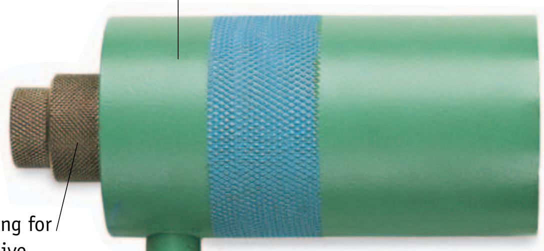


Thirty-day clockwork

This waterproof CIA 30-day clockwork incorporates a time-delay mechanism that can be used to detonate various types of explosive. The clockwork could be set to delay the explosion for any period between 1 hour and 30 days.


Time lock is kept on after setting until activation is desired
Activating screw
Time adjustment sets desired time-delay in days and hours
Hours read-out
Days read-out
HOURS
DAYS

TIME-DELAY MECHANISM



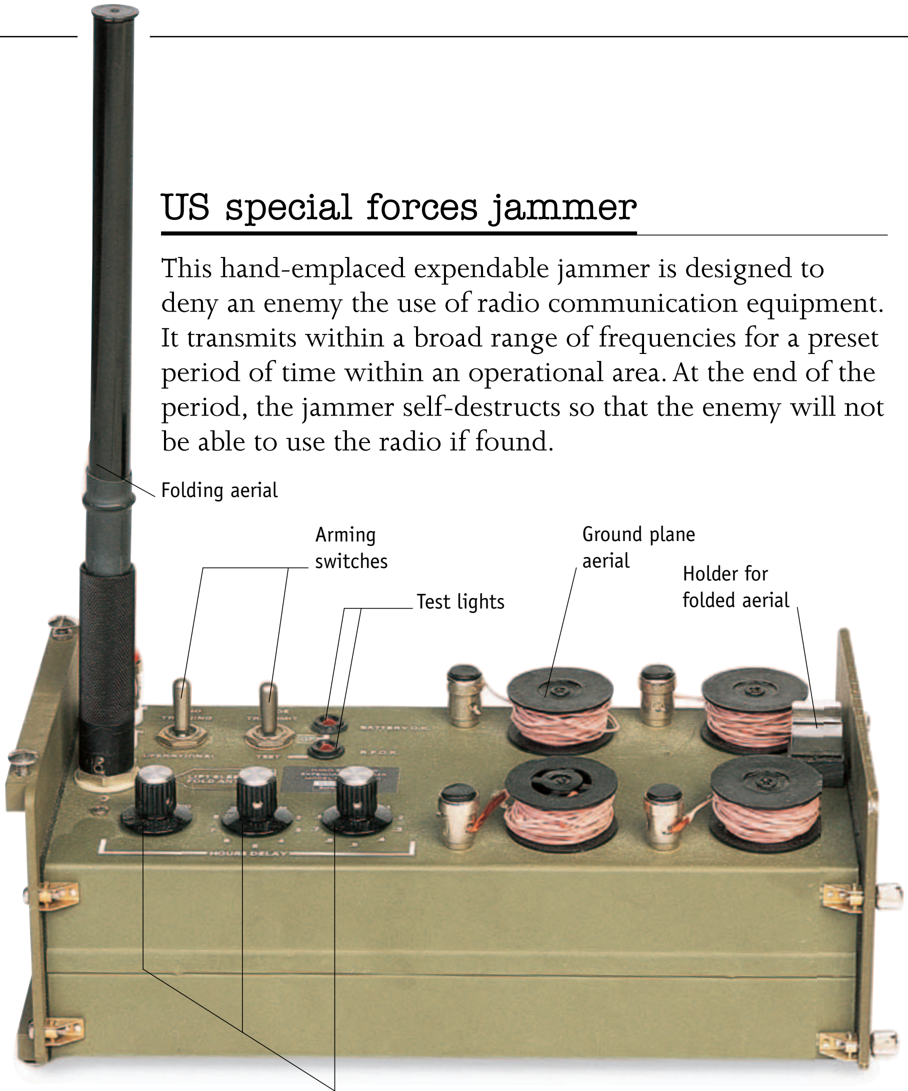
SIDE VIEW OF CLOCKWORK

END CAP

Activating screw to start timing
Winder for setting time-delay mechanism

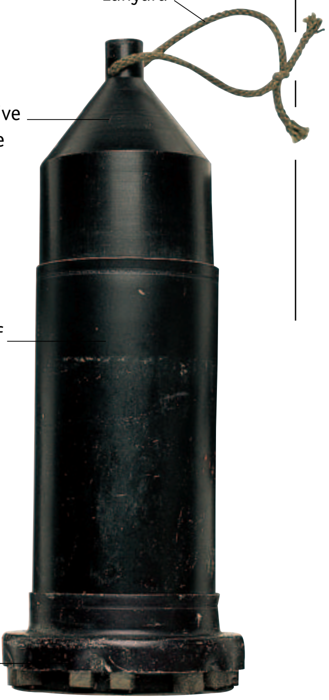
US special forces jammer

This hand-emplaced expendable jammer is designed to deny an enemy the use of radio communication equipment. It transmits within a broad range of frequencies for a preset period of time within an operational area. At the end of the period, the jammer self-destructs so that the enemy will not be able to use the radio if found.



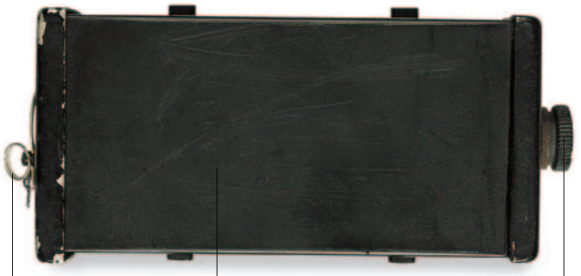
Shaped charge

Capable of punching a hole through 7–10 in (18–25 cm) of steel, this CIA plastic demolition charge contains 4 oz (100 g) of the explosive RDX. The charge is used to pierce shafts, bearings, gear boxes, and other vital parts of machinery. This type of charge is used to disable rather than destroy machines.



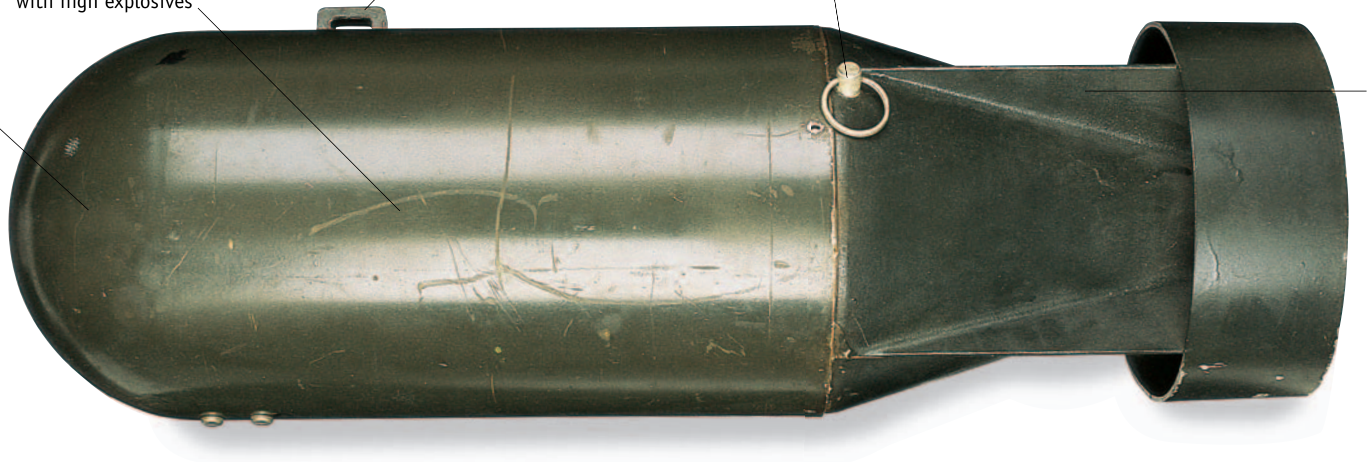
OSS antidisturbance mine

This highly sensitive anti-disturbance mine will, when properly loaded and activated, explode if moved in any direction or vibrated. It has a timing device that detonates it after 10–13 minutes and cannot be deactivated once the timer has started. The mine is waterproof up to a depth of 6 m (20 ft).



Boat mine

Despite its resemblance to an aerial bomb, this buoyant boat mine, made by the CIA, has a hydrodynamic shape that allows it always to turn itself in the direction of the oncoming water current. In use, the boat mine is moored beneath the surface in a river, channel, or harbor, where it "waits" as its sensors count passing metal targets. After a preset number of targets have been detected, the mine explodes.


Mine body filled with high explosives
Attachment point for mooring
Safety ring
Rounded nose
Fin

Amphibious sabotage

THE CHIEF GOALS of amphibious sabotage are to destroy enemy ships and attack coastal defenses. Raiding parties, well trained and equipped with special craft, secretly enter enemy harbors and other waters to undertake perilous operations. During World War II, a number of innovations in tactics and equipment contributed to the effectiveness of amphibious raids. Canoes and submersible craft, such as the "Sleeping Beauty," were developed for use in enemy harbors. And new types of explosive devices, such as limpet mines, were invented for use under water.

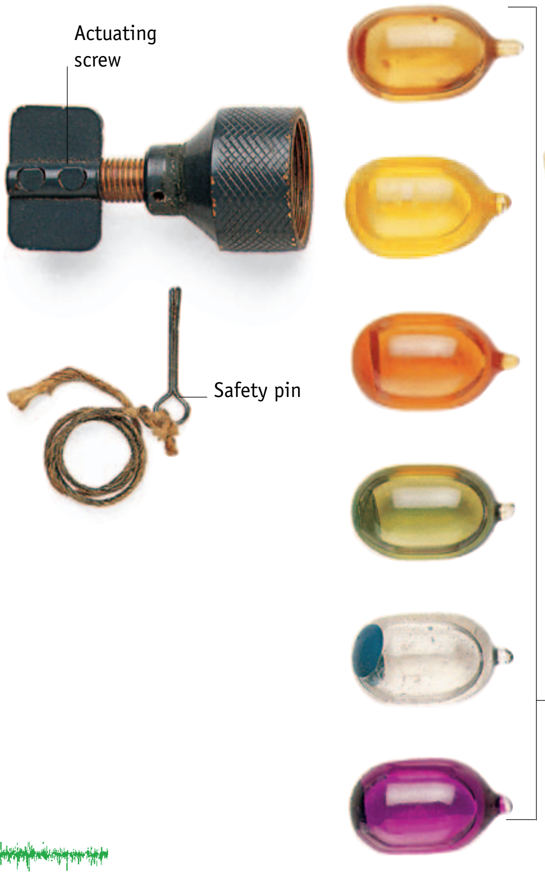
OSS acetone time-delay fuse

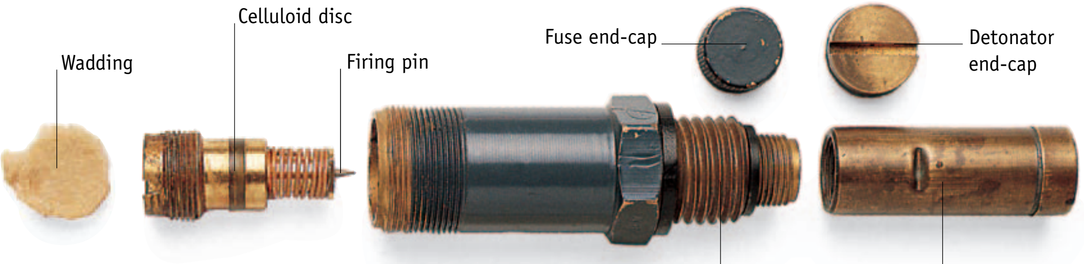
Limpet mines were attached magnetically to the hulls of ships. Many had acetone fuses that would detonate the mines after an interval indicated by the color of an acetone ampule. The color represented the concentration of the acetone, which ate through a celluloid disk, releasing a firing pin and detonating the mine. The fuse was set manually by twisting an actuating screw, which crushed the ampule and released the acetone.

OPERATION FRANKTON

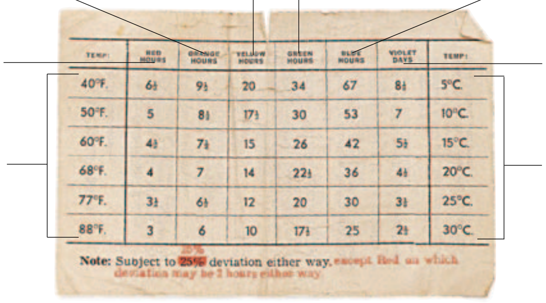
During World War II, the Allied navies tried to blockade German-held France. However, German ships continued to call at the French harbors. In 1942, a party of British Royal Marines attacked German vessels in the French harbor of Bordeaux. The raiders were taken by submarine to a river estuary nearby, and then set off by canoe to the target. Only two of the five canoes reached Bordeaux. During the night the raiders attached 16 limpet mines to six German ships, sinking four and damaging the other two ships. Only two of the 10 saboteurs survived and returned home safely to Britain.

Royal Marine saboteurs
Major H. G. "Blondie" Hasler (1914–87, in front) and Corporal W. E. Sparks (1922–2002) were the only survivors of the Bordeaux raid.





COMPONENTS OF FUSE


Orange ampule (delay in hours)
Yellow ampule (delay in hours)
Green ampule (delay in hours)
Blue ampule (delay in hours)
Red ampule (delay in hours)
Violet ampule (delay in days)
Temperature in degrees Fahrenheit
Temperature in degrees Centigrade

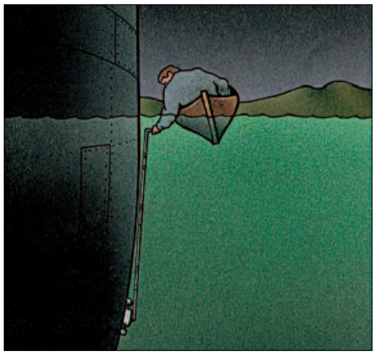
TEMP:	RED HOURS	ORANGE HOURS	YELLOW HOURS	GREEN HOURS	BLUE HOURS	VIOLET DAYS	TEMP:
40°F.	6½	9½	20	34	67	8½	5°C.
50°F.	5	8½	17½	30	53	7	10°C.
60°F.	4½	7½	15	26	42	5½	15°C.
68°F.	4	7	14	22½	36	4½	20°C.
77°F.	3½	6½	12	20	30	3½	25°C.
88°F.	3	6	10	17½	25	2½	30°C.

Note: Subject to ~~25%~~ 15% deviation either way. except Red on which deviation may be 2 hours either way

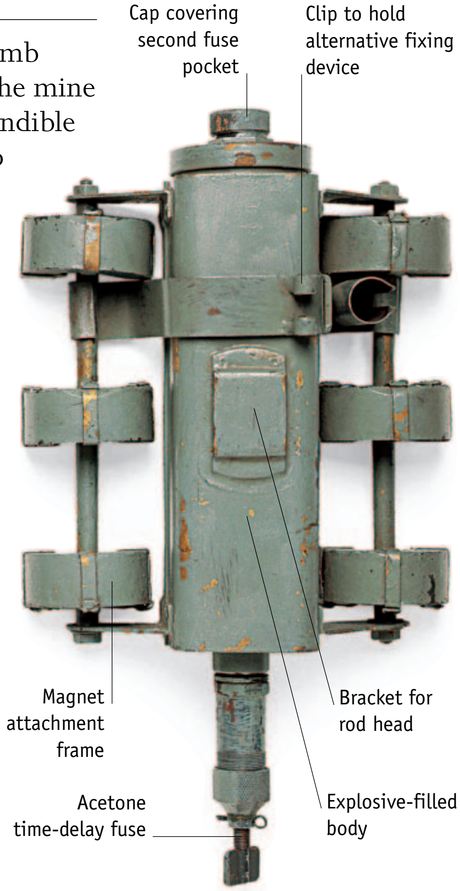
INSTRUCTION SHEET SHOWING TIME DELAYS

OSS limpet mine

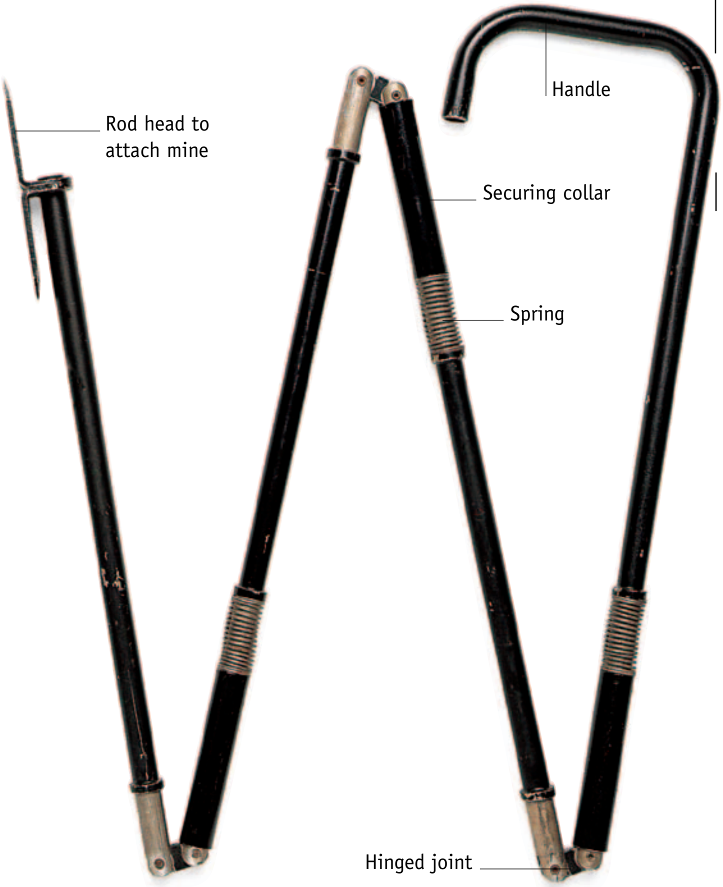
A limpet mine was a waterproof bomb designed to sink or damage ships. The mine was positioned by means of an extendible placing rod, and held by magnets to the ship's steel hull. An acetone time-delay fuse was used to detonate the mine. The limpet mine could blow a hole of up to 25 sq ft (2.3 sq m) in a ship's hull.



Placing a limpet mine
Saboteurs had to approach the target ship silently, usually in a small boat. They attached the mine carefully, using an extendible placing rod 5 ft (1.5 m) below the waterline.



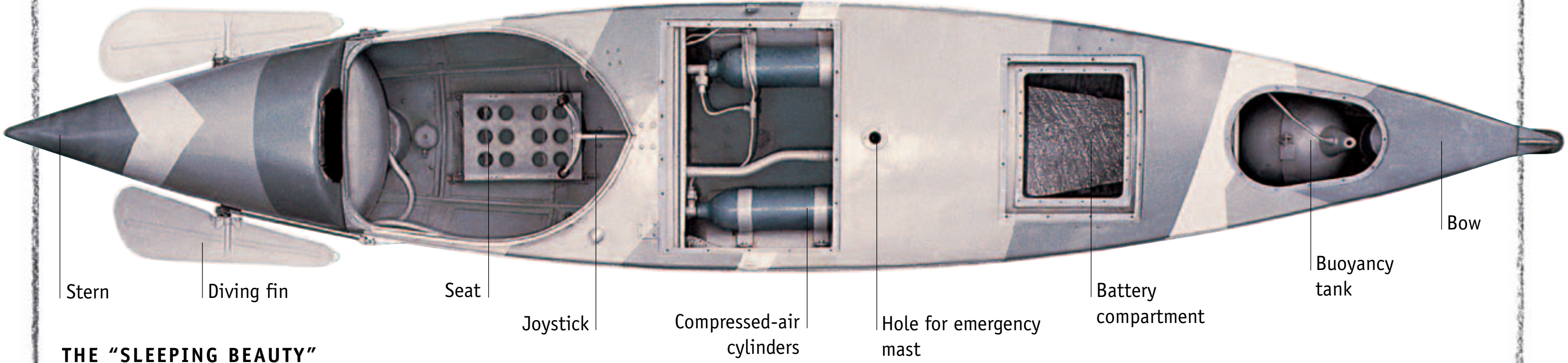
LIMPET MINE



PLACING ROD

OPERATION RIMAU: THE RAID ON SINGAPORE HARBOR

The Japanese captured Singapore island from the British in 1942. Later that year, raiders belonging to the Allied Intelligence Bureau (a special operations force set up by Britain and its allies) launched an attack from Australia against Japanese ships in Singapore harbor. The saboteurs entered the harbor in folding canoes and attached limpet mines to the Japanese ships. Seven ships, with a total tonnage of 37,000 tons, were completely destroyed. A second raid was attempted in 1944, using a newly developed craft, the "Sleeping Beauty." This electric-powered submersible canoe could either be operated fully under water or with the pilot's head above the surface. Raiders were about to launch these craft from a captured cargo ship when they were detected by water police. The operation was aborted. The saboteurs tried to escape, but all died fighting or were captured and executed by the Japanese.



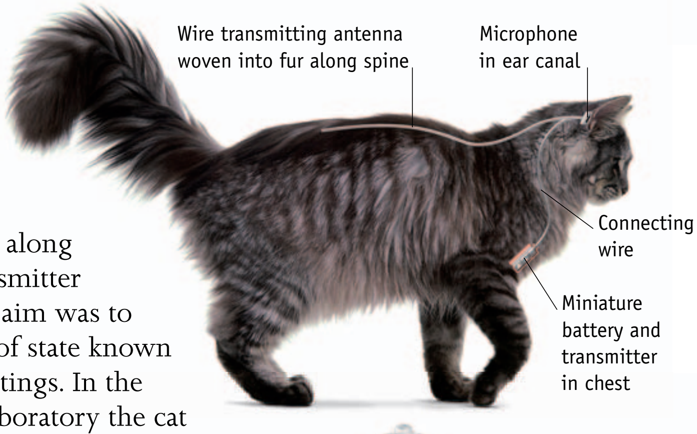
THE "SLEEPING BEAUTY"

Animals in espionage

INTELLIGENCE SERVICES have long used animals to support and sometimes even replace the work of human agents. An animal may be the ideal "spy" since it rarely draws suspicion from guards, blends in with natural surroundings, and can cross borders and enter areas denied to traditional agents. Animals real and robotic continue to be used for visual and audio surveillance in both wartime and peacetime. Dead or alive, animals can also be used to carry secret messages—or even weapons. Some animals have a proven track record for reliability in espionage. Others need a little more work …

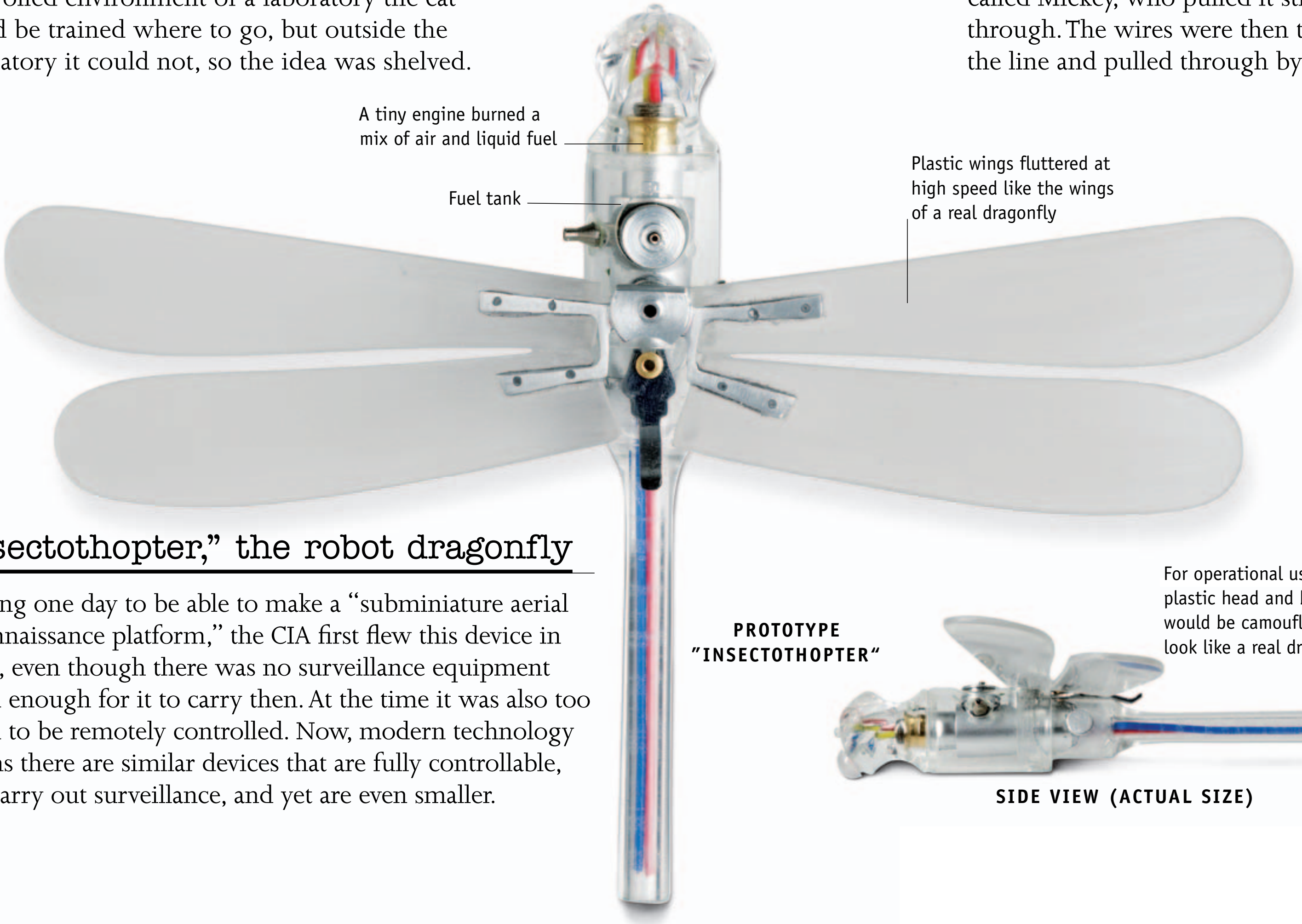
"Acoustic kitty"

In 1961 the CIA turned a cat into a "mobile acoustic collection platform" (MACP) by inserting a microphone in its ear, running a wire antenna along its back, and implanting a transmitter and battery under its skin. The aim was to use it to spy on an Asian head of state known to let cats wander into his meetings. In the controlled environment of a laboratory the cat could be trained where to go, but outside the laboratory it could not, so the idea was shelved.


Wire transmitting antenna woven into fur along spine
Microphone in ear canal
Connecting wire
Miniature battery and transmitter in chest

Mickey the M16 mouse

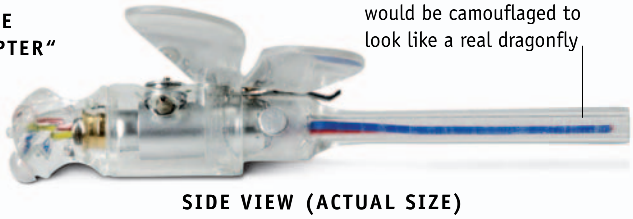
To bug the apartment of a suspected Soviet spy in Portugal in the early 1990s, MI6 needed to link hidden microphones to the listening post several floors below by running wires through a drainpipe that had many bends. Mechanical crawlers were tried and found wanting. So fishing line was tied to a mouse called Mickey, who pulled it straight through. The wires were then tied to the line and pulled through by hand.


A tiny engine burned a mix of air and liquid fuel
Fuel tank
Plastic wings fluttered at high speed like the wings of a real dragonfly

PROTOTYPE "INSECTOTHOPTER"

"Insectothopter," the robot dragonfly

Hoping one day to be able to make a "subminiature aerial reconnaissance platform," the CIA first flew this device in 1976, even though there was no surveillance equipment small enough for it to carry then. At the time it was also too small to be remotely controlled. Now, modern technology means there are similar devices that are fully controllable, can carry out surveillance, and yet are even smaller.


For operational use the plastic head and body would be camouflaged to look like a real dragonfly

SIDE VIEW (ACTUAL SIZE)

“*This page left intentionally blank.*”

COUNTER-INTELLIGENCE

"No Spies"
Members of FBI counterintelligence units adopted this unofficial lapel pin representing their commitment to keeping America free of spies. The pin was not worn operationally.

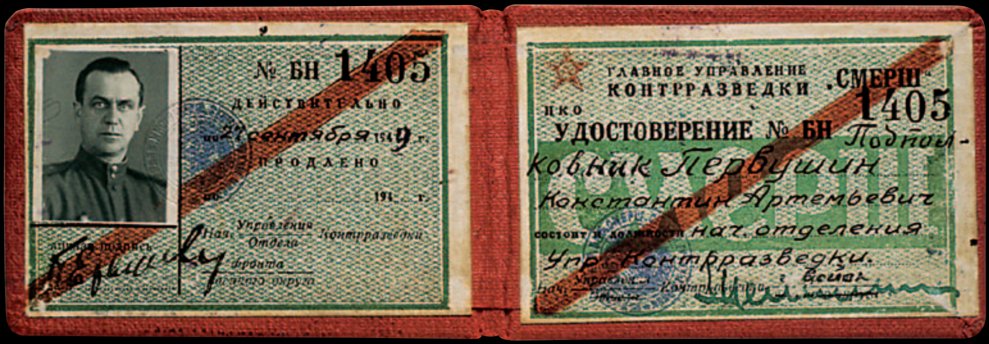
COUNTERINTELLIGENCE IS INTENDED to penetrate hostile intelligence agencies and to prevent the passage of sensitive information to the enemy. A great deal of counterintelligence work targets enemy agents when they communicate with their handlers. Counterintelligence services employ highly trained agents, often skilled in using technologically advanced equipment—although they also need to have good judgment and intuition to contend with suspected enemy spies. Because of the numerous layers of deception involved, counterintelligence has been called a "wilderness of mirrors."

REGNUM DEFENDE

MI5 emblem
The internal counterintelligence service in Britain is known as MI5. It achieved an amazing record of apprehending German spies during World War II.

DETECTORS

Many devices have been developed for detecting hostile agents in the act of espionage. The internet is constantly monitored by counterintelligence organizations searching for foreign agents. Other techniques are employed to track the movements of suspected agents. For example, powders that are invisible unless viewed with special equipment have historically been used by the KGB and FBI to reveal the footprints or fingerprints of spies. Detection equipment, such as cameras with telephoto lenses, has also been used.



№ БН 1405
ДЕЙСТВИТЕЛЬНО
по 21 сентября 1949 г.
ПРОДЛЕНО
по ______ 194_ г.
Нач. Управления / Отдела Контрразведки
фронта
военного округа
Личная подпись

ГЛАВНОЕ УПРАВЛЕНИЕ КОНТРРАЗВЕДКИ «СМЕРШ»
НКО
УДОСТОВЕРЕНИЕ № БН 1405
Подполковник Первушин Константин Артемьевич
состоит в должности нач. отделения Упр. Контрразведки.
Нач. Управления Контрразведки войск

"Death to spies"
This slogan, abbreviated to SMERSH as seen in this set of credentials, was the name of the Soviet military counterintelligence service (see p. 218).

ANTIBUGGING DEVICES

Intelligence agencies frequently use listening devices, otherwise known as bugs, to eavesdrop on sensitive conversations. In response to this, the counterintelligence services have developed special electronic equipment and techniques for detecting bugs. Use of these has to be backed up by physical searches of the site being

Invisible detection powders

To set a trap for an intruding spy, counterintelligence personnel put down invisible powders. After contact with human skin, these powders become visible under ultraviolet light.

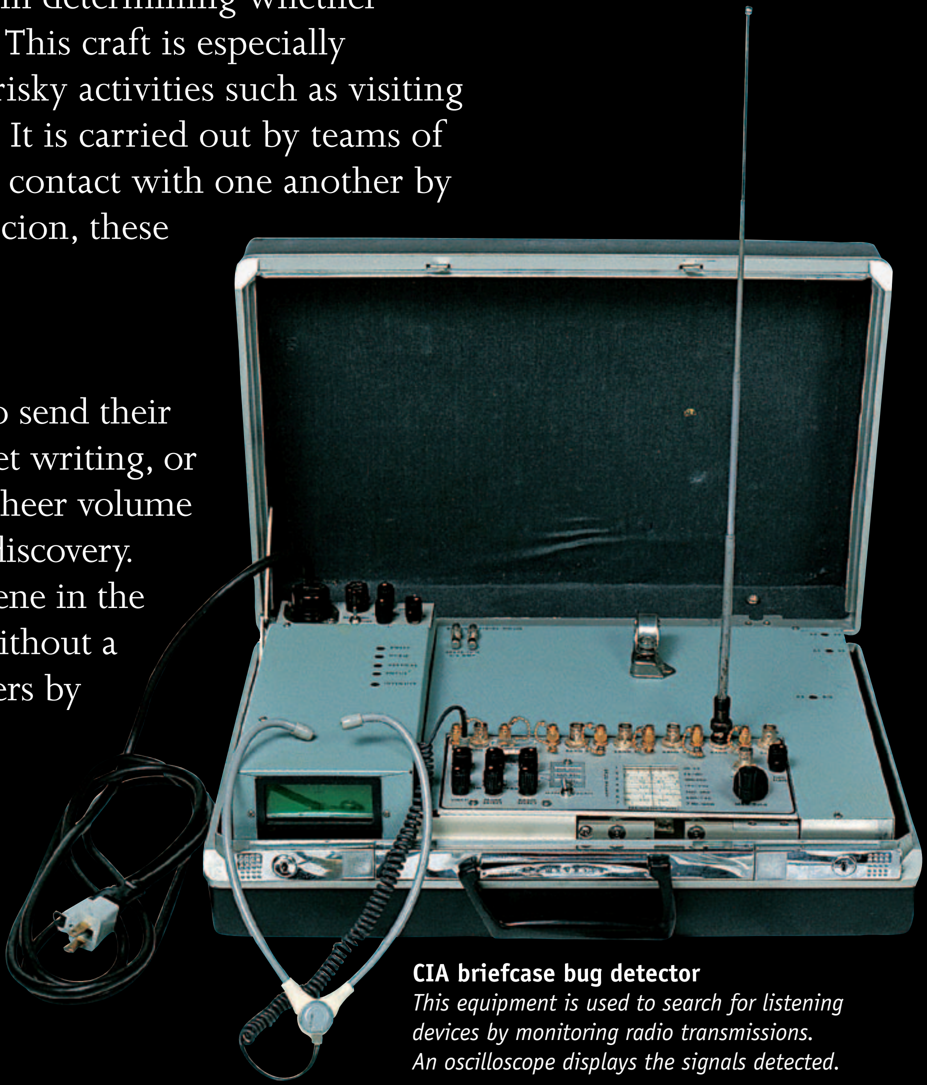
investigated for bugs. Audio countersurveillance devices work by picking up signals as the bugs transmit them. Such devices need to overcome certain difficulties that are commonly presented by bugs. Some bugs can be switched off remotely to avoid detection. Others hide themselves by transmitting on a frequency very close to that of a powerful radio station: this is known as "snuggling," in the trade.

COUNTERSURVEILLANCE

The goal of countersurveillance is to help in determining whether conditions are safe for an agent operation. This craft is especially important for agents who are engaged in risky activities such as visiting a dead drop or meeting their case officers. It is carried out by teams of specially trained personnel, who maintain contact with one another by hidden radios. To avoid arousing any suspicion, these personnel may need to be in disguise.

LETTER INTERCEPTION

Spies can of course use the ordinary mail to send their messages. They may write in code, use secret writing, or incorporate microdots in their letters. The sheer volume of the mail is their best protection against discovery. Counterintelligence officers who do intervene in the mail service (which may not be possible without a warrant) may hope to find some spies' letters by concentrating on the addresses of suspects. Letters are opened by "flaps and seals" experts, so named because in the past their work had to do with envelope flaps and wax seals. There are now special tools and materials that open correspondence without alerting the recipient to the fact that the mail has been examined.



CIA briefcase bug detector

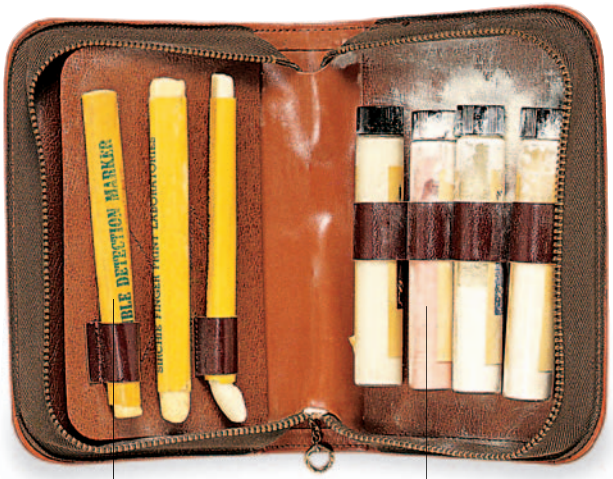
This equipment is used to search for listening devices by monitoring radio transmissions. An oscilloscope displays the signals detected.

Detectors

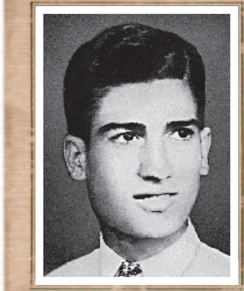
THE COUNTERINTELLIGENCE TOOLS that are used to monitor and trap spies are often referred to as detectors. Detectors are frequently electronic or photographic. But sometimes more subtle techniques are used, like the invisible spy dust laid down by the KGB to track the movements of CIA officers in Moscow. Various intelligence agencies, the KGB among them, have set up surveillance cameras with telephoto lenses to monitor movements of personnel at foreign embassies in the hope of detecting intelligence activities. Electronic detectors include the many devices used for detecting clandestine radios, such as radios used in a system referred to as radio direction finding (RDF). Elements of the Schulze-Boysen spy ring in Germany in World War II (see p. 38) and the Israeli spy Elie Cohen in Syria were caught using RDF.

Detection chemicals

The presence of a possible spy may be revealed by detection chemical kits, like this commercial kit used by the CIA. The chemicals are invisible when dusted onto objects such as doorknobs or documents. They react when touched by human skin and become visible, in ultraviolet light, on the skin of anyone who has been in contact with them.


Invisible crayon for sticking the powder to a surface
Invisible detection powder

ELIE COHEN

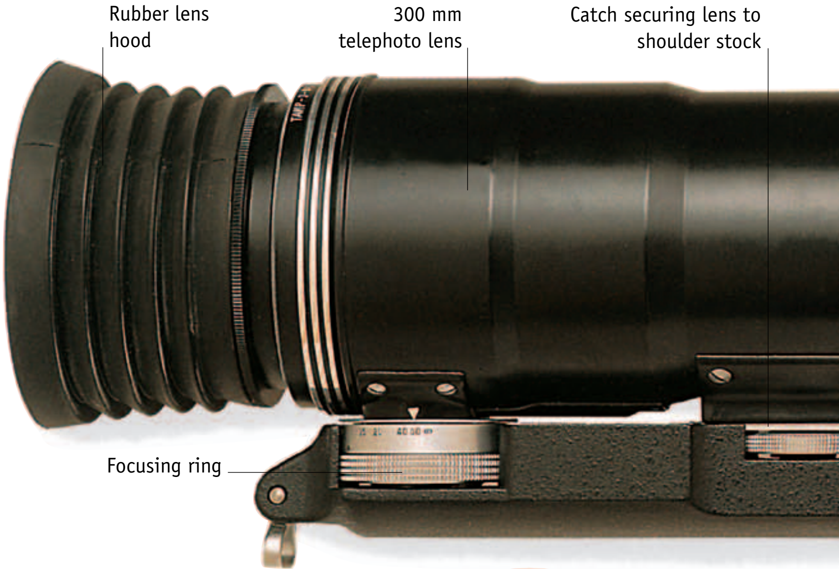


SPY PROFILE

In 1962, Egyptian-born Elie Cohen (1924–65) began spying for Israel in Syria, posing as a wealthy Syrian businessman. He infiltrated Syrian society and used the contacts he made to gather intelligence. Cohen passed information about the Syrian armed forces by radio to Israel, but his frequent and predictable transmission schedule led to his detection by RDF equipment. He was tried and publicly hanged in 1965.

Photo-sniper

This 35mm surveillance camera is capable of taking high-definition pictures over long distances. It was used by counterintelligence teams of the KGB's Second Chief Directorate and by KGB Border Guards. The shoulder stock mounting for the camera allows it to be held steady without using a cumbersome and conspicuous tripod.



GREEN FILTER

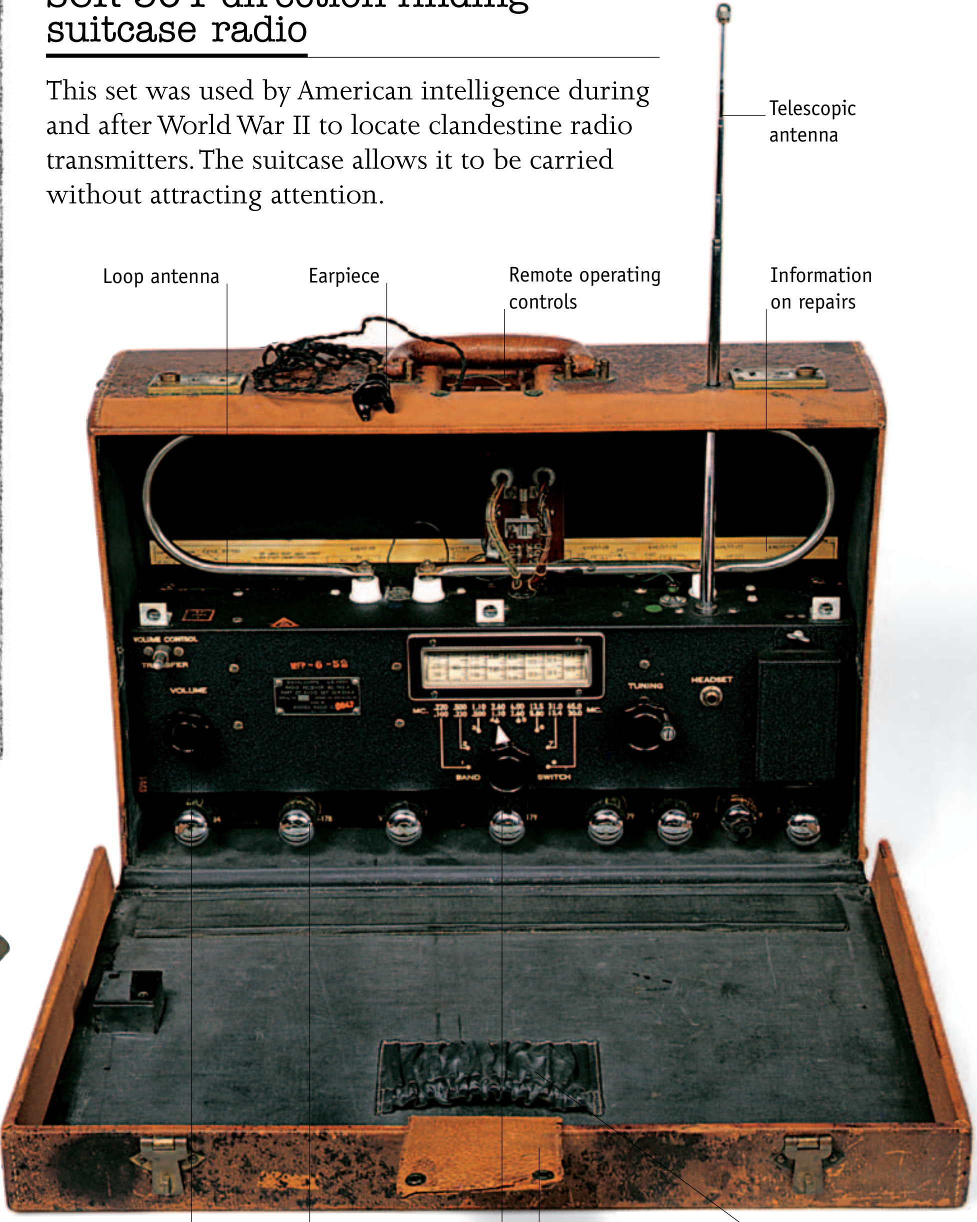
YELLOW FILTER

JAMES J. ANGLETON

James J. Angleton (1917–87), a wartime OSS (see p. 32) officer, became the chief of the CIA's Counterintelligence Staff in 1954. During the 1960s, convinced by KGB defector Anatoli Golitsyn (b.1926) that a spy had penetrated the CIA, Angleton set up an investigation that disrupted the Agency and led to the rejection of several potential KGB defectors to the West. As a result of this affair and his role in an illegal "mail cover" operation, he resigned in 1974.

SCR-504 direction-finding suitcase radio

This set was used by American intelligence during and after World War II to locate clandestine radio transmitters. The suitcase allows it to be carried without attracting attention.


Telescopic antenna
Loop antenna
Earpiece
Remote operating controls
Information on repairs
Volume control
Valves located for easy replacement
Switch to locate radio band
Flap to conceal controls when case is closed
Accessory pocket for earpiece

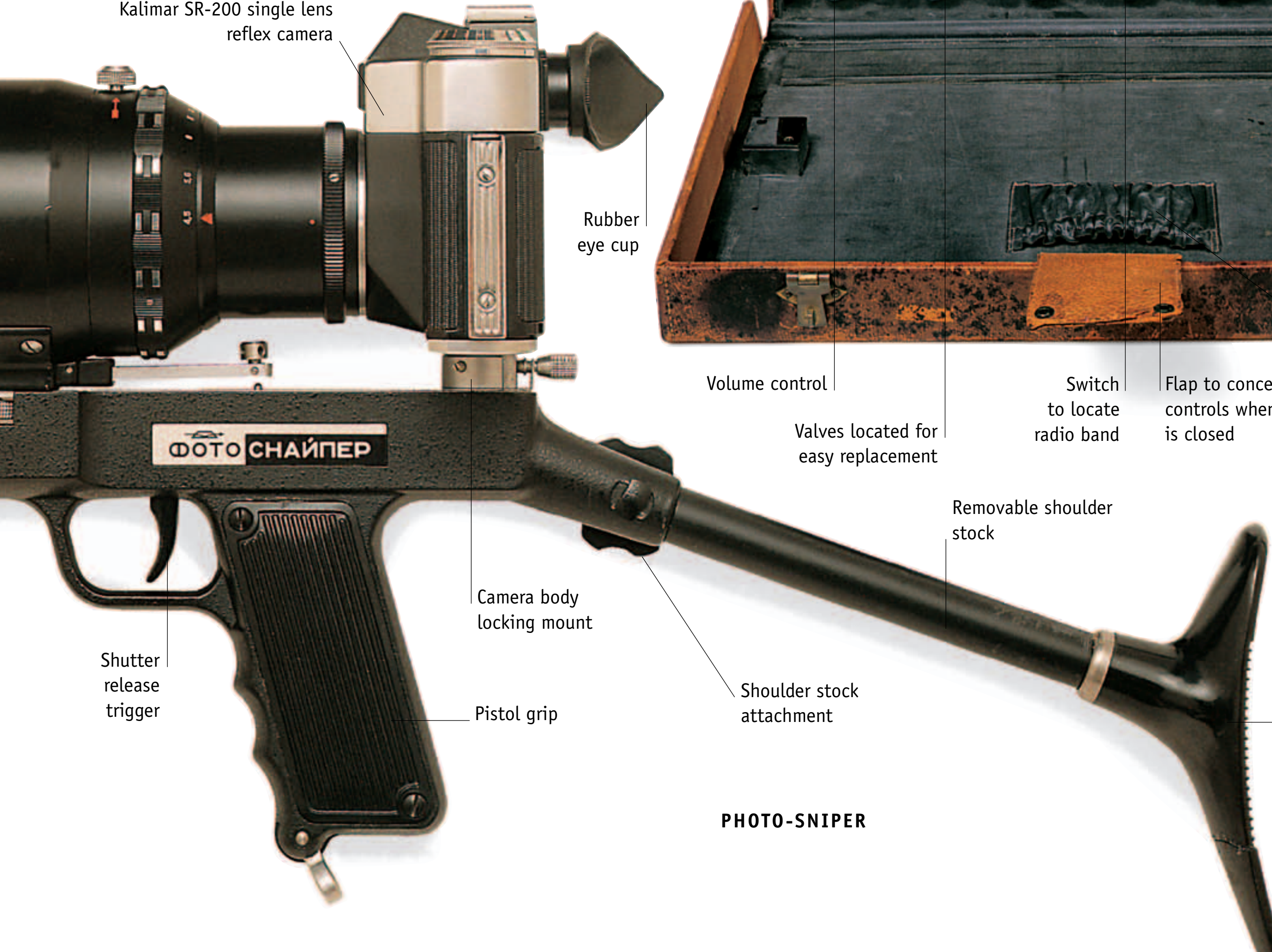


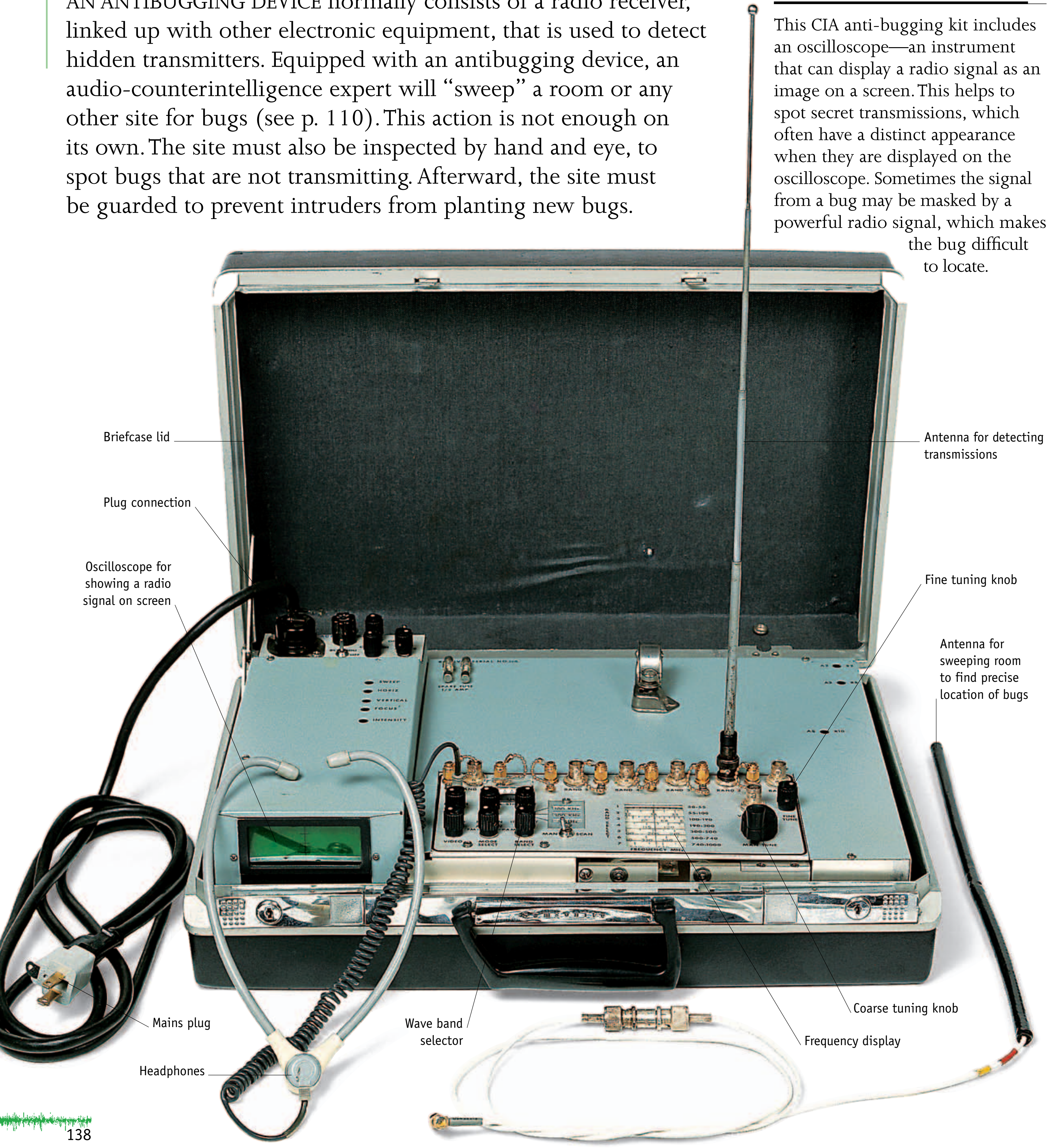
PHOTO-SNIPER

Antibugging devices

AN ANTIBUGGING DEVICE normally consists of a radio receiver, linked up with other electronic equipment, that is used to detect hidden transmitters. Equipped with an antibugging device, an audio-counterintelligence expert will "sweep" a room or any other site for bugs (see p. 110). This action is not enough on its own. The site must also be inspected by hand and eye, to spot bugs that are not transmitting. Afterward, the site must be guarded to prevent intruders from planting new bugs.

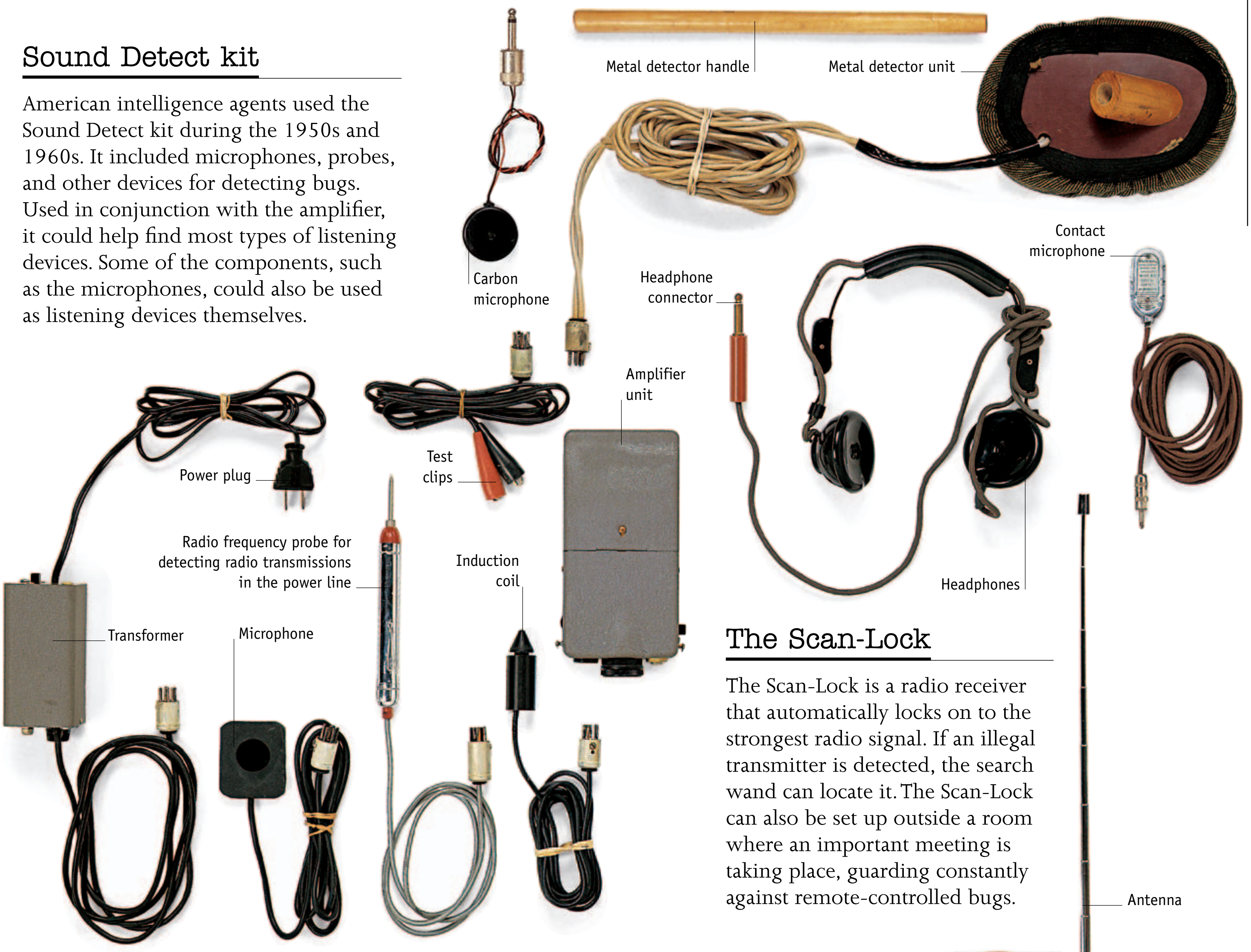
Portable detection kit

This CIA anti-bugging kit includes an oscilloscope—an instrument that can display a radio signal as an image on a screen. This helps to spot secret transmissions, which often have a distinct appearance when they are displayed on the oscilloscope. Sometimes the signal from a bug may be masked by a powerful radio signal, which makes the bug difficult to locate.


Briefcase lid
Plug connection
Oscilloscope for showing a radio signal on screen
Mains plug
Headphones
Wave band selector
Antenna for detecting transmissions
Fine tuning knob
Antenna for sweeping room to find precise location of bugs
Coarse tuning knob
Frequency display

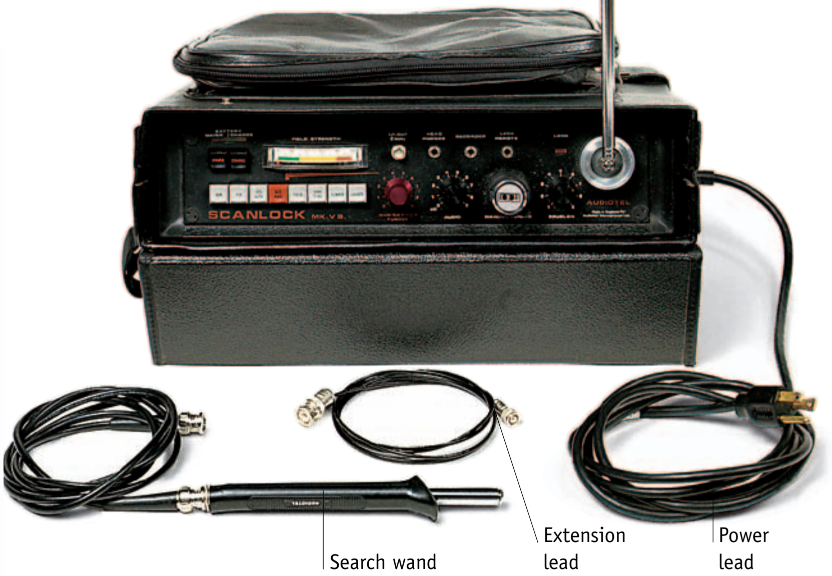
Sound Detect kit

American intelligence agents used the Sound Detect kit during the 1950s and 1960s. It included microphones, probes, and other devices for detecting bugs. Used in conjunction with the amplifier, it could help find most types of listening devices. Some of the components, such as the microphones, could also be used as listening devices themselves.



The Scan-Lock

The Scan-Lock is a radio receiver that automatically locks on to the strongest radio signal. If an illegal transmitter is detected, the search wand can locate it. The Scan-Lock can also be set up outside a room where an important meeting is taking place, guarding constantly against remote-controlled bugs.



HEINZ FELFE

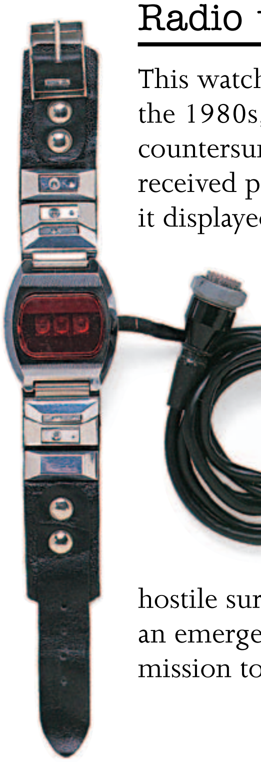
SPY PROFILE

Heinz Felfe (1918–2008) was a member of the World War II Nazi SD (see p. 34). In 1950 he was recruited as a Soviet spy and infiltrated the West German Foreign Intelligence Service, the BND. Felfe compromised West German intelligence operations for 11 years. With his inside knowledge he was able to warn Soviet audio technicians of the movements of BND sweepers, so the Soviets had time to remove or switch off their bugs.

Countersurveillance

SPIES RECEIVE SPECIAL TRAINING in countersurveillance, the object of which is to detect hostile surveillance, for instance, of personnel, meetings, safe houses, or dead drops. The discovery of hostile surveillance is sufficient cause to cancel a meeting, bypass a safe house, or abort the planned servicing of a dead drop. Specialized technology exists that can help the countersurveillance team, including video and radio monitoring of likely threats. Team members may have to use disguises to avoid being recognized. The resources available to countersurveillance teams are likely to vary according to circumstances. Obviously, it is easier to mount such operations in a friendly country than in a hostile one.

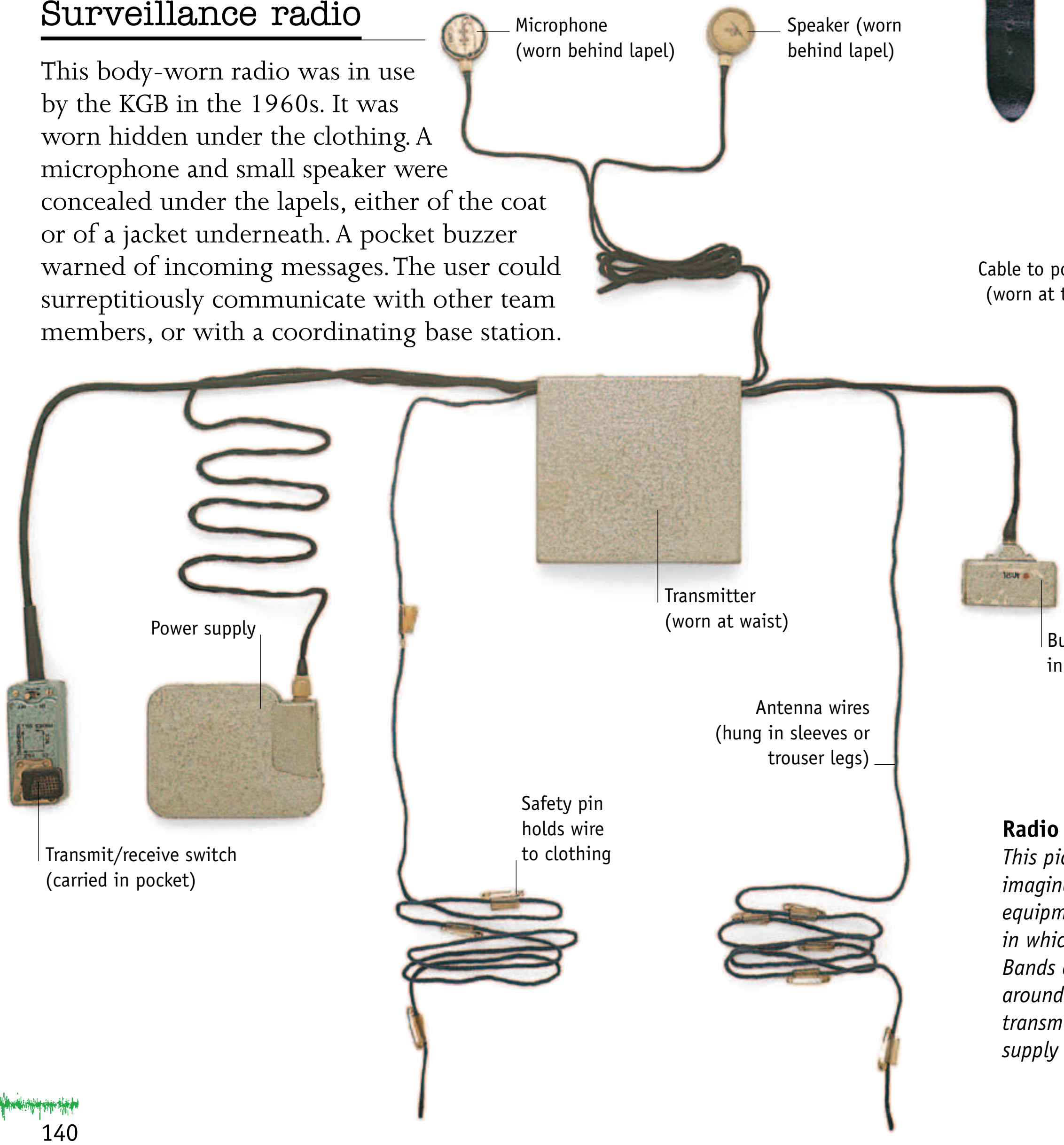
Radio wristwatch

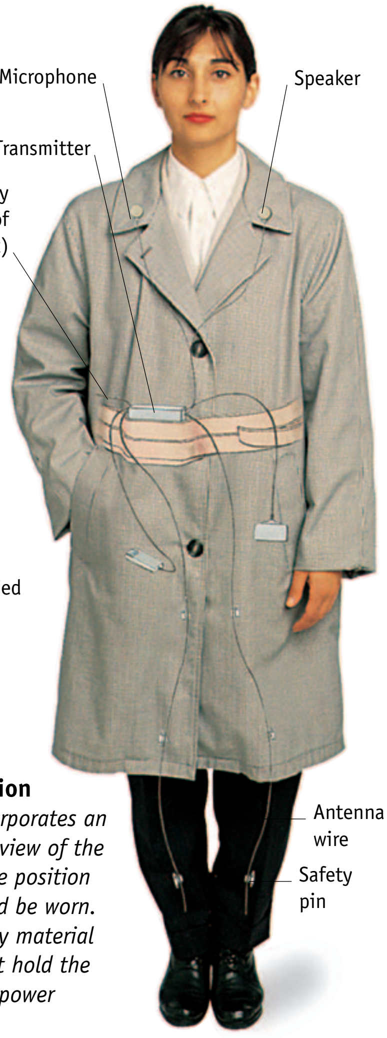


This watch was used by the KGB in the 1980s, both for surveillance and countersurveillance operations. It received prearranged signals, which it displayed on a screen. Its receiver was worn on the body, with a vibrator to indicate when a signal came in. The watch was used to control the movements of a spy. If the controllers became aware of hostile surveillance, they could send an emergency code ordering the mission to be aborted.

Surveillance radio

This body-worn radio was in use by the KGB in the 1960s. It was worn hidden under the clothing. A microphone and small speaker were concealed under the lapels, either of the coat or of a jacket underneath. A pocket buzzer warned of incoming messages. The user could surreptitiously communicate with other team members, or with a coordinating base station.


Microphone (worn behind lapel)
Speaker (worn behind lapel)
Power supply
Transmitter (worn at waist)
Buzzer (carried in pocket)
Antenna wires (hung in sleeves or trouser legs)
Safety pin holds wire to clothing
Transmit/receive switch (carried in pocket)

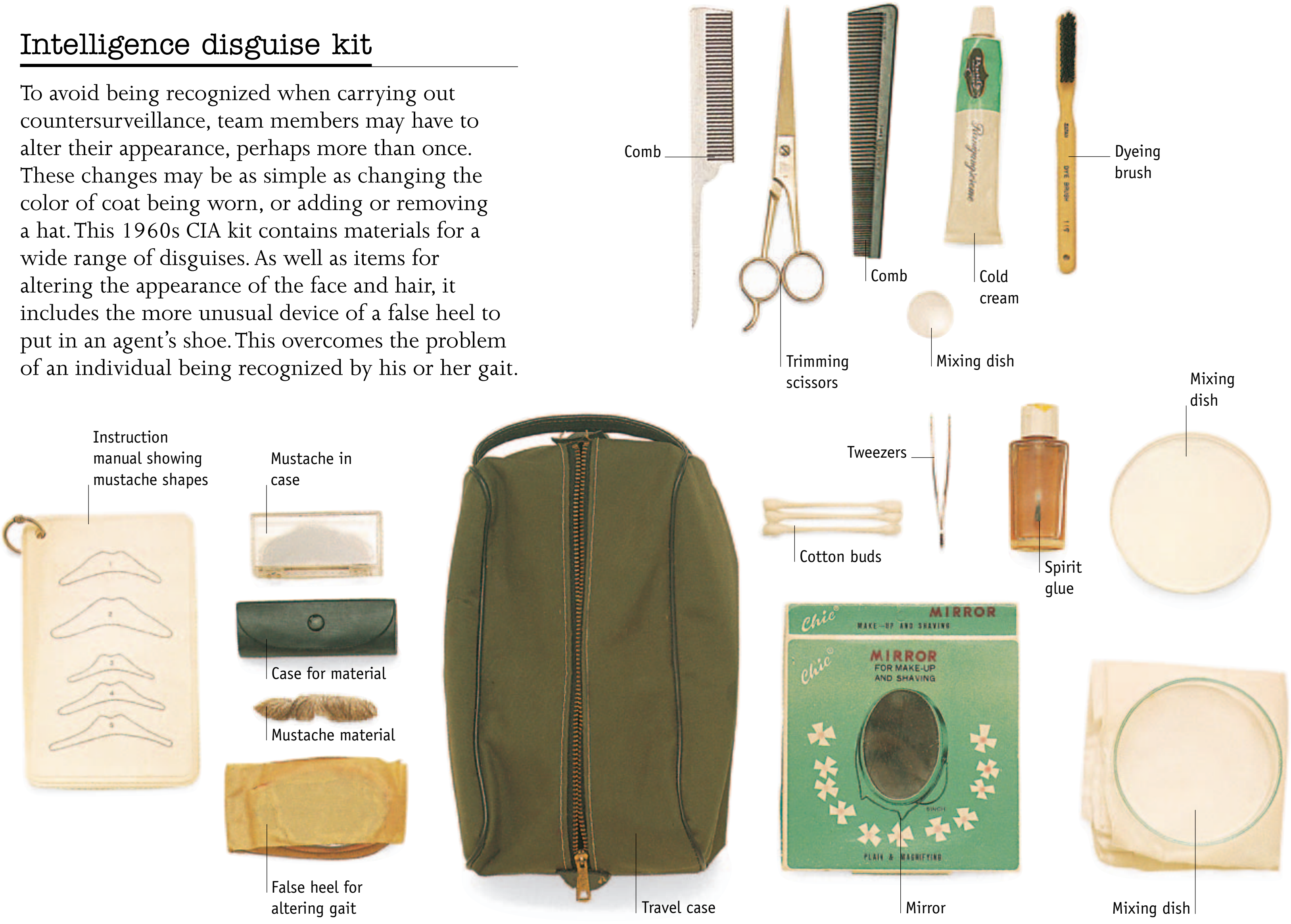


Radio in position

This picture incorporates an imaginary X-ray view of the equipment in the position in which it would be worn. Bands of stretchy material around the waist hold the transmitter and power supply in place.

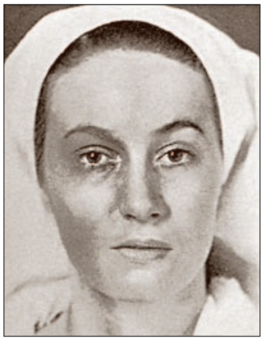
Intelligence disguise kit

To avoid being recognized when carrying out countersurveillance, team members may have to alter their appearance, perhaps more than once. These changes may be as simple as changing the color of coat being worn, or adding or removing a hat. This 1960s CIA kit contains materials for a wide range of disguises. As well as items for altering the appearance of the face and hair, it includes the more unusual device of a false heel to put in an agent's shoe. This overcomes the problem of an individual being recognized by his or her gait.

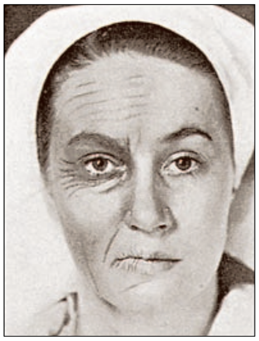


FACIAL DISGUISE BY ARTIFICIAL AGING

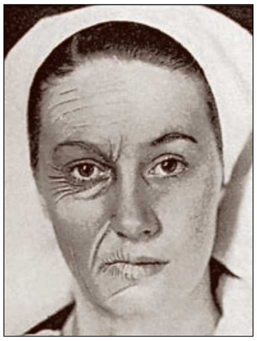
Artificial aging is an effective and widely applicable method of disguise, since it does not rely too heavily on disguising the bone structure of the face. Makeup is used to accentuate existing wrinkles and creases. Care is needed to avoid an artificial appearance and to ensure that the hands and throat match the face. The stages in using makeup to simulate aging are shown on the right. In each picture, makeup is on the subject's right (our left) side only.



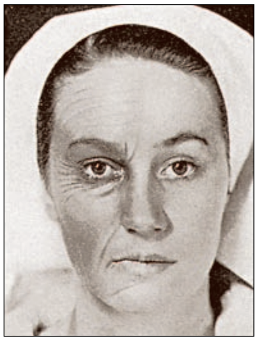
Skeleton modeling
Makeup can disguise the bone structure of the face to a small extent.



Reinforcing the lines
Existing facial lines are emphasized by applying dark makeup.



Adding the highlights
Areas of the face that stand out naturally are artificially lightened.



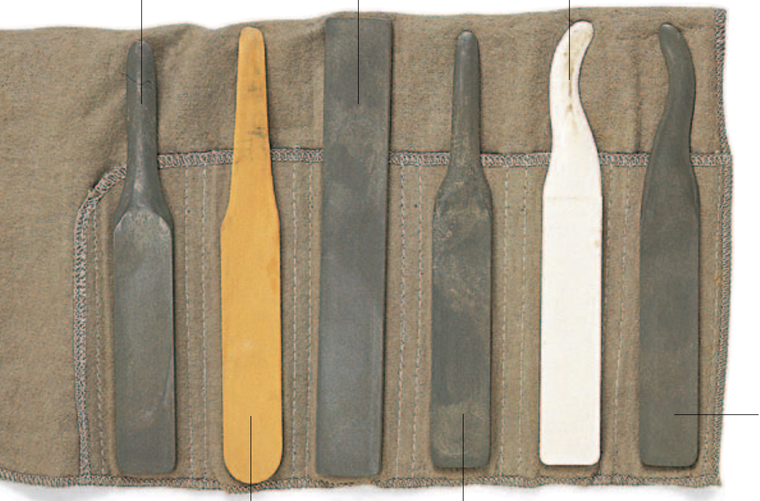
Blending
The balance of lines and highlights is adjusted to give a natural appearance.

Letter interception

WHEN SPIES SEND letters through the mail system they risk interception by enemy counterintelligence. The volume of regular mail makes it impossible for counterintelligence services to search it all, but they may search letters to and from suspect groups, individuals, or addresses. In Western countries, this cannot be done without first obtaining a warrant. Special techniques have been developed to take a letter out of an envelope without damaging it. There are also specialized technical terms: secret opening of mail is known as "flaps and seals" work. Three of the most common techniques are known as "steam openings," "dry openings" (using a separation of the glue), and "wet openings" (using water).

Flaps and seals tool roll

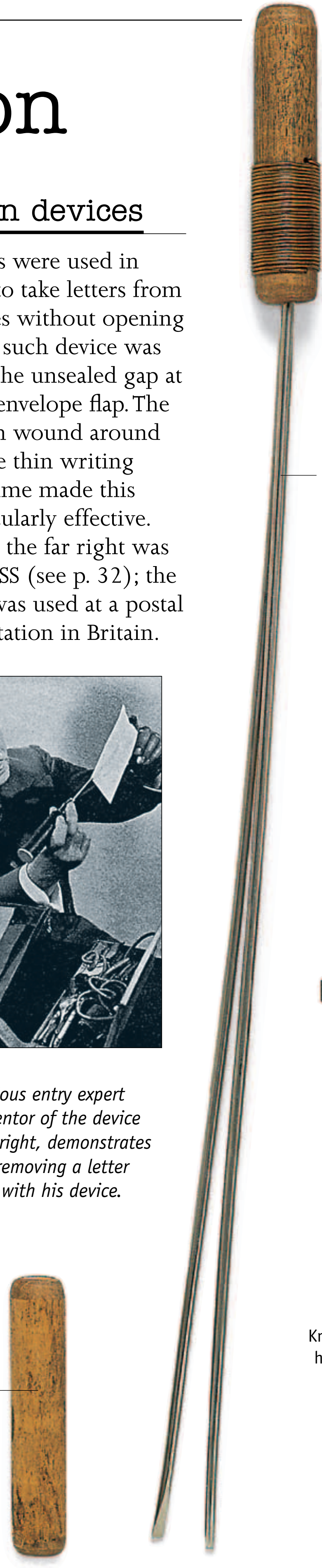
This American set of six tools may be used for surreptitious opening of most kinds of envelope. The tools are either used alone, or in conjunction with steam, water, or another solvent.



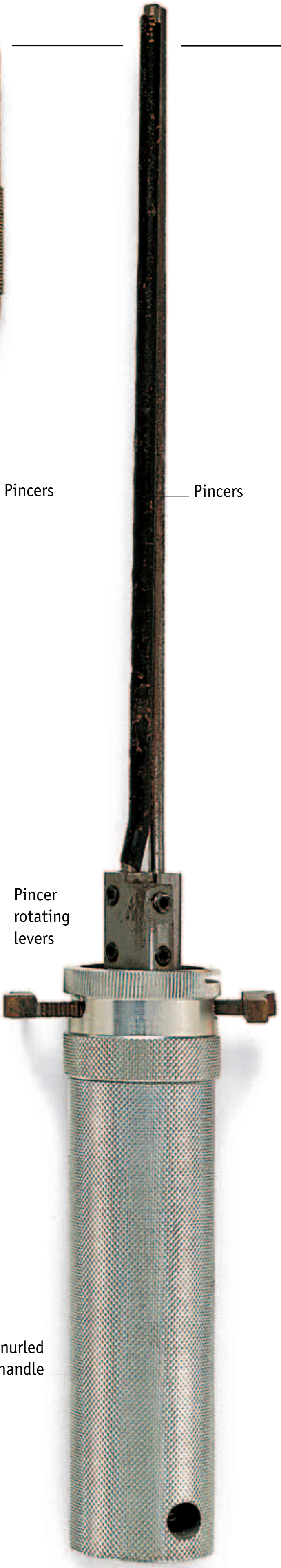
Letter extraction devices

Special devices were used in World War II to take letters from their envelopes without opening the seals. One such device was inserted into the unsealed gap at the top of an envelope flap. The letter was then wound around the device. The thin writing paper of the time made this method particularly effective. The device on the far right was used by the OSS (see p. 32); the other device was used at a postal interception station in Britain.

Willis George
The OSS surreptitious entry expert Willis George, inventor of the device shown on the far right, demonstrates the technique of removing a letter from its envelope with his device.



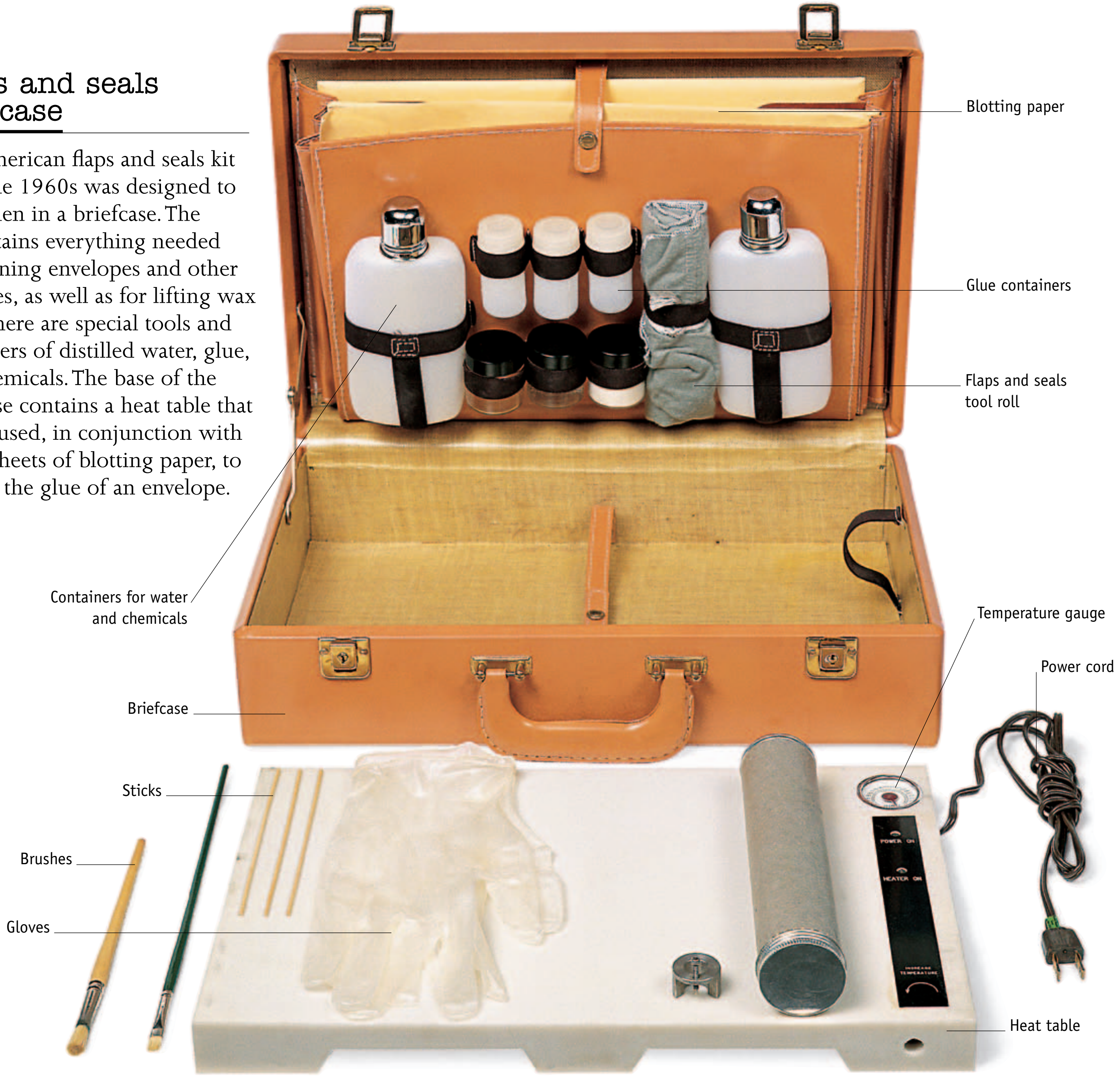
BRITISH LETTER REMOVAL DEVICE



OSS LETTER REMOVAL DEVICE

Flaps and seals briefcase

This American flaps and seals kit from the 1960s was designed to be hidden in a briefcase. The kit contains everything needed for opening envelopes and other packages, as well as for lifting wax seals. There are special tools and containers of distilled water, glue, and chemicals. The base of the briefcase contains a heat table that can be used, in conjunction with damp sheets of blotting paper, to unstick the glue of an envelope.



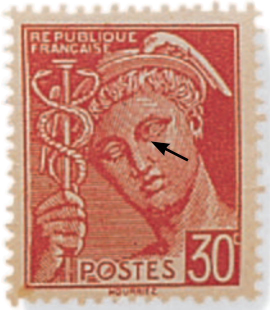
STAMPS FOR THE FRENCH RESISTANCE

During World War II, French resistance groups (see p. 31) were engaged in secret operations against the occupying German army. These groups often used the mail to communicate when arranging meetings.

The Germans had a practice of luring patriotic Frenchmen to false resistance meetings, using forged letters. If a French resistance sympathizer received such a fake letter and, believing it to be genuine, turned up for a meeting, the Germans would arrest him. If, however, he gave the letter to the Germans to avoid being accused of complicity, he risked betraying the resistance if the letter should prove to be genuine after all.

To resolve this problem, British intelligence made fake French stamps that differed from genuine ones in a tiny detail known only to the resistance. Any "resistance" letters that did not bear this special stamp were assumed to be traps. The Germans never discovered the secret of the stamps.

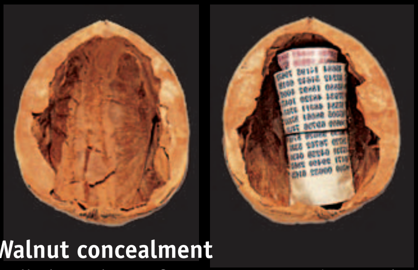
GENUINE STAMP



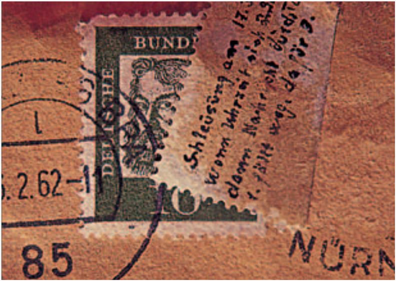
FAKE STAMP (ARROW SHOWS DIFFERENCE)

CLANDESTINE COMMUNICATIONS

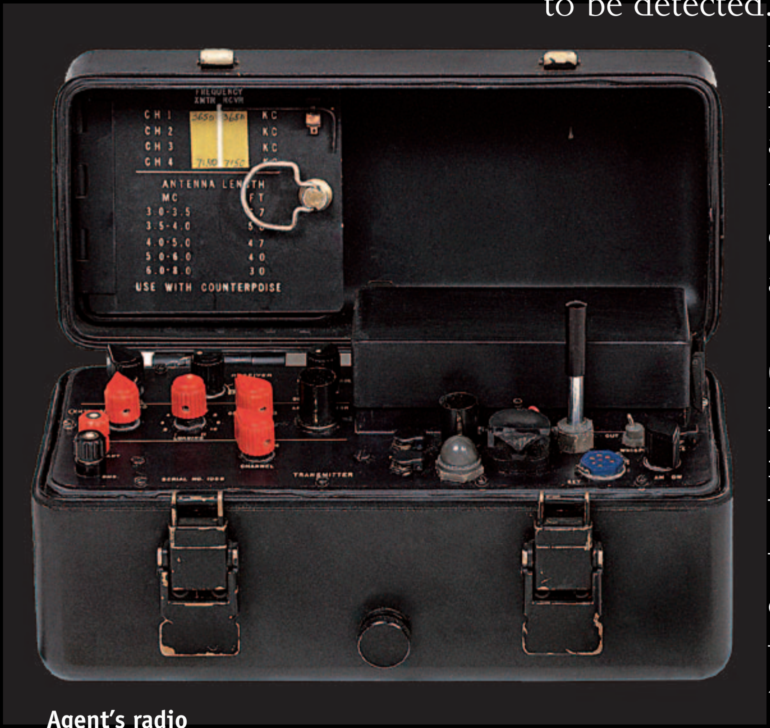
TO OPERATE SUCCESSFULLY, it is essential for spies to have secret methods of communicating with their controllers. These clandestine communications must provide a safe and reliable form of contact between spy and spymaster, while remaining secure from interception by the enemy. Methods used for clandestine communication are extremely varied—they range from radios, secret writing, and photography to new forms of digital steganography and the internet. Common to all is the care taken to protect them from detection. Radios were once made as small as possible and messages were enciphered, or put into code, before transmission. Additionally, they were speeded up and transmitted in short bursts that were less likely to be detected. Using the internet, modern spies send covert messages hidden inside digital attachments of images and music. Information may be photographed and reduced to microdots. Special inks are employed to write invisible messages. Concealments have been developed to disguise or hide clandestine messages and the equipment used to produc them.



Walnut concealment
Rolled-up sheets from a KGB one-time pad are hidden in an empty walnut shell. When used properly, the one-time pad system of coding messages is virtually impossible to crack.



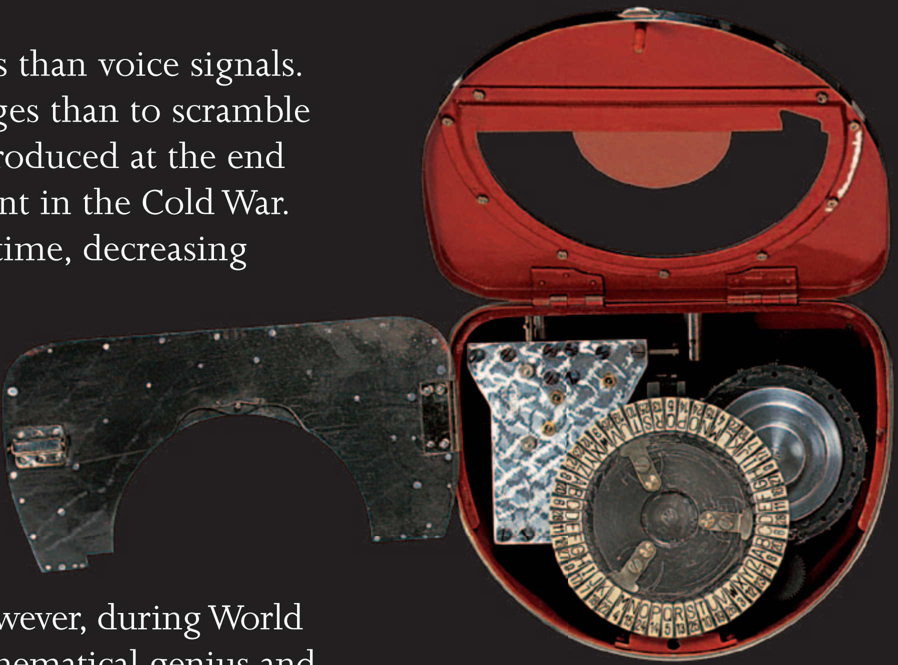
Stamp concealment
A secret message has been written on the back of this postage stamp, mailed from Nuremberg in West Germany.



Agent's radio
The compact Delco 5300 radio was used by CIA agents during the 1960s in Cuba. It could easily transmit messages from that country to the United States.

CLANDESTINE RADIOS

First conceived during the 1920s, special radios for communications were used extensively in World War II. They were often packaged inside suitcases when issued to personnel operating in enemy-occupied Europe, so that they could be carried without suspicion. Technological advances permitted the progressive miniaturization of radios during the war. Development continued after World War II with the introduction of transistors to replace bulky valves. Spy radios most often use Morse code, since this can be transmitted and received more clearly over long distances than voice signals. It is also easier to encrypt Morse code messages than to scramble voice messages. Burst transmissions were introduced at the end of World War II and continued to be important in the Cold War. The technique lessens a radio's transmitting time, decreasing the likelihood of it being located by radio direction finding (RDF).



Kryha cipher device
Invented in 1924, the Kryha device employed a spring-driven alphabetic rotor to turn messages into code (encipher them). The device was used by the German diplomatic corps in World War II.

CIPHER DEVICES

During the early 20th century, a number of electromechanical cipher machines were invented; these produced ciphers so complex that they were thought to be unbreakable. However, during World War II they were broken, both by human mathematical genius and by the use of the world's first electronic computer. One form of cipher that remains virtually unbreakable, even by modern computers, is the one-time pad system.

Ring with concealment
This British ring from World War II could conceal microdots or microfilm.

CONCEALMENTS

Concealments are frequently used for communications, and may be made to resemble everyday objects, such as pens. Discovery of a secret message by the enemy can often give away information about the source of the message, so concealments may be booby-trapped to explode if they are not opened in the correct way, destroying the contents. Information is also often sent in ways that assist its concealment. Special inks can produce secret writing, which is invisible until it has been treated with the correct chemical reagent. Photographic negatives, greatly reduced in size, can convey information in the form of microdots, which are easy to hide and very hard to find. To avoid the dangers of personal meetings, spies deliver or collect material at agreed hiding places, called dead drops. Some very ingenious concealments make dead drop containers blend in unnoticeably with their surroundings.

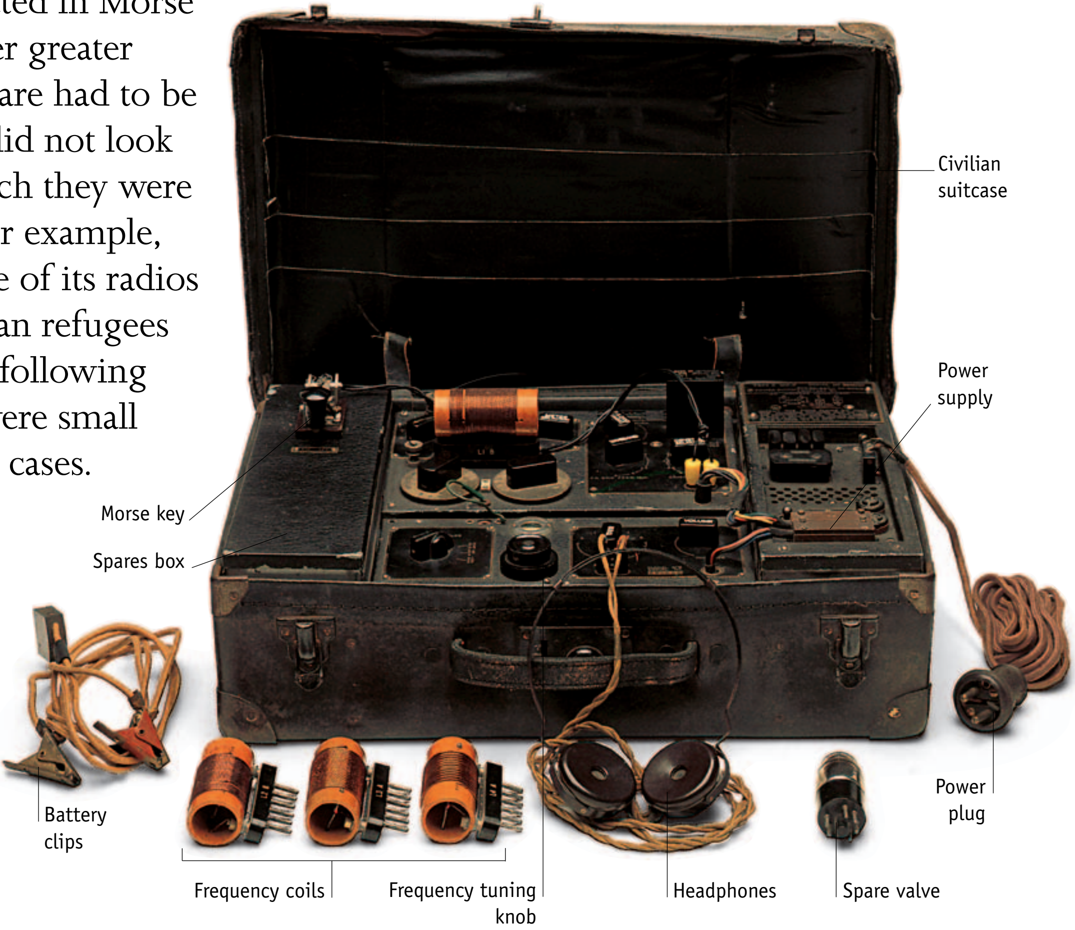
Modified objects
Technicians can modify everyday objects to make concealments. The Stasi (see p. 99) modified the key shown here, while the KGB modified the bolt.

Suitcase radios I

THE CONCEPT OF CONCEALING and transporting radios in suitcases was first developed in the late 1930s by the French and German intelligence services. Quickly adopted by other nations, these suitcase radios were extensively used during World War II. Early examples were bulky and inefficient, but technological advances permitted a reduction in size, while performance was improved. Messages were transmitted in Morse code, which could be received over greater ranges than voice transmissions. Care had to be taken to ensure that the suitcases did not look out of place in the country in which they were to be used. In the United States, for example, the OSS (see p. 32) packaged some of its radios in suitcases obtained from European refugees arriving in New York. In the years following World War II, clandestine radios were small enough to be concealed in attaché cases.

Type B Mk II radio

The most widely used SOE suitcase radio of World War II was the Type B Mk II. It was developed by John Brown in 1942, and was originally designed to operate at a range of up to 500 miles (800 km). In practice it could manage twice that distance in good conditions.



TECHNICAL DATA

Dimensions	18½ x 13½ x 6 in (47 x 34 x 15 cm)
Weight	32¾ lb (14.9 kg)
Range	up to 500 miles (800 km)
Power supply	97–250 V AC from house; 6 V DC from car battery
Power output	average 20 W
Transmitter	3.0 to 16.0 MHz in three bands
Receiver	4-tube superheterodyne receiving voice, tone, and Morse; 3.1 to 15.5 MHz in three bands

Transmitting
In a still taken from a film about the SOE, operative Jacqueline Nearne can be seen transmitting with a suitcase radio.

JACQUELINE NEARNE

SPY PROFILE

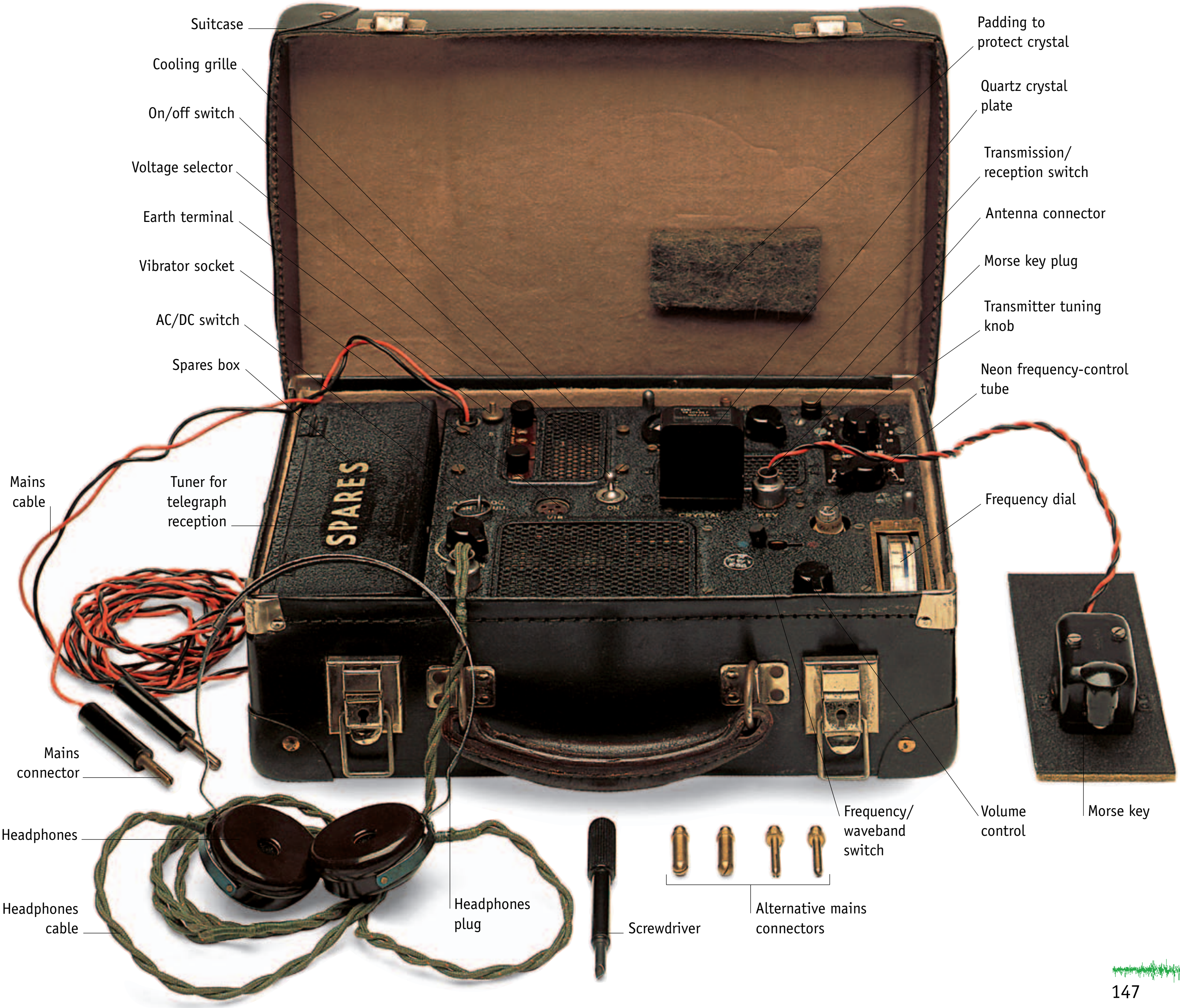
The SOE (see p. 30) recruited Jacqueline Nearne (1916–82) from the First Aid Nursing Yeomanry (FANY). She was taught how to make Morse code transmissions with a suitcase radio. In 1943 Nearne was sent to France to act as a courier. There she formed the link between several SOE groups covering a large area around Paris. The British later awarded Nearne the MBE (Member of the Order of the British Empire) for her work.

Type A Mk III radio

John Brown worked with the Marconi Company in 1943 to produce the Type A Mk III radio, which was smaller and lighter than any previous model. It was created by reducing the size of some components of the Type B Mk II radio. Because it was so light, the Mk III was an instant success with SOE operatives. Almost 20 lb (9 kg) lighter than the Type B Mk II, it had the same transmission range of about 500 miles (800 km).

JOHN BROWN: SUITCASE RADIO INVENTOR

In 1941, John Brown (1917–93), a signals officer in the British Army, was posted to a secret research station where his task was to design specialized radios for the SOE. He invented the "biscuit tin" radio (see p. 150) and the Type B Mk II suitcase radio. These were both widely used during World War II, but it was Brown's Type A Mk III suitcase radio, which contained miniaturized components obtained from the United States, that became the lightest, smallest SOE suitcase radio of the war.



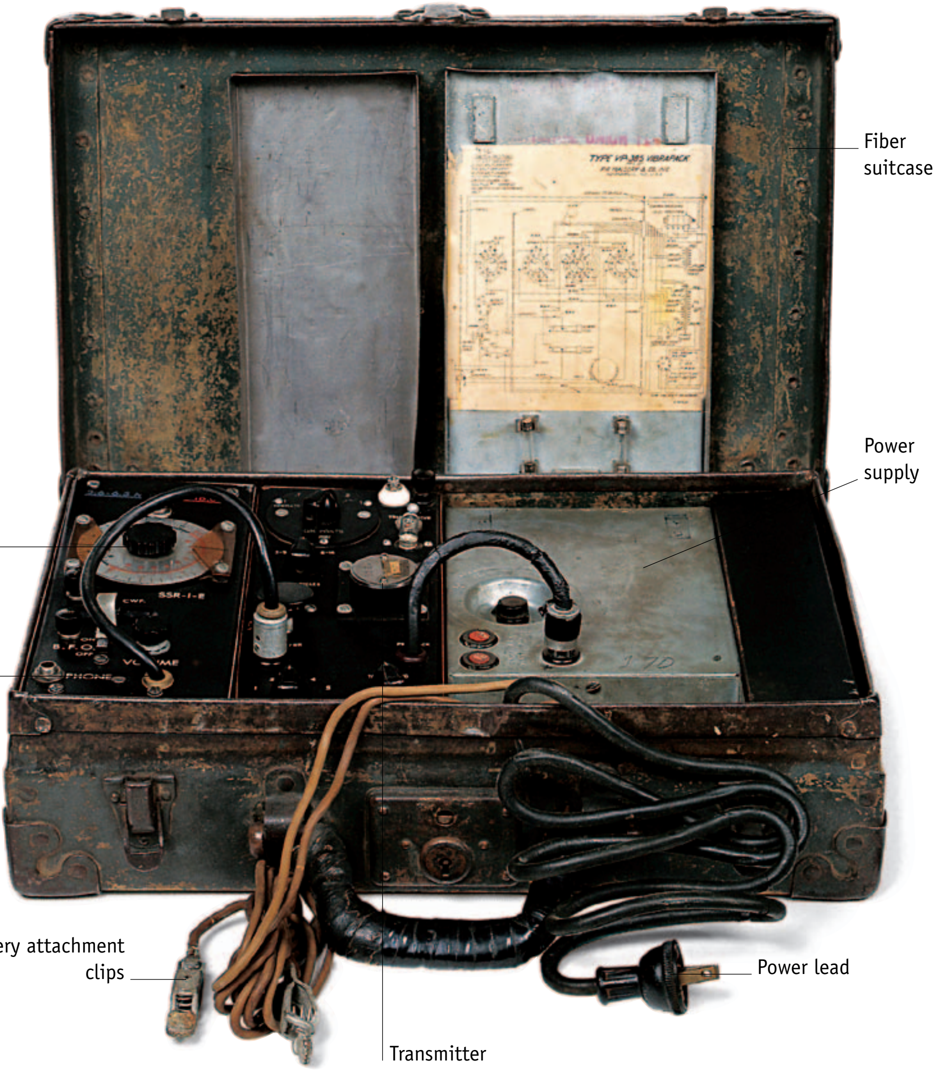
Suitcase radios II

SSTR-1 radio

This transceiver was the standard radio for the OSS (see p. 32). The transmitter, receiver, and power supply were packed in separate boxes for concealment. Often hidden in civilian suitcases for disguise, the radio was packed in the case illustrated here for some operations.

TECHNICAL DATA

Dimensions	4 x 9½ x 3½ in (10 x 24 x 9 cm)
Weight	20–45 lb (9–20 kg)
Range	300–1,000 miles (480–1,600 km)
Power supply	110/220 V AC; 6 V DC; generator
Power output	8–15 W
Transmitter	3.0 to 14.0 MHz in three bands
Receiver	5-tube superheterodyne receiving voice, tone, and Morse

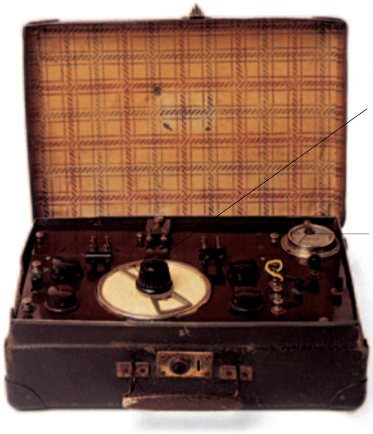


Crystals

Rectifier

Suitcase receiver

This compact 1920s radio was used in World War II by the French intelligence service, which clandestinely monitored German radio traffic for the British.



SOE RADIO SECURITY

During World War II, personnel who used suitcase radios transmitted their messages to receiving stations set up for the purpose. The SOE (see p. 30) established its stations (known as home stations) at various sites around Britain, with staff recruited from the First Aid Nursing Yeomanry (FANY).

To avoid the need for messages to be repeated, all transmissions were recorded—the longer an agent spent transmitting, the greater the danger of capture by the Germans, who had radio direction finding vehicles for hunting clandestine radios.

In the SOE home stations, a system known as fingerprinting was employed to recognize the distinctive Morse signature of each SOE sender. The system also made it possible to detect bogus transmissions made by the Germans on captured radios.

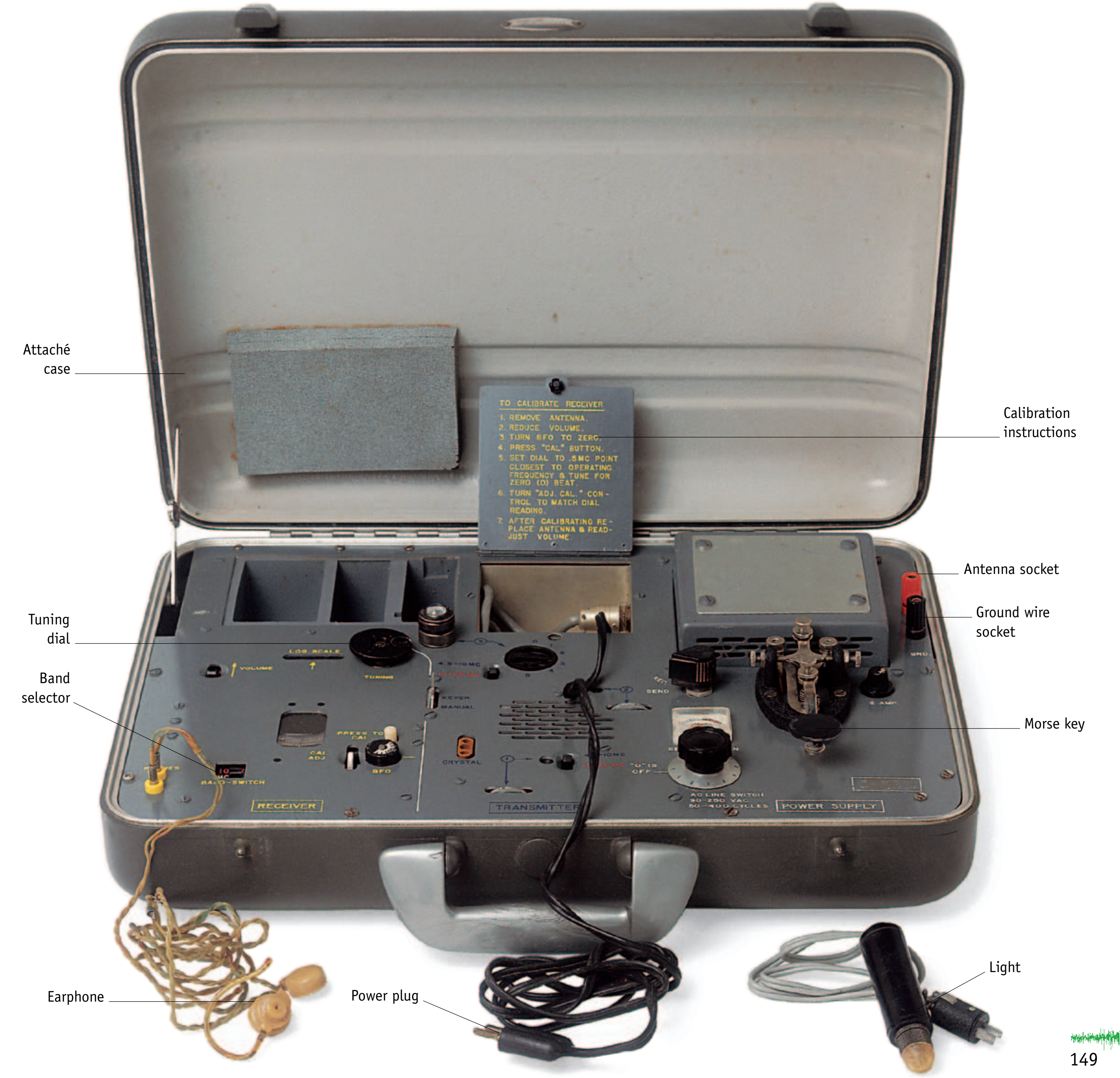
Inside an SOE home station
FANY radio operators at an SOE home station in Britain during World War II listen on sensitive receivers for coded messages that are sent from operatives in occupied Europe.

TECHNICAL DATA

Dimensions	18 x 13 x 4½ in (46 x 33 x 11 cm)
Weight	21 lb (9.5 kg)
Range	300–3,000 miles (480–4,800 km)
Power supply	90–250 V AC
Power output	6–10 W
Transmitter	4.5 to 22.0 MHz in two bands
Receiver	8-tube superheterodyne receiving two bands: voice and Morse

Attaché case radio

In the 1950s, radios were developed to fit into the standard attaché cases carried by business people. This radio could transmit for about 300 miles (480 km) using a short indoor antenna. With a longer outdoor antenna, the radio had a range of about 3,000 miles (4,800 km) for shortwave Morse code messages. This radio was used in Miami during the 1960s to communicate with agents involved in covert operations against the Castro regime in Cuba (see p. 195).



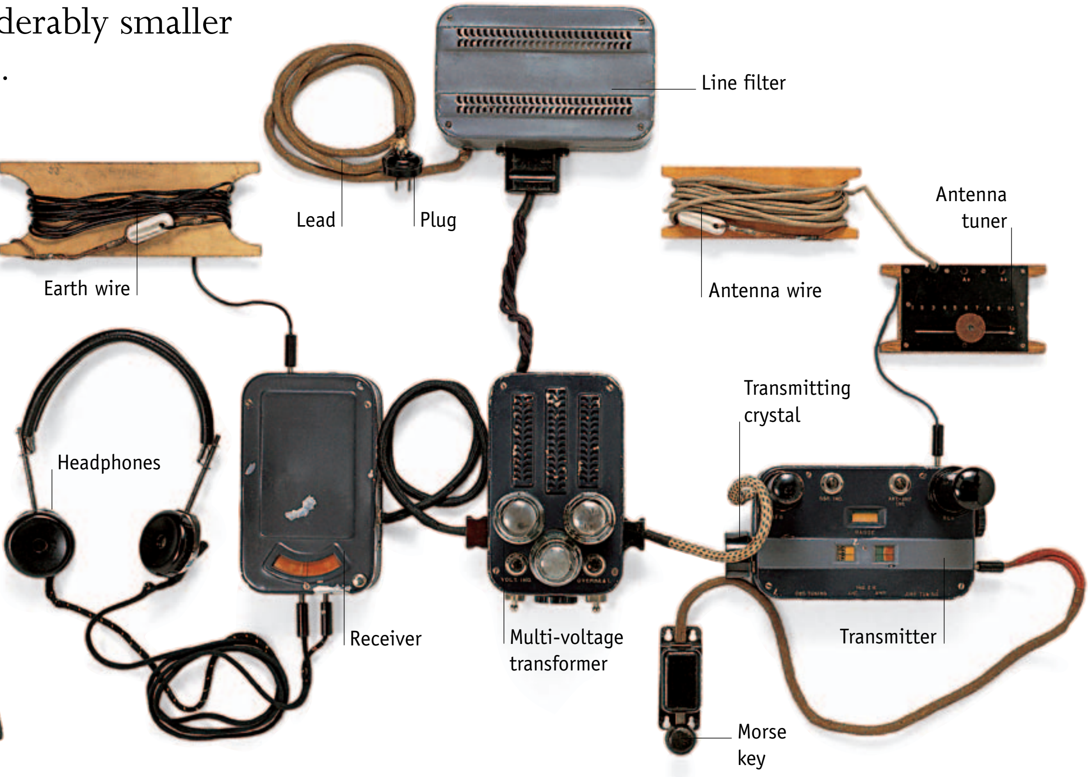
TO CALIBRATE RECEIVER
1. REMOVE ANTENNA.
2. REDUCE VOLUME.
3. TURN BFO TO ZERO.
4. PRESS "CAL" BUTTON.
5. SET DIAL TO .5MC POINT CLOSEST TO OPERATING FREQUENCY & TUNE FOR ZERO (O) BEAT.
6. TURN "ADJ. CAL." CONTROL TO MATCH DIAL READING.
7. AFTER CALIBRATING REPLACE ANTENNA & READJUST VOLUME.

Agents' radios

AGENTS OFTEN USE SPECIAL RADIOS to communicate rapidly with their home bases. Radios may be used when it is important for an agent to communicate with a controller, or when it is necessary to send an intelligence report without delay. As well as being powerful enough to transmit over long distances, agents' radios must be small enough to carry and conceal with ease. World War II agents' radios often comprised two or three major component elements (known as modules), as this made them more portable. With advances in technology since the war, agents' radios have become considerably smaller and can now transmit to satellites.

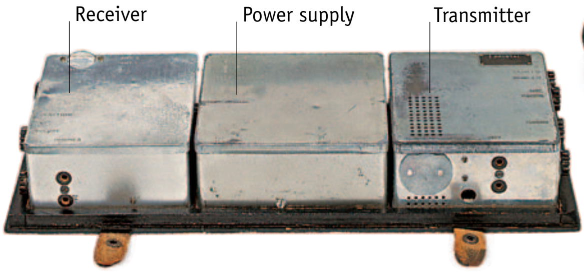
Agents' radio

This type of Soviet equipment was used in the 1950s and early 1960s. Such radios were issued to KGB agents in western Europe and eastern Asia. They could both transmit and receive, and were used to send long-range signals in Morse code to receiving stations in the Soviet bloc. The example shown below was found in Japan in the late 1950s.



Se-100/11 agents' radio

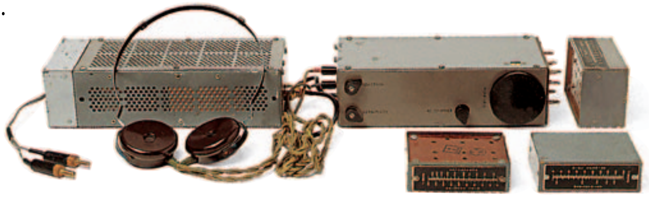
This powerful electrically powered radio was used by German military intelligence (Abwehr) agents. Like most agents' radios of World War II, this outfit was divided into three modules: transmitter, receiver, and power supply. Modular construction made the set portable and easy to hide. It was also simple to assemble quickly.



MCR-1 radio in action
SOE operatives in action use a "biscuit tin" radio to receive coded messages from base.

COMMUNICATING WITH RESISTANCE GROUPS

During World War II, resistance groups made use of radios to receive coded broadcasts from Britain. As well as war news, broadcasts from the BBC provided secret messages from the SOE (see p. 30). The German army, realizing how important radio communications could be for resistance groups, confiscated all shortwave radios in the countries they occupied. SOE radio expert John Brown (see p. 147) designed a special covert radio set, called the Miniature Communication Receiver Mk 1 (MCR-1). This outfit was issued to resistance fighters concealed in cookie tins. Thousands of these portable sets were sent to France during the war for distribution to the SOE and resistance groups.



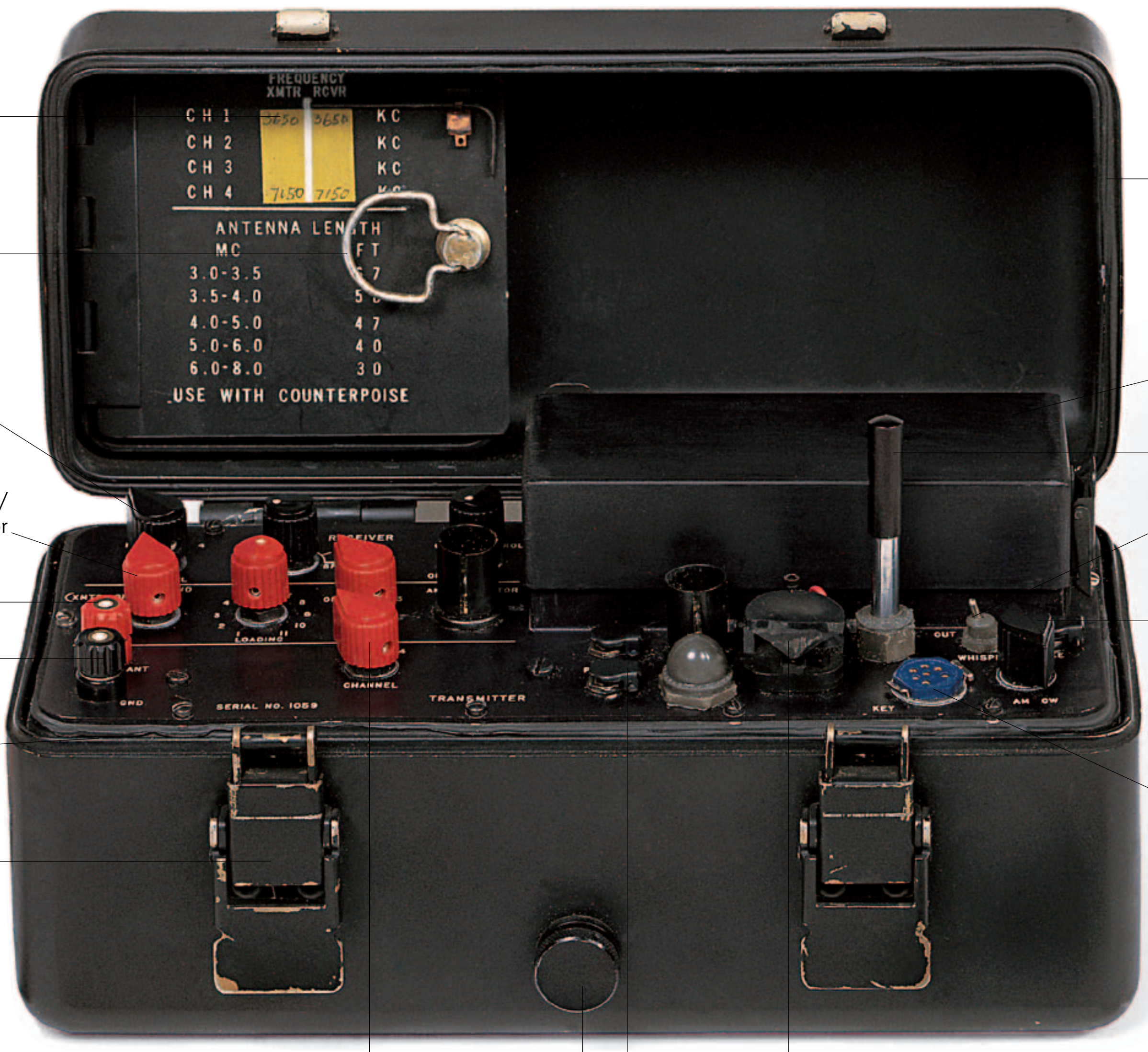
The MCR-1 "biscuit tin" radio
The main parts of the radio could be packed discreetly in cookie tins.

Delco 5300 radio

Used by CIA agents in the 1960s and 1970s, this small but powerful set had a number of advanced features for its time. It could send voice or Morse code transmissions. Messages were transmitted and received on separate frequencies to maintain secrecy. In an emergency, an agent could use a low voice for transmission by using the whisper switch, or even shut down the transmission instantly with the dead-man switch. A GRA-71 burst encoder (see p. 152) could be added to the radio.

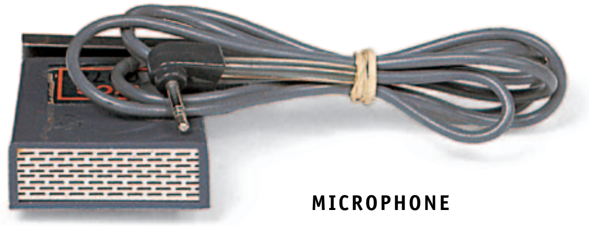
TECHNICAL DATA

Dimensions	10 x 5 x 4½ in (254 x 127 x 114 mm)
Weight	7½ lb (3.4 kg) with battery
Range	Antenna dependent
Power supply	Battery with 4, 12, and 28 volt taps
Power output	5 watts Morse, 1.5 watts voice
Transmitter	Morse/voice; 3 to 8 MHz in four channels
Receiver	Superheterodyne for voice, tone, and Morse; coverage same as transmitter



EARPHONE

REMOTE LEAD



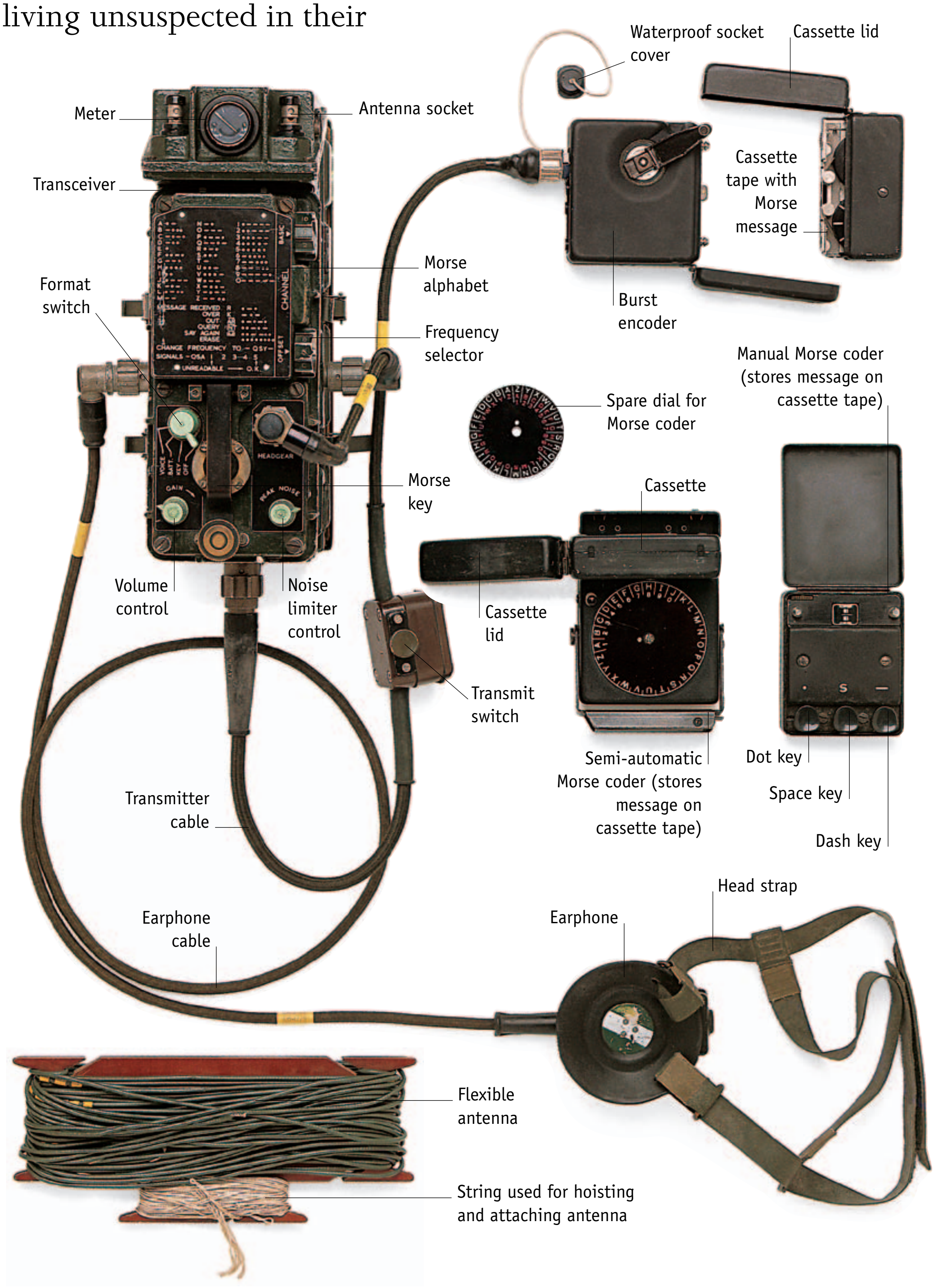
MICROPHONE

Specialized communications

FACE-TO-FACE MEETINGS ARE RISKY, so a variety of specialized devices have been developed to enable agents to communicate with their controllers. Those that facilitate contact within the same locality are known as short-range agent communications (SRAC) devices. For long-distance communications, messages are often sent in Morse code and compressed by means of a burst encoder, which reduces the chances of detection. Special radios are issued to "sleepers"—agents living unsuspected in their target country for years, while leading apparently normal lives. Sleepers tune in to prearranged radio frequencies at set times to listen for coded instructions from their controllers.

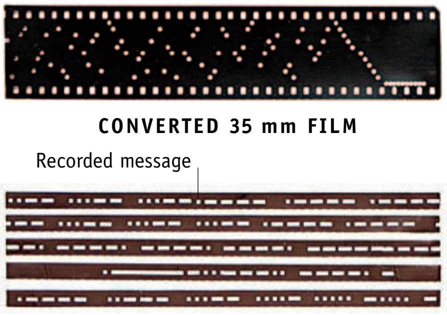
Radio with burst encoder

This equipment was used by the SAS (see p. 178). It consists of a transceiver coupled with a GRA-71 burst encoder, which compresses Morse code messages for transmission in a short burst. This reduces the chance of detection by radio direction-finding equipment.



KGB BURST TRANSMISSIONS

The KGB provided its radio operators who were working abroad in the post-World War II period with specially designed equipment for sending messages back to the Soviet Union. Many of the radio sets that were given to the operators were coupled with equipment for preparing and sending burst transmissions. The equipment used to prepare the tapes, on which the secret messages were recorded in Morse code, had the advantage that it could also be loaded with standard 35mm photographic film, which was always readily available, as an alternative to audio tape.



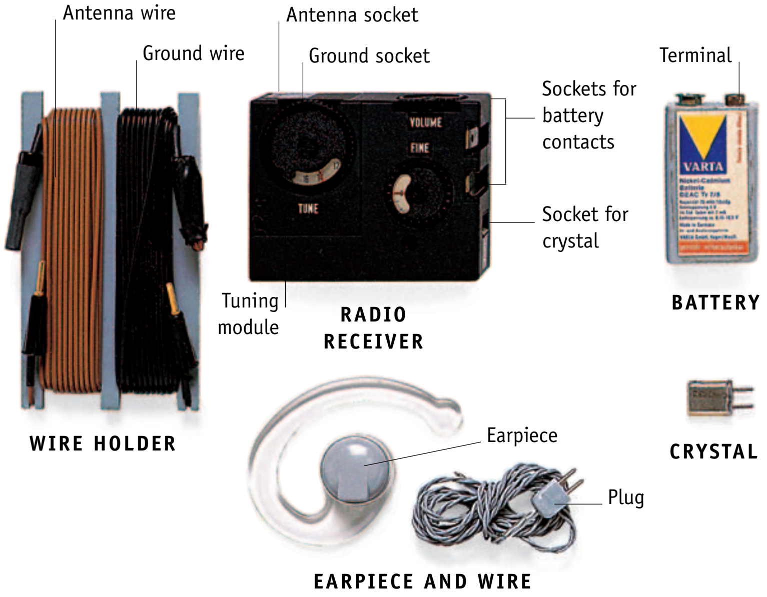
CONVERTED 35 mm FILM

CONVERTED AUDIO TAPE

Burst transmission tapes
Before transmission, the message was recorded in Morse code by punching a series of holes in 35mm film or audio tape.

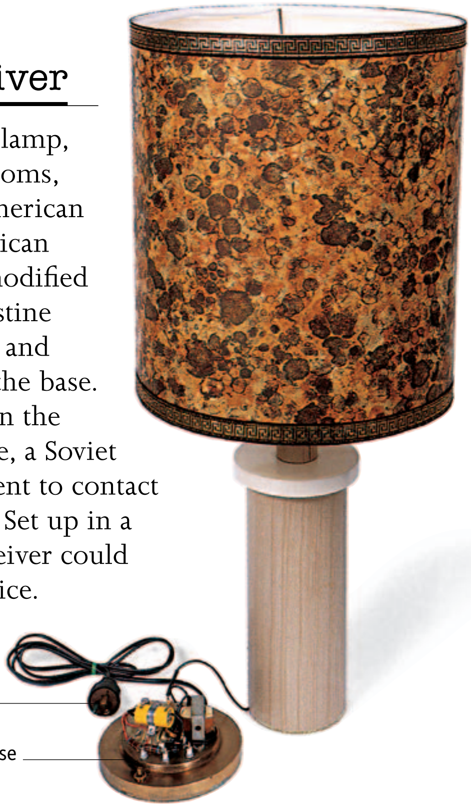
FE-10 agents' receiver

This small East German (HVA) receiver was issued to "sleeper" agents (see opposite) in the 1980s, complete with a signal plan. This stated the agent's call number and gave a transmission schedule and decoding instructions. The receiver was powered by a 9 volt rechargeable battery. Sleeper agents would use the receiver to monitor a variety of frequencies, inserting different crystals in a socket to receive signals on different frequencies.



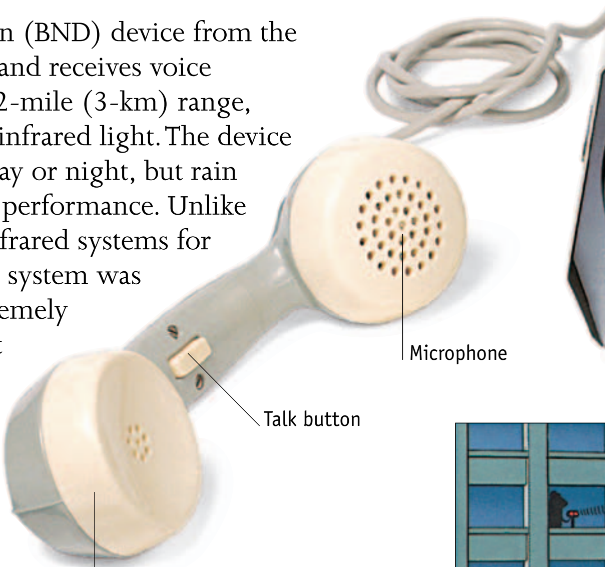
Hotel lamp transceiver

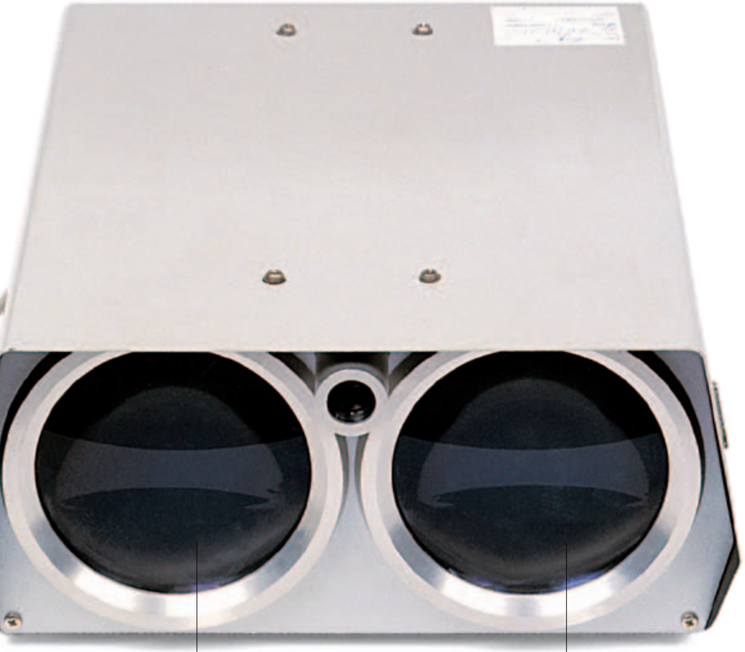
This is a mass-produced table lamp, suitable for use in hotel bedrooms, which was available on the American market in the 1960s. An American intelligence agency covertly modified a number of lamps for clandestine use, installing a radio receiver and transmitter (a transceiver) in the base. Such a lamp could be placed in the hotel bedroom of, for example, a Soviet double agent, enabling the agent to contact his or her controller in secret. Set up in a different way, the lamp transceiver could also be used as a listening device.

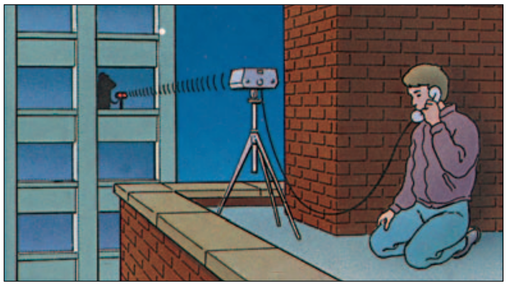


Infrared communication system

This West German (BND) device from the 1960s transmits and receives voice messages over a 2-mile (3-km) range, using a beam of infrared light. The device can be used by day or night, but rain or fog reduce its performance. Unlike contemporary infrared systems for night vision, this system was (and still is) extremely difficult to detect or intercept.







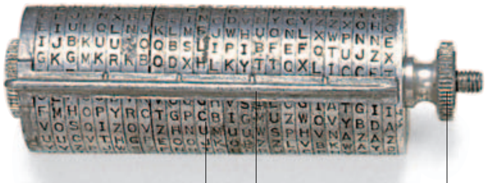
Infrared communication
This type of communication is particularly useful in an urban setting, allowing secure conversation between, for example, agent and case officer. A clear line of sight between the two is essential for the infrared beam to link the transceivers.

Cipher devices

CIPHER DEVICES are used to make messages unintelligible to all except the intended recipient. Essentially, they work by replacing the letters or numbers in a message with other letters or numbers. Early cipher devices used simple letter-for-letter substitution, in which a given letter is always enciphered as the same other letter. In the 1920s, French and American cryptographers (cipher experts) developed machines that used polyalphabetic substitution. In this more sophisticated method, a given letter may be substituted by a different one from a range of possible letters each time it occurs.

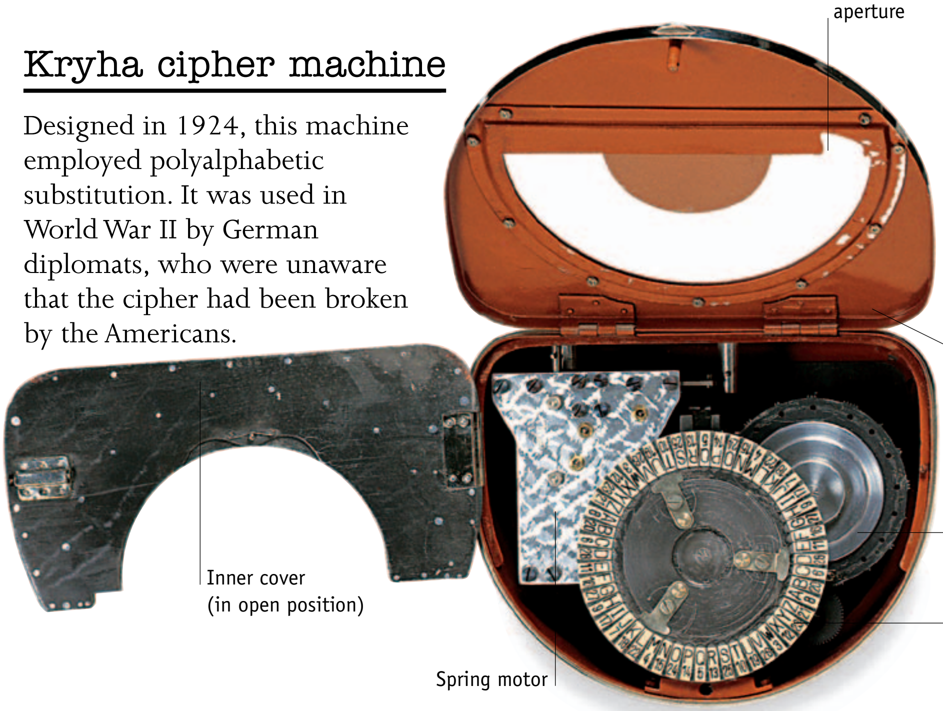
M-94 cipher device

The M-94, based on an 18th-century cipher device, worked by rotating the disks of letters around the cylinder. The M-94 cipher device was used by the US Army from 1922 until 1943, when it was replaced by the Converter M-209.


Disk with letters in random sequence
Bar to align letters on disks
Nut to lock disks in position

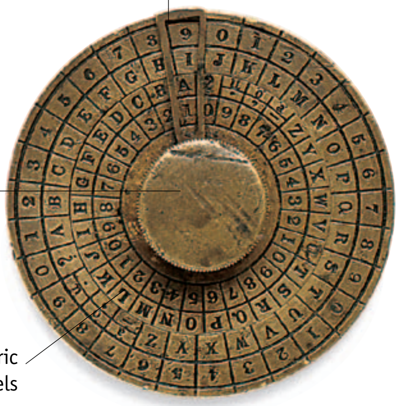
Kryha cipher machine

Designed in 1924, this machine employed polyalphabetic substitution. It was used in World War II by German diplomats, who were unaware that the cipher had been broken by the Americans.



Bolton's patent cipher wheel

This device substituted one letter for another. It is typical of late 19th-century cipher devices and was based on the cipher disk of Leon Battista Alberti, a 15th-century Italian scholar and cryptographer.



THE HEBERN CIPHER MACHINE

EDWARD HEBERN

Edward Hebern (1869–1952) was a self-taught American inventor. From 1909 on he produced a series of electromechanical cipher machines with rotating disks. Hebern's machines were designed to send secret messages between businessmen who were anxious to prevent industrial espionage.

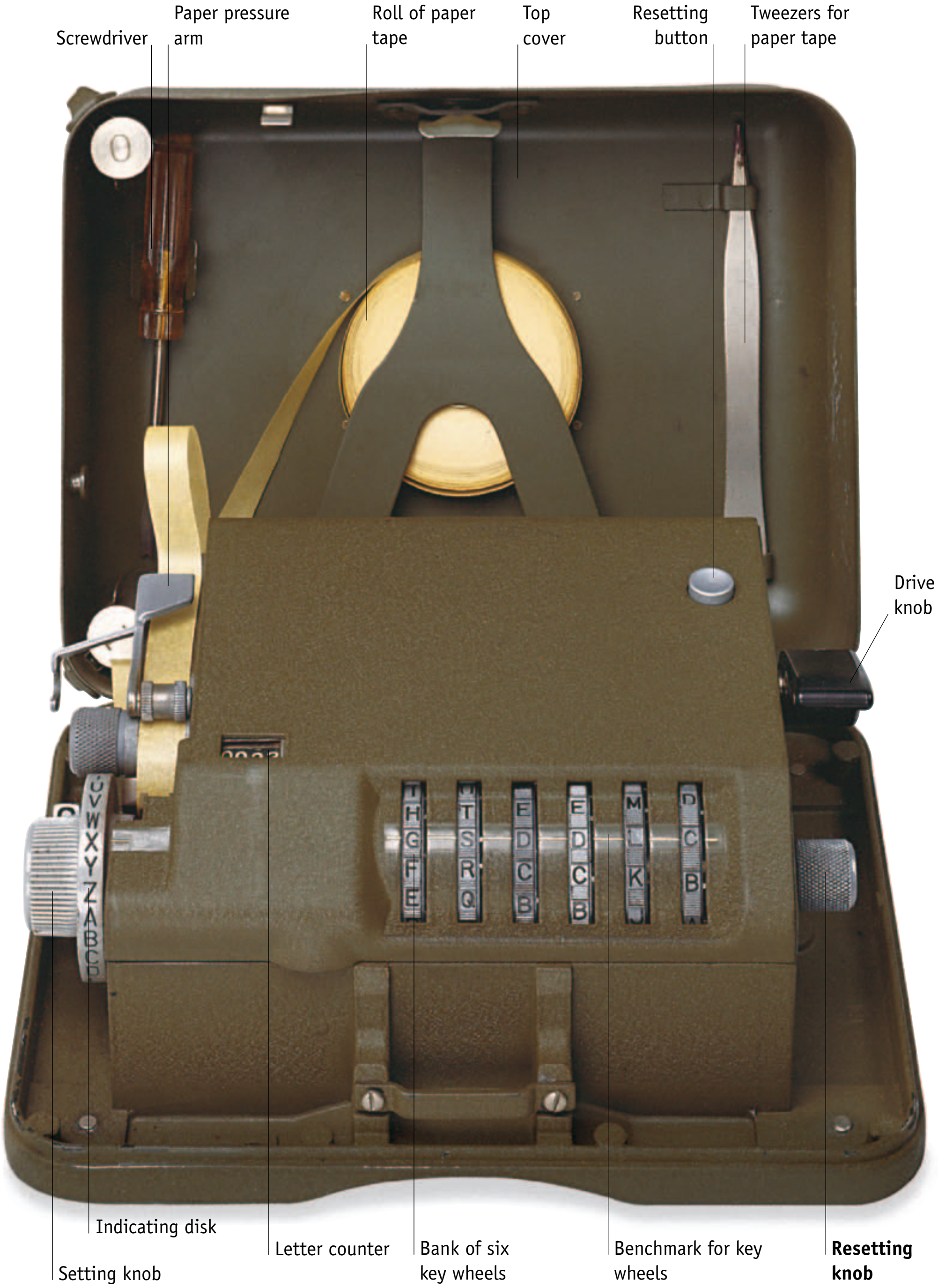
In 1915, Hebern introduced a system in which two typewriters were connected by wires to a rotor in the center. This concept was very advanced for its time, and was later used by the Japanese diplomatic service for its Red ciphers (see p. 36).

The US Navy evaluated this machine, but during testing, the cryptographer William Friedman (see p. 36) broke the cipher. Not deterred, Hebern developed the Mark II, or SIGABA, machine, which became the most secure American cipher system in use during World War II.

1921 HEBERN CIPHER MACHINE

Converter M-209 cipher machine

The Converter M-209 cipher machine was designed by Boris Hagelin and was widely used by the US Army during World War II. It was a compact and portable machine that used a series of rotors to encipher and decipher secret military messages. Once a message was nciphered through the Converter M-209, it printed the text on paper tape in five-letter groups. The message was then transmitted by radio and deciphered. An enciphered M-209 message could be deciphered and printed on another M-209 machine.

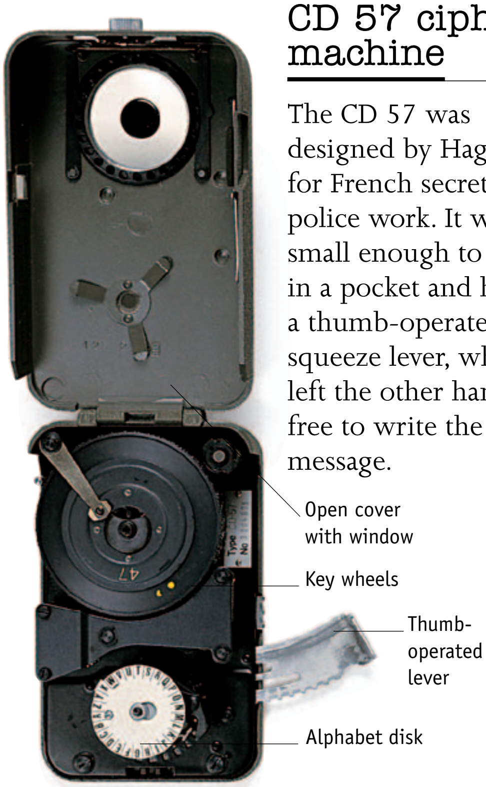


BORIS HAGELIN

In 1934, the Swedish cryptographer Boris Hagelin (1892–1983) designed a cipher machine for the French secret service. He developed this into the Converter M-209, which was used by the US Army. During World War II, more than 140,000 of these machines were produced.

CD 57 cipher machine

The CD 57 was designed by Hagelin for French secret police work. It was small enough to fit in a pocket and had a thumb-operated squeeze lever, which left the other hand free to write the message.



Enigma machine

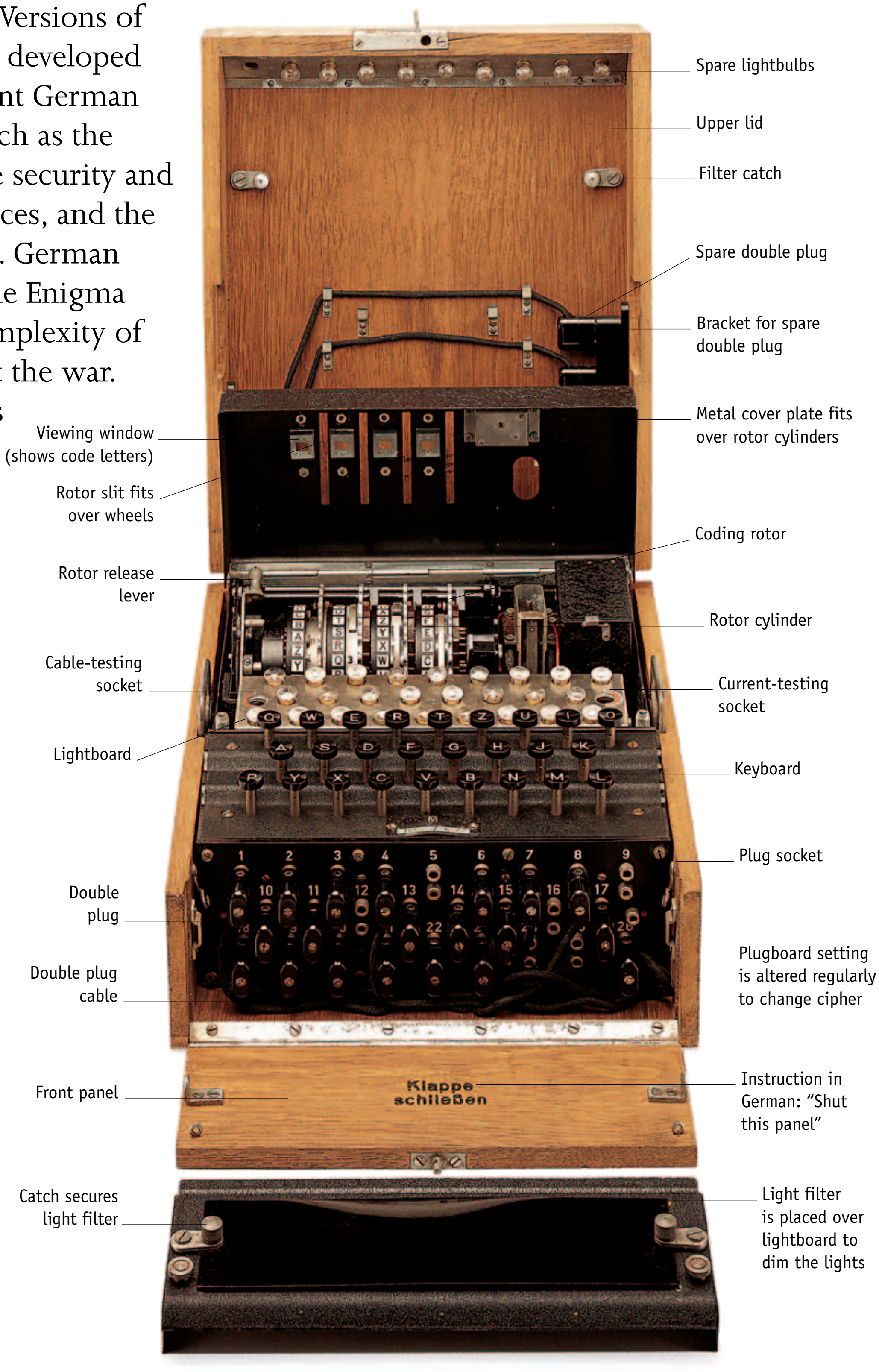
GERMANY'S STRATEGY IN WORLD WAR II was to wage a war of total mobility on land, at sea, and in the air. This required the fastest and most secret communications possible, and the Enigma cipher machine, originally designed to protect the secrecy of business messages, was adopted for this purpose. Versions of the Enigma were developed for use in different German organizations, such as the armed forces, the security and intelligence services, and the diplomatic corps. German refinements to the Enigma increased the complexity of the cipher continually throughout the war. The seizure of German codebooks aided in the continuing ability to break the cipher. The ability to break the cipher is seen by historians as a major actor in the Allied victory in the war.

Japanese Enigma
A special version of the Enigma was made for use by Japan during World War II.

German soldiers using the Enigma
One soldier is typing a message, while another calls out the enciphered letters as they are illuminated. The enciphered letters are being copied down ready for transmission by radio.

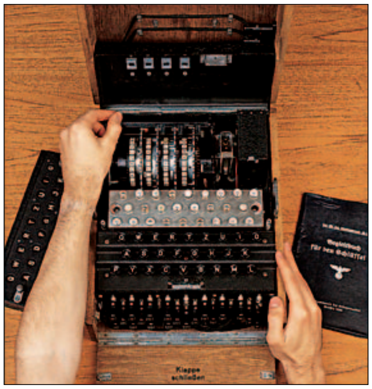
Enigma cipher machine

Invented in 1923, this was a mechanized electric device for enciphering and deciphering messages. Each letter was enciphered separately through a series of plug connections and rotors.

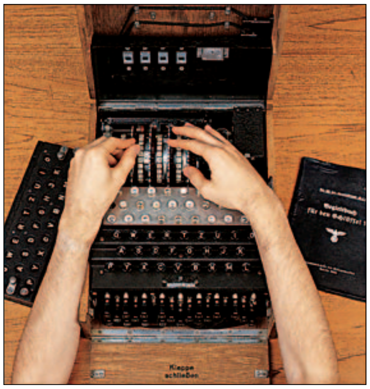

Spare lightbulbs
Upper lid
Filter catch
Spare double plug
Bracket for spare double plug
Metal cover plate fits over rotor cylinders
Viewing window (shows code letters)
Rotor slit fits over wheels
Coding rotor
Rotor release lever
Rotor cylinder
Cable-testing socket
Current-testing socket
Lightboard
Keyboard
Plug socket
Double plug
Plugboard setting is altered regularly to change cipher
Double plug cable
Front panel
Klappe schließen
Instruction in German: "Shut this panel"
Catch secures light filter
Light filter is placed over lightboard to dim the lights

Mechanism of the Enigma

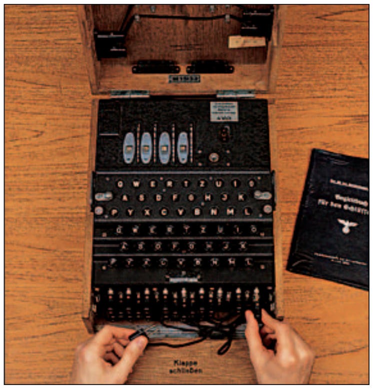
The key to the security of the Enigma lay in the way the machine was set up. The order of the machine's alphabetical rotors, which were arranged on the rotor cylinder, and their internal wiring could be altered. The cipher was determined by the initial settings of these rotors. The plugs were inserted in the plugboard in any combination. All these variables—the key settings—were changed on a regular basis. Even if an enemy had a machine identical to the one used to create a message, he could not break the cipher without also learning the key settings used when the message was enciphered.



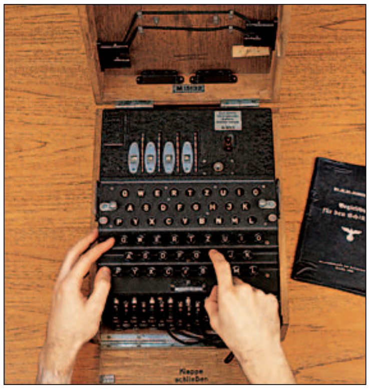
1 A lever is lifted to release the rotors. The rotors are removed and the internal wiring, known as the "ring setting," altered. The rotors are put back in the order specified in the current instructions.



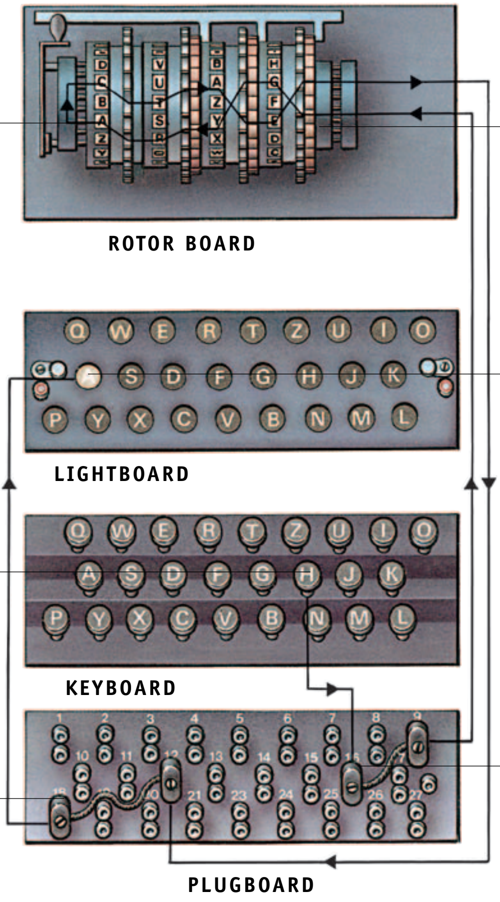
2 A letter from each rotor shows through the windows of the cover. The rotors are turned until the letters are arranged as specified in the current instructions. These letters form the "ground setting."



3 Once the rotors are positioned correctly, the cover is shut over them. Then the connections on the plugboard are changed: they are manipulated to link pairs of letters specified by the operator's codebook.



4 The Enigma operator picks four random letters and enters them twice. The resulting eight-letter cipher is used as a message prefix. Before enciphering the message, the rotors are set to show the four random letters.



5 The first letter of a message is typed on the keyboard. The letter H is used as an example to show the enciphering process.

6 An electrical signal from H travels to 16 then 9 on the plugboard. At this stage, the letter is changed.

7 A signal from 9 passes through the rotor cage and is altered each time it passes through a rotor.

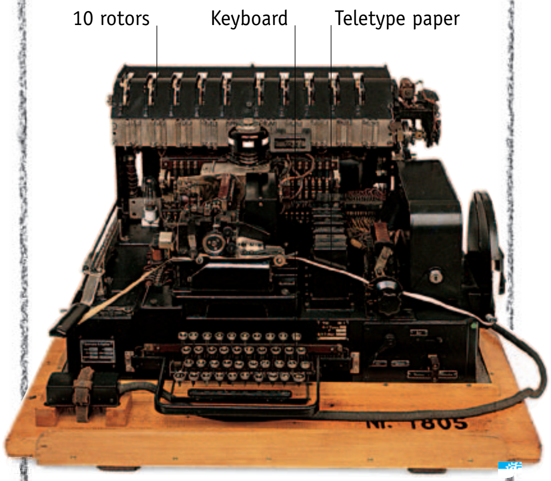
8 A reflecting disk at the end of the row of rotors reflects the signal back through the rotors.

9 The signal returns to the plugboard, in this example to 12. It is rerouted by a connection to 18.

10 The signal goes to the lightboard. It lights A, which then becomes the first letter of the enciphered message. This procedure is repeated for each letter of the message.

THE GEHEIMSCHREIBER

A more complex cipher device than the Enigma was the Geheimschreiber. It had either 10 or 12 rotors, which made enciphered messages extremely difficult to break. The Geheimschreiber was very large and was installed only in main communications centers, in Germany itself or in German-held territories.



GEHEIMSCHREIBER, SIEMENS MODEL (CODENAME STURGEON)

Ciphers and secret writing

SPIES OFTEN NEED TO WRITE messages that cannot be discovered or understood by the enemy. A written message can be encrypted by means of a cipher device (see p. 154) or with a cipher system such as a one-time pad, which, if properly used, is completely safe from code-breakers. (For the difference between a code and a cipher, see the glossary, p. 216.) Messages can also be hidden by means of secret writing, which is normally done by one of two methods: the wet system, in other words writing in invisible inks; and the transfer system, in which a piece of chemically impregnated paper, known as a carbon, transfers ink to a piece of normal paper when this is placed beneath it.

GERMAN WORLD WAR I INVISIBLE INK AND SPONGE

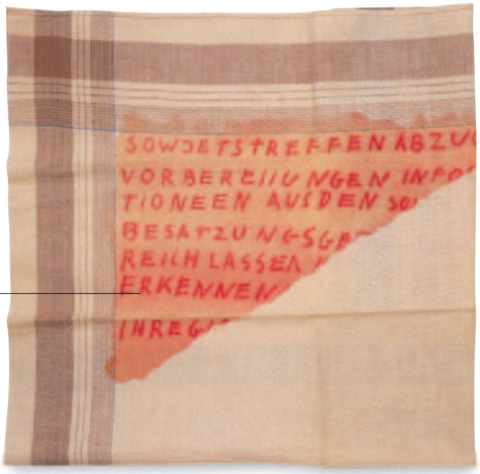
HERBERT BOECKENHAUPT

SPY PROFILE

Herbert Boeckenhaupt (b.1942) was a US Air Force radio communications specialist. As a young man, he volunteered to work for the Soviet Union for money. From 1962 until his arrest in 1966, Boeckenhaupt sent American military secrets to the KGB, often using secret writing. After his arrest, instructions concerning a dead drop, on 35mm film, and secret writing carbons were found in Boeckenhaupt's home.

Handkerchief with secret writing

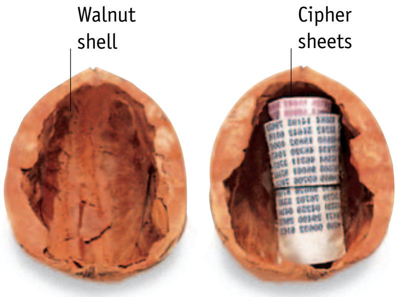
Some invisible inks may be used on cloth as well as on paper. This handkerchief message was prepared by the BND in West Germany in the 1960s. It concerns a meeting that is about to take place and information that will arrive from East Germany.



Section where a chemical has been applied to reveal message

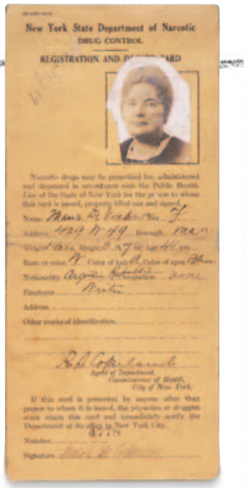
Cipher sheets in walnut shell

Rolled up inside this walnut shell, which was found in the possession of a Soviet agent in former West Germany, are two cipher sheets from one-time pads.



MADAME DE VICTORICA

US Military Intelligence intercepted a letter written in secret ink to a suspected German spy during World War I. The letter was traced back to Madame Marie de Victorica (1882–1920), who lived in New York. On her arrest in April 1918, she was found to own two silk scarves that were impregnated with water-soluble secret inks. She was indicted on spying charges but, as she offered to work for the government, she was not tried. She was a heroin addict, and the authorities supplied her with drugs to ensure her cooperation. Her drug control card is shown here.



New York State Department of Narcotic
DRUG CONTROL

REGISTRATION AND [illegible] CARD

Narcotic drugs may be prescribed for, administered and dispensed in accordance with the Public Health Law of the State of New York for the person to whom this card is issued, properly filled out and signed.

Name Marie de Victorica Sex F
Address 429 W 49 Borough Man
Weight [illegible] Height [illegible] Age [illegible]
Race or color W Color of hair [illegible] Color of eyes Blue
Nationality Argentine Republic Occupation [illegible]
Writer
Employer
Address
Other marks of identification

R. S. Copeland
Agent of Department.
Commissioner of Health,
City of New York.

If this card is presented by anyone other than person to whom it is issued, the physician or druggist must retain this card and immediately notify the Department at its office in New York City.

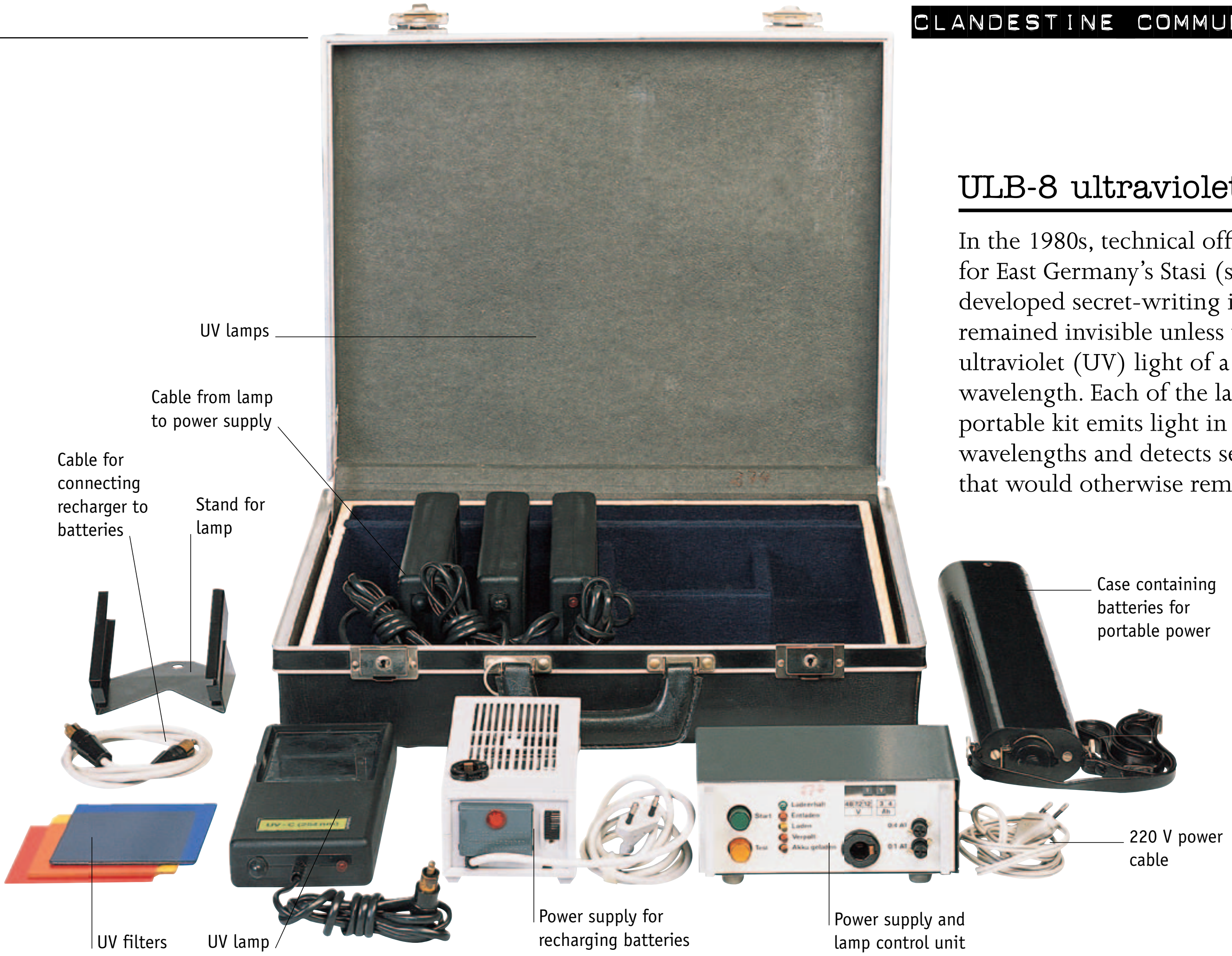
Number [illegible]
Signature Marie de Victorica

DRUG CONTROL CARD

Sub-latent photographic image

Secret writing can be concealed by printing a photograph over it. The message is revealed by applying chemicals that remove only the top image. This photograph was used in the 1960s by the East German security service to cover a layer of secret writing, part of which has been revealed. Once a message has been concealed in this way it can be carried safely without fear of detection. Radio communication plans are often hidden in this way.

Section where a chemical has been applied to reveal message

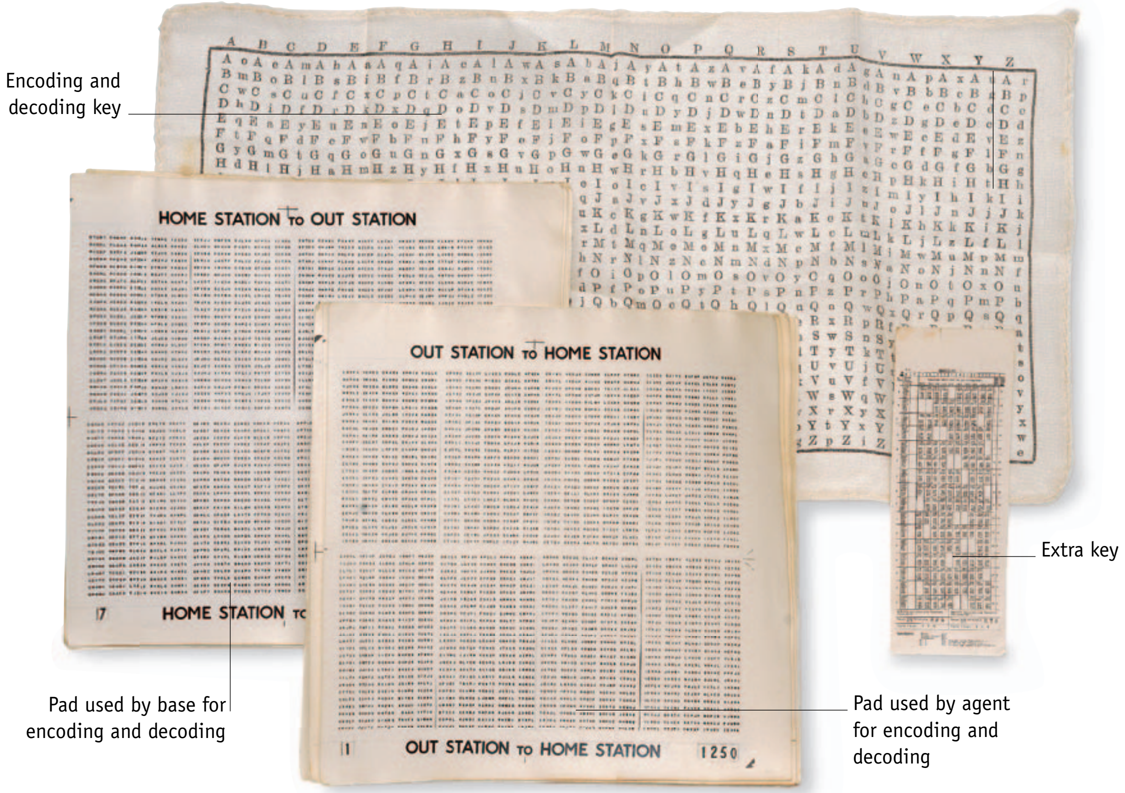

UV lamps
Cable from lamp to power supply
Cable for connecting recharger to batteries
Stand for lamp
Case containing batteries for portable power
220 V power cable
UV filters
UV lamp
Power supply for recharging batteries
Power supply and lamp control unit

ULB-8 ultraviolet light set

In the 1980s, technical officers working for East Germany's Stasi (see p. 99) developed secret-writing inks that remained invisible unless viewed using ultraviolet (UV) light of a specific wavelength. Each of the lamps in this portable kit emits light in one of four wavelengths and detects secret writing that would otherwise remain hidden.

One-time pads

The one-time pad system of enciphering was first used by the German diplomatic service during the 1920s. Both sender and recipient have an identical pad of cipher sheets, each of which is used to encipher a single message and then destroyed. As the cipher is never repeated, it is theoretically unbreakable. However, if an opposing intelligence agency were to obtain a copy of one of the pads, the message might be compromised. In 1943, the system was adopted by the SOE (see p. 30). Pads, and the keys that were used for encoding and decoding, were printed on silk for its durability and ease of transportation.

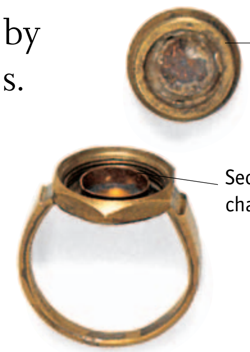

Encoding and decoding key
HOME STATION TO OUT STATION
HOME STATION TO
OUT STATION TO HOME STATION
OUT STATION TO HOME STATION
1250
Extra key
Pad used by base for encoding and decoding
Pad used by agent for encoding and decoding

Microdots I

MICRODOTS ARE TINY PHOTOGRAPHS of messages, secret documents, or other images which are so small that they can be read only with a magnifying viewer. The camera and the method shown on these pages produce microdots as small as 1 mm in width; but cameras exist that can produce even smaller microdots. Historic accounts indicate that microphotography was used by spies and couriers during the Civil War in the 1860s. The KGB trained some of its agents, including its American spy Robert Thompson, to produce and conceal microdots. Methods of concealment include secret chambers in rings and coins, or a tiny piece of film that can be embedded in the edge of a postcard. Microdots are read with special viewers, and these, too, are often skillfully concealed.

Concealments

Microdots can be concealed in everyday objects or in special concealments. The German coin could conceal hundreds of microdots. The ring, designed during World War II, concealed either microdots or a compass. The slitter made incisions in the edges of postcards in which microdots could be hidden.



RING

POSTCARD SLITTER

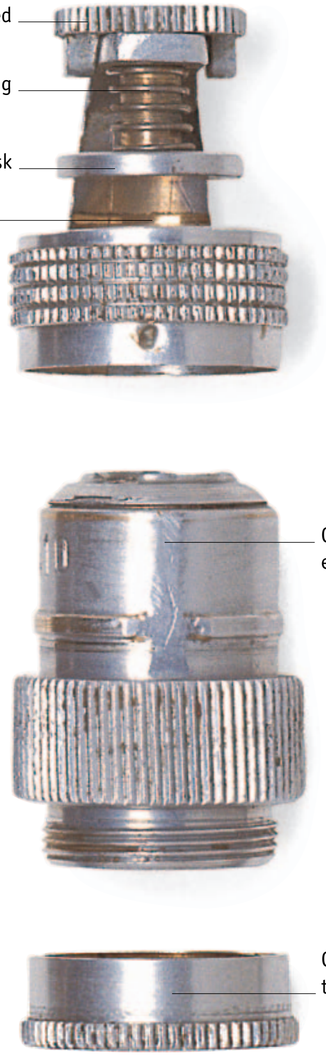
COIN

Microdot camera

The intelligence agencies of former Soviet bloc countries, such as East Germany, used this miniaturized microdot camera. Shown actual size and enlarged, this camera could be hidden easily. It was used to make the three microdots shown on the right, also actual size. The camera produces a finished microdot from the original photograph, without using an intermediate negative.

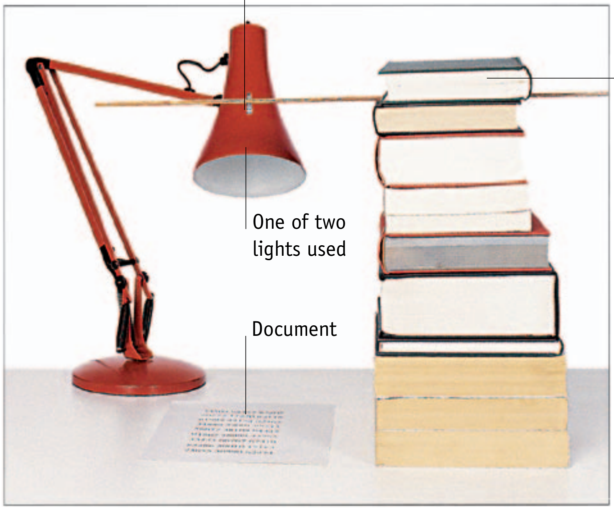
MICRODOT CAMERA (ACTUAL SIZE)

MICRODOTS (ACTUAL SIZE)


Top opens to allow film to be inserted
Spiral spring
Film retaining disk
Film placed here
Container for lens elements
Cap acts as a shutter for the long exposures used

MICRODOT CAMERA (ENLARGED)

PEN CAP


Microdot camera fits in hole made in ruler
Books hold ruler at correct height
One of two lights used
Document

Using a microdot camera
The camera is attached to a ruler and positioned above the document to be photographed, using a stack of books. Each type of camera must be held securely at a specific distance from the document. Depending on the kind of film being used, the exposure time may be up to several minutes long.

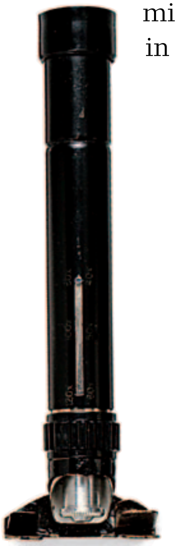
ROBERT GLENN THOMPSON

SPY PROFILE

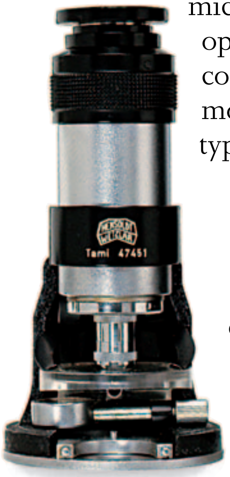
In 1965, Robert Glenn Thompson (b.1935), a former member of the US Air Force Office of Special Investigations, was arrested and given a 30-year jail sentence for passing secrets to the KGB. He was trained by the KGB in Moscow in 1957, learning secret writing techniques, microphotography, and how to use a Minox camera. In 1978 Thompson was involved in a spy swap deal that allowed him to go to East Germany in exchange for an Israeli pilot.

Microdot readers

In order to read microdots, agents need high-powered magnifying devices. These can range from specially designed miniature viewers, small enough to be concealed in a cigarette, to commercially produced pocket microscopes. Agents operating in hostile countries prefer the most easily concealed types of readers.



MICRODOT VIEWER (EAST GERMAN)



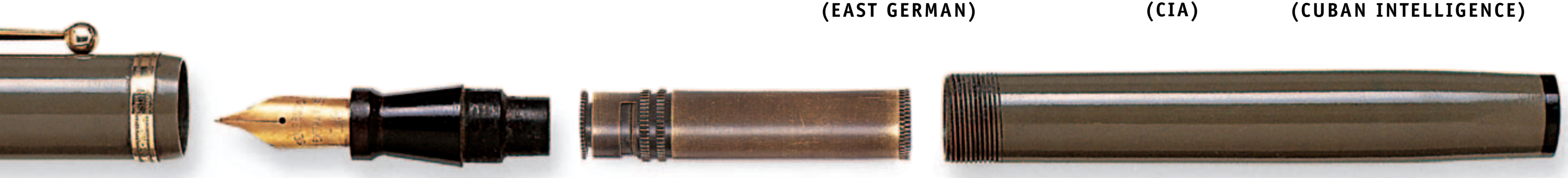
POCKET MICROSCOPE (CIA)

Viewer small enough to fit in a cigarette

MINIATURE MICRODOT VIEWER (CUBAN INTELLIGENCE)

Fountain pen viewer concealment

This East German microdot viewer is concealed within a 1950s fountain pen. A small ink sac could be installed, allowing the pen to work so that it would not arouse suspicion if examined. The pen would be used to transport the viewer between secure hiding places, or conceal it inside a desk.



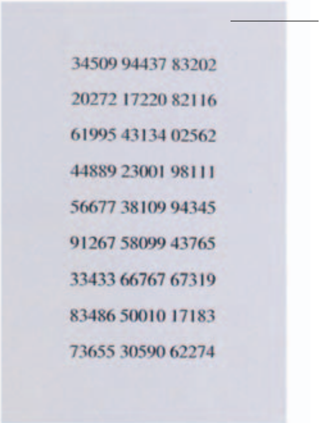
FOUNTAIN-PEN NIB

MICRODOT VIEWER

PEN BODY

How to make a microdot

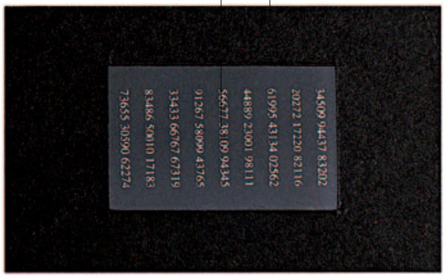
A microdot can be made with a high-quality 35mm camera by using a two-stage technique known as the British Method, which is shown here. Using high-contrast black-and-white film, a photograph of a document is taken so that the image of the document fills the whole frame of the film. The film is processed and the resulting negative is mounted in an opening cut in a piece of black cardboard. When lit from behind, the text on the negative shows up as white on black. This image is photographed from a distance of 4 ft 2 in (127 cm)—with a lens of focal length 50mm—to produce a black-on-white image that occupies a 1 mm length of the resulting negative. This tiny image is cut out to produce a microdot.



34509 94437 83202
20272 17220 82116
61995 43134 02562
44889 23001 98111
56677 38109 94345
91267 58099 43765
33433 66767 67319
83486 50010 17183
73655 30590 62274

Original document (in code)

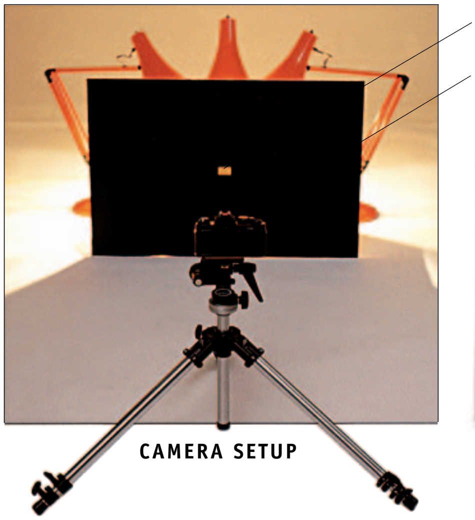
DOCUMENT



Negative mounted in opening

Black cardboard with central opening

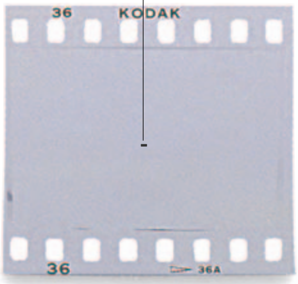
MOUNTED NEGATIVE



Mounted negative

Camera in position

CAMERA SETUP



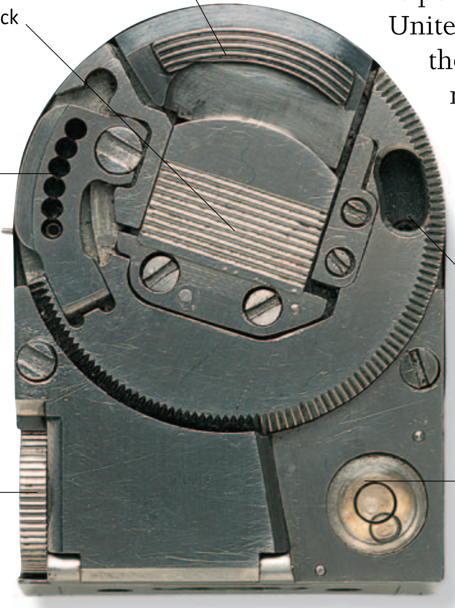
Microdot

MICRODOT ON NEGATIVE

Microdots II

Microdot system

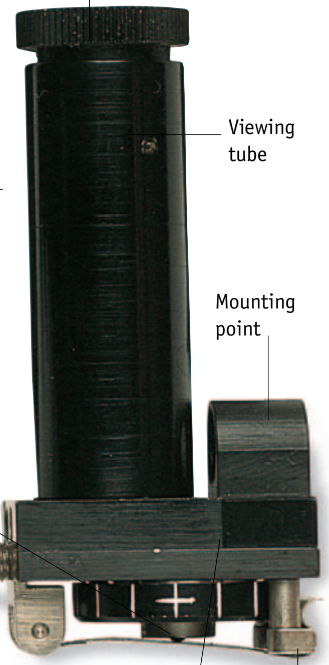
This pocket-sized microdot system was made in the United States. It photographs the document, develops the image, dries the film, and allows the finished microdot to be punched out into the agent's hand. The camera's stainless-steel body allows developing chemicals to be poured directly into it, eliminating the need for other equipment. Its small size makes it easy to conceal.


Thumb lever
Sliding lock
Punch
Film advance
Pouring point for chemicals
Built-in level ensures system is kept level during film photography

FILM DISK

Uranus-M camera and viewer

This East German Uranus-M camera and viewer could produce a microdot and could also be used for viewing the microdot in its film disk after development. Without the viewing tube, the tiny camera could be effectively hidden inside a hollow 35mm film cassette.



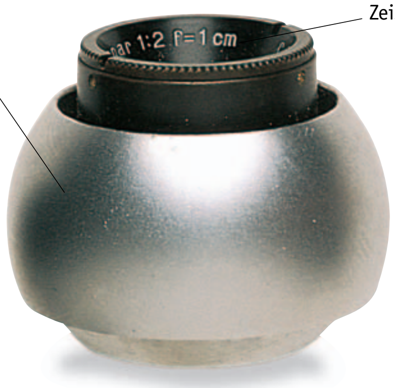
MICRODOT CAMERA AND VIEWER

LUCIEN NIKOLAI

Colonel Nikolai (1928–2000) joined the NKVD (the predecessor of the KGB) in 1944 and was part of the graduating class of its first special Operational-Technical (OT) college in 1948. In the 1950s, Nicholai traveled throughout Europe providing secret tradecraft training to KGB "illegals" such as Rudolf Abel (see p. 208) and Konon Molody (see p. 50). In 1978, he was appointed head of the OT photographic department in the KGB's First Chief Directorate, where he pioneered special cameras and clandestine techniques for microdots and document copying.

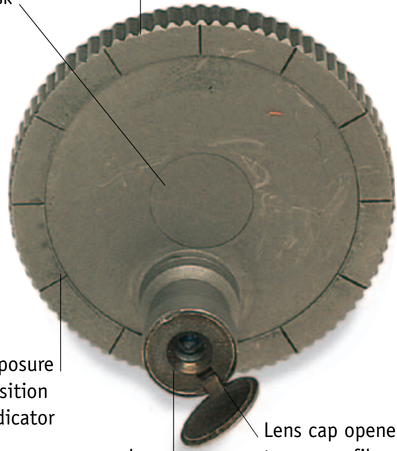
Sliva microdot system

The KGB used the Sliva with a 100 W lightbulb, magnifying glass, and 35mm negative (of a document) to make microdots. The Zeiss lens of the Sliva focused the image from the negative onto a piece of cellophane, directly underneath the lens, that had been converted into high-resolution film using a collodion emulsion.



Mk IV microdot camera

This small camera is less than 1 in (25 mm) in diameter and produces 12 microdots onto a round film disk. Only the tiny lens protrudes from the flat surface of the camera, which could be disguised as a large coat button. The Mk IV is the only microdot camera officially acknowledged by the CIA.

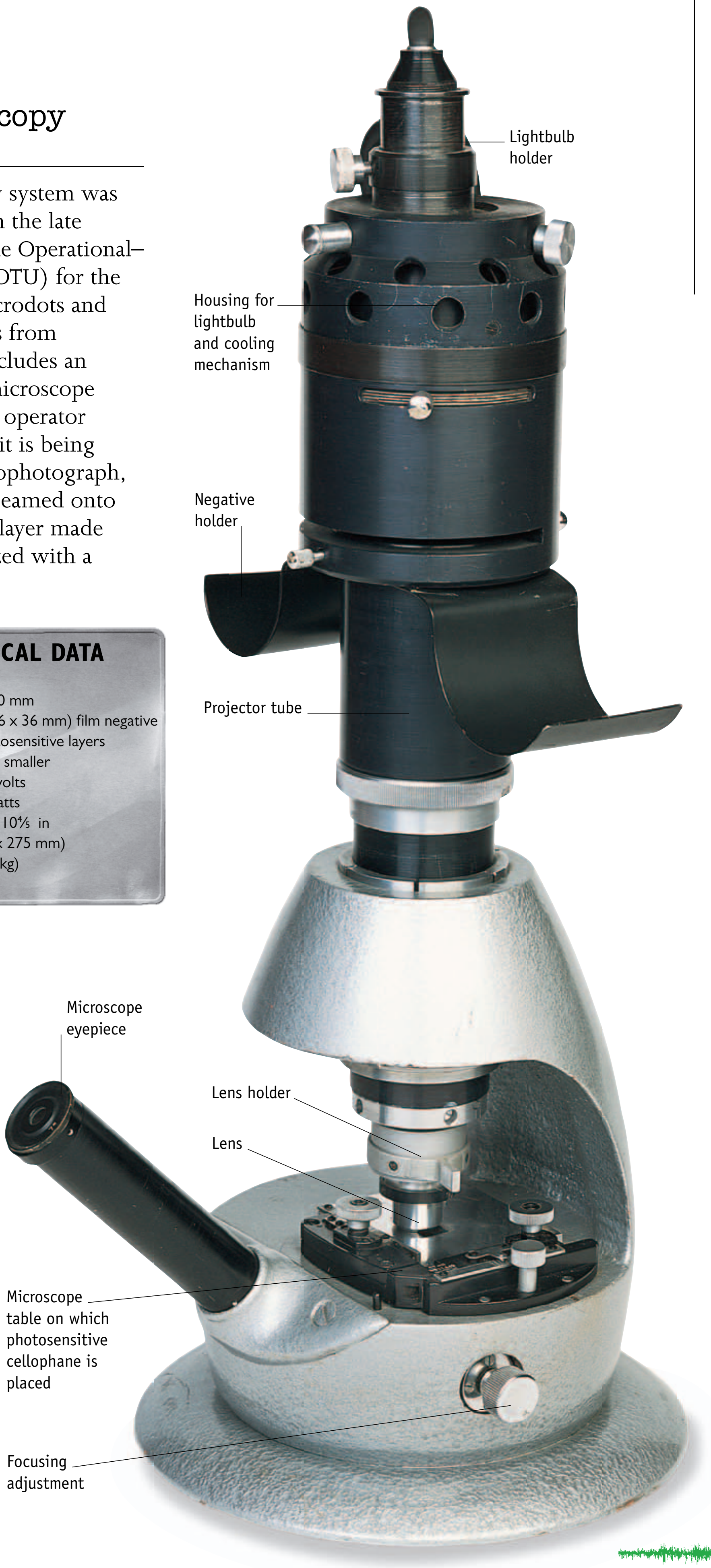

Metal body containing round film disk
Serrated outer ring held while inner film disk rotated for each exposure
Exposure position indicator
Lens
Lens cap opened to expose film

Bagulnik microcopy system

The Bagulnik microcopy system was developed by the KGB in the late 1960s. It was used by the Operational–Technical Department (OTU) for the quick production of microdots and other microphotographs from negatives. The system includes an image projector and a microscope table, which enables the operator to observe the image as it is being formed. To make a microphotograph, the negative's image is beamed onto a special photosensitive layer made from cellophane sensitized with a collodion emulsion.

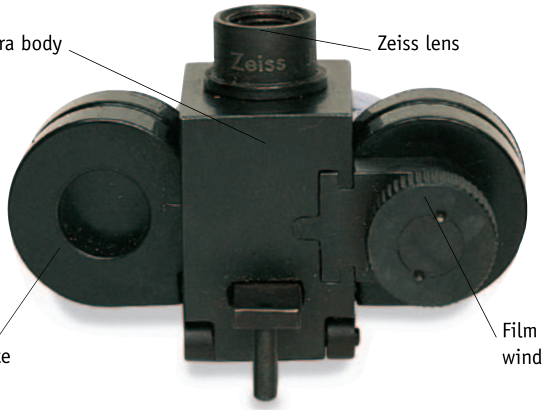
TECHNICAL DATA

Date	Late 1960s
Lens	Zonnar f2 10 mm
Document size	1 x 1⅜ in (26 x 36 mm) film negative
Film type	Special photosensitive layers
Microdot size	1 x 1 mm or smaller
Voltage	127 or 220 volts
Copy lamp	30 or 75 Watts
Dimensions	16½ x 7⅞ x 10⅘ in (420 x 200 x 275 mm)
Weight	26½ lb (12 kg)


Lightbulb holder
Housing for lightbulb and cooling mechanism
Negative holder
Projector tube
Microscope eyepiece
Lens holder
Lens
Microscope table on which photosensitive cellophane is placed
Focusing adjustment

Uranus-2 microdot camera

In this East German device, a Zeiss lens has been attached to a standard Minox film cassette to create a small, easily concealable microdot camera. Separated from the cassette, the camera could be hidden inside a matchbox. Minox cassettes were used because they were readily available and reloadable with the high-resolution films necessary for producing microdots.



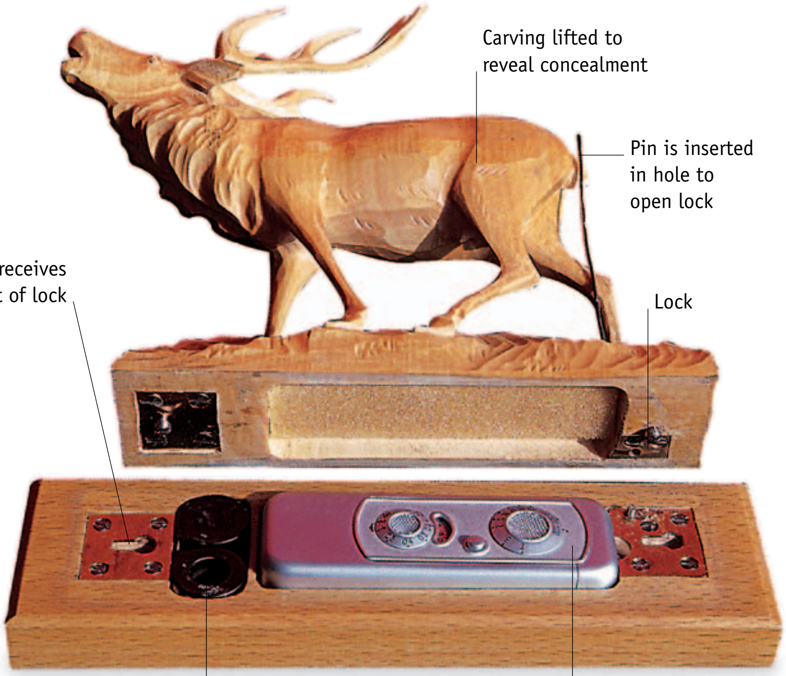
Concealments I

MANY INGENIOUS CONCEALMENTS have been devised to allow spies to hide information and equipment. They vary widely in size and format. The basic principle followed is to disguise or hide the item concerned so that it appears to be an innocent object that will not arouse suspicion. It is essential that the concealment used is in keeping with the lifestyle and circumstances of the agent equipped with it. Some concealments are made specifically for the purpose; others are converted from everyday objects. Some are booby-trapped, so that unauthorized attempts to open them will result in the destruction of their contents. Frequent use is made of reverse threads, which unscrew clockwise, rather than counterclockwise, as is usual.

STATUETTE

Statuette concealment

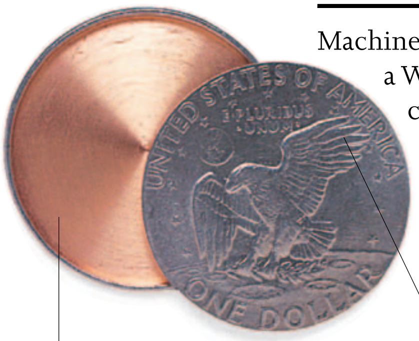
This wooden carving of an elk covers a secret storage place for a subminiature camera. The elk can be lifted to reveal a compartment containing a Minox IIIS camera complete with a spare cassette of film. The statuette was found by the West German counterintelligence service (BfV) in the apartment of an East German spy who had been operating in West Germany during the Cold War period.

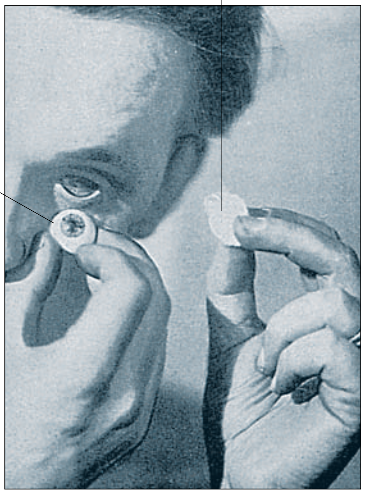

Carving lifted to reveal concealment
Pin is inserted in hole to open lock
Slot receives bolt of lock
Lock
Spare film cassette
Camera

CONCEALMENT IN BASE

Silver dollar concealment

Machined from two real 1978 coins for a Western intelligence service, this concealment was used to hide microfilm and one-time pads. It is opened by pressing on the eagle's wing tip.


Point that is pressed to open coin
Bottom half of hollow coin



Eye concealment

This German photograph dates from the period between the two World Wars. It illustrates the use of an artificial eye to conceal and transport a secret message.

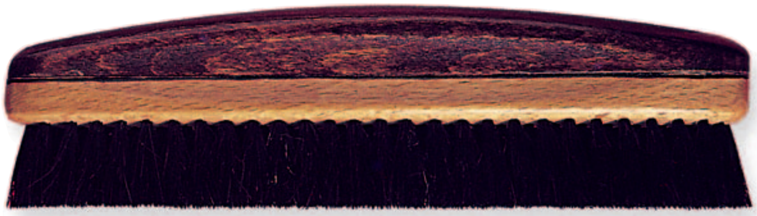
MARIA KNUTH

SPY PROFILE

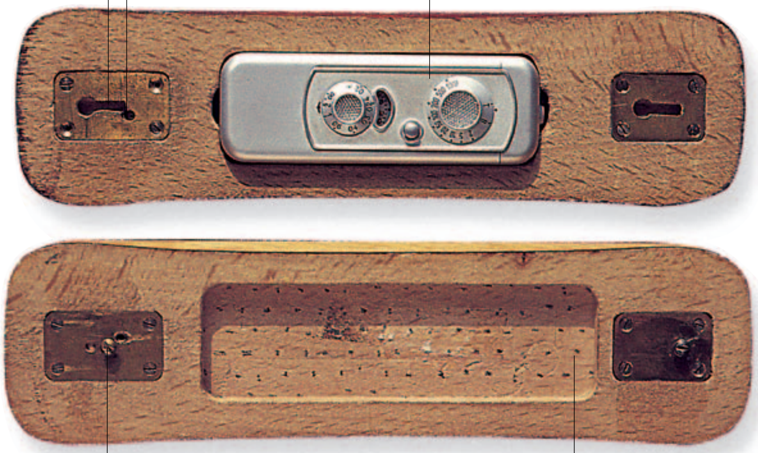
Polish intelligence recruited German Maria Knuth in 1948. She specialized in seduction as a means of recruiting agents to her side. Her first job was as a "letter box" for a spy ring in West Berlin. She was equipped with a number of concealment devices to hide microdots and sheets from one-time cipher pads. Later she attempted to recruit a member of West German counterintelligence (BfV), which led to her arrest in May 1952. She died in prison in 1954.

Brush concealment

Minox cameras were hidden in a variety of objects by the Soviet and East German intelligence services. The example shown here is concealed inside a gentleman's clothes brush. Services that issued such items had to ensure that they fitted in with the lifestyle adopted by their agent; otherwise, the concealment might arouse suspicion.



CLOTHES BRUSH CONCEALMENT



Slot for locking pin

Hole for inserting pin to open concealment

Minox IIIS camera

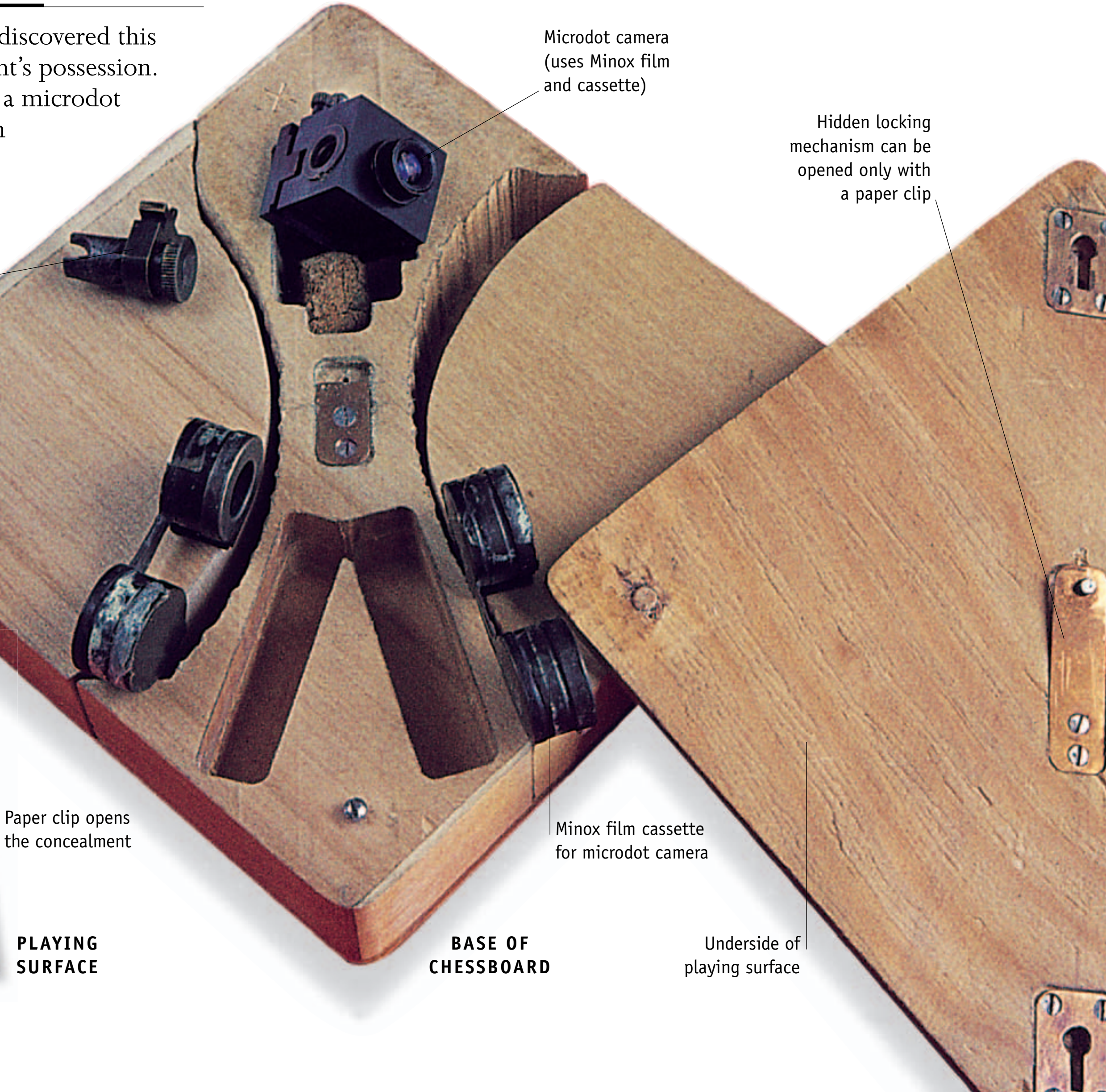
Locking pin keeps concealment shut

SECRET COMPARTMENT WITH CAMERA

Hollow to accommodate camera

Chessboard concealment

West German counterintelligence discovered this chessboard in an East German agent's possession. It has an internal cavity to conceal a microdot camera, accessories, and film. Such concealments were almost always "one-of-a-kind" items, designed in special workshops for specific missions.



Microdot camera (uses Minox film and cassette)

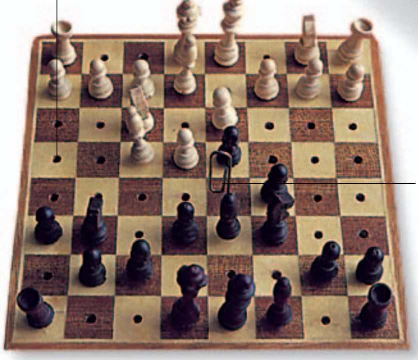
Hidden locking mechanism can be opened only with a paper clip

Manual winder to advance film in cassette

Minox film cassette for microdot camera

BASE OF CHESSBOARD

Underside of playing surface



Socket for chess pieces (not part of the concealment)

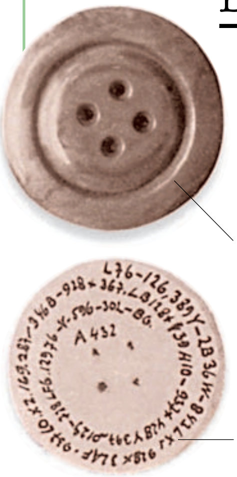
Paper clip opens the concealment

PLAYING SURFACE

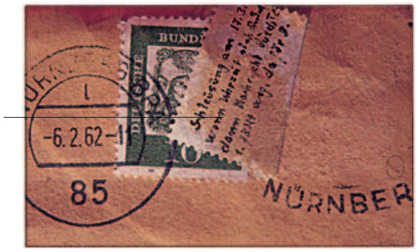
Concealments II

Button and stamp concealments

Even careful counterintelligence searches rarely reveal messages such as this inscription under a button, made during World War I, or the tiny message under a postage stamp, used in 1962.



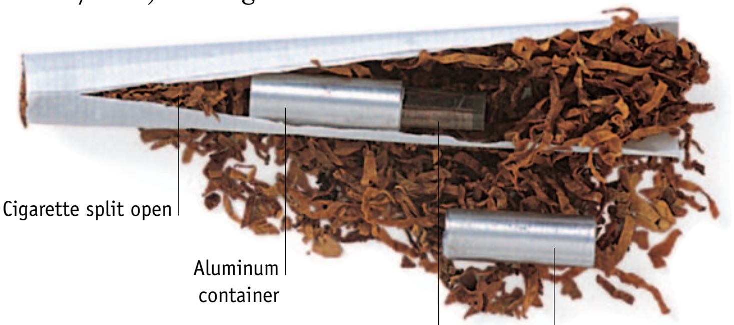
BUTTON (RUSSIAN INTELLIGENCE)



POSTAGE STAMP (HVA)

Cigarette concealment

The Polish intelligence service made this metal cylinder so that spies and couriers could conceal tightly rolled "soft film" (film from which the celluloid has been removed to make the film extremely thin) in a cigarette.

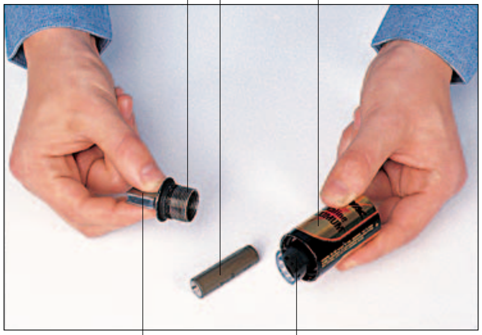


KGB battery casing concealment

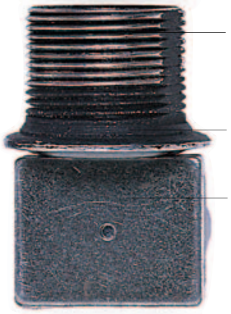
This style of concealment was used by intelligence agencies in the countries of the former Soviet bloc. Inside the casing of a standard flashlight battery was a cavity in which film, money, and even microdot cameras and viewers could be hidden. Also in the casing was a much smaller real battery that gave the correct voltage so that the fake battery could actually be used. To open the fake battery casing, the base plate had to be unscrewed using a magnet.

INNER BATTERY

HOLLOW BATTERY CASING



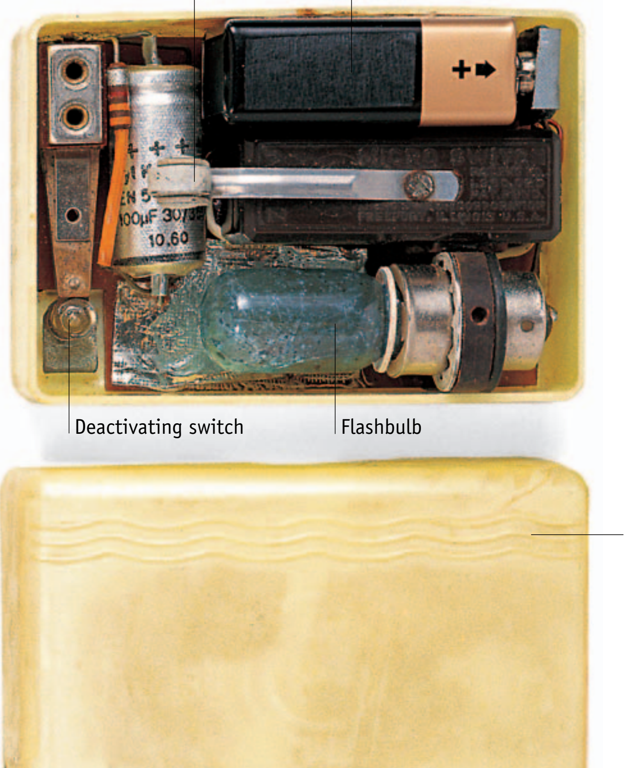
OPENED CONCEALMENT



MAGNET AND BASE PLATE

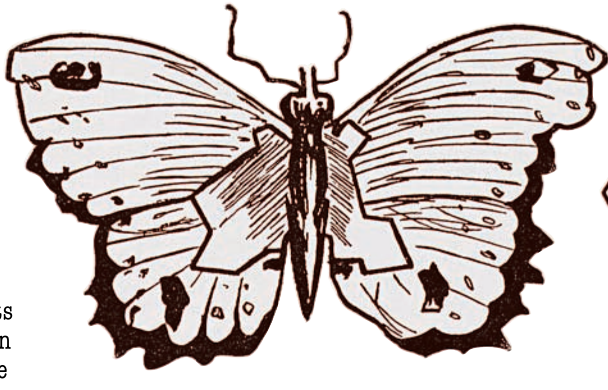
Soap case concealment

Czech intelligence (StB) invented devices for couriers carrying film, such as this soap case. The devices destroy the evidence if opened incorrectly: here the film is wrapped around a flashbulb, which flashes and destroys the film if the case is not opened in the correct manner. To open the case safely, a magnet is placed beneath the case. The magnet pulls open a switch that deactivates the flash.

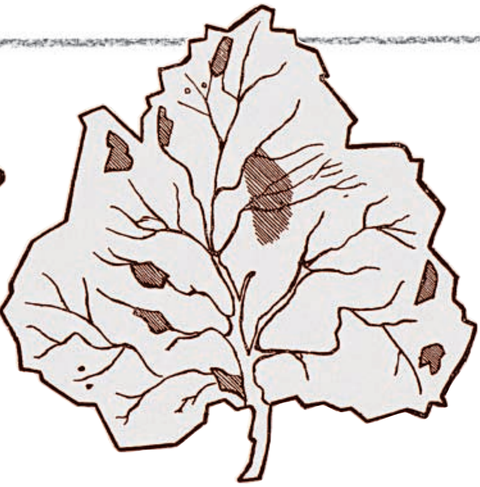


THE ARTWORK OF BADEN-POWELL

Lord Baden-Powell (1857–1941) is best known as the founder of the Boy Scouts, but he was involved in intelligence-gathering during his early military career. One mission was to obtain details of enemy fortresses in the Balkans in 1890. Baden-Powell disguised himself as an entomologist and sketched butterflies in the area. The veins on the butterfly's wings contained a plan of the fortifications, while the spots on the veins denoted the size and position of guns. The drawing of the leaf was made to show trench lines.



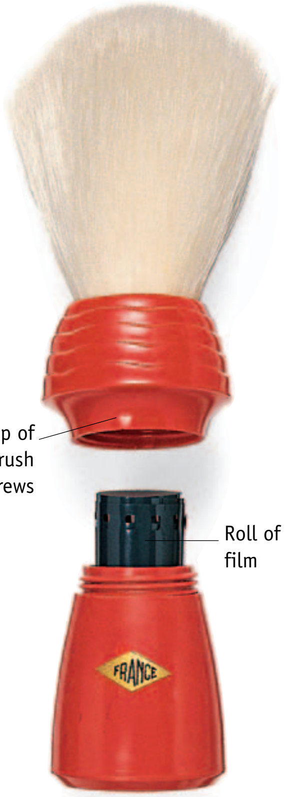
BUTTERFLY SKETCH



LEAF SKETCH

CIA shaving concealments

Everyday objects, such as these toiletry items, can be carried without attracting any suspicion. The handle of this French shaving brush has a cavity that opens only when the base is turned clockwise. The can holds and dispenses a small amount of shaving cream; the rest of the space in the can may be used for concealment.

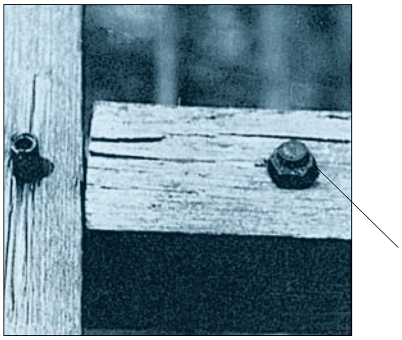


SHAVING BRUSH

SHAVING CREAM CAN

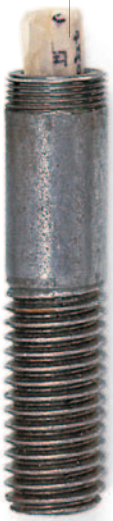
Hollow bolt

This hollow bolt was made by the KGB and used as a dead drop (see p. 170) by Soviet agents operating in West Germany. The head of the bolt could be removed to reveal a cavity in which items could be concealed. Once the bolt was filled it could be screwed into the dead drop site, in this case a wooden railing on a bridge, ready for the arrival of an agent or handler.



BOLT ON BRIDGE

HEAD OF BOLT



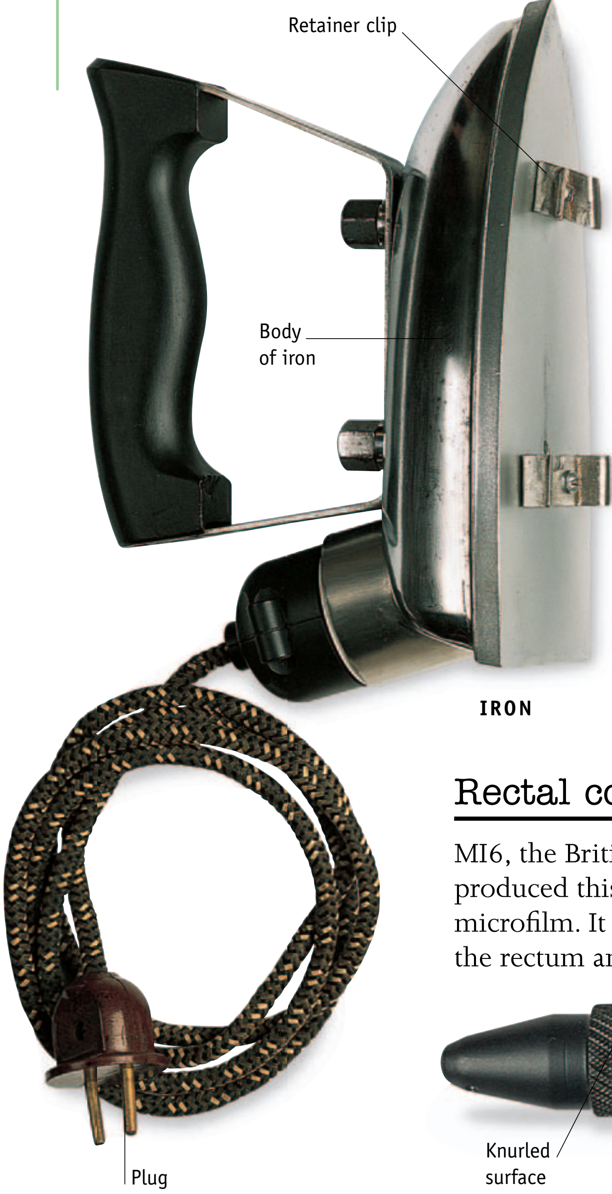
HOLLOW BOLT

DEAD DROP SITE ON BRIDGE

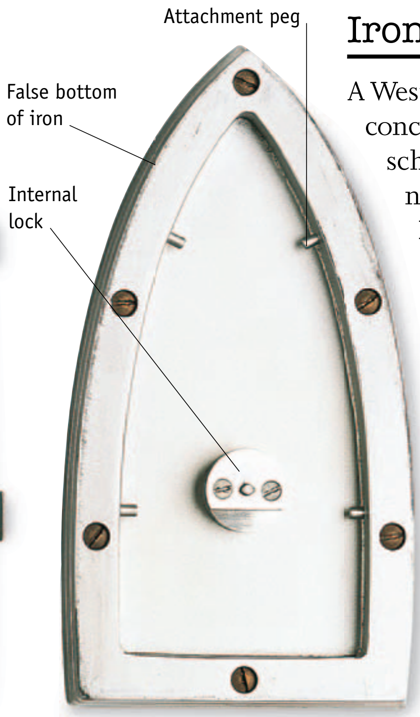
Concealments III

Iron concealment

A West German housewife used this modified iron to conceal one-time pads (see p. 159) and communication schedules. With her tradecraft items safely hidden, nothing else in the apartment linked her to the HVA, the East German foreign intelligence service. Even when her apartment was searched by the West German Criminal Police (BKA), the concealment was not found. The iron could not be operated when the concealment was filled.



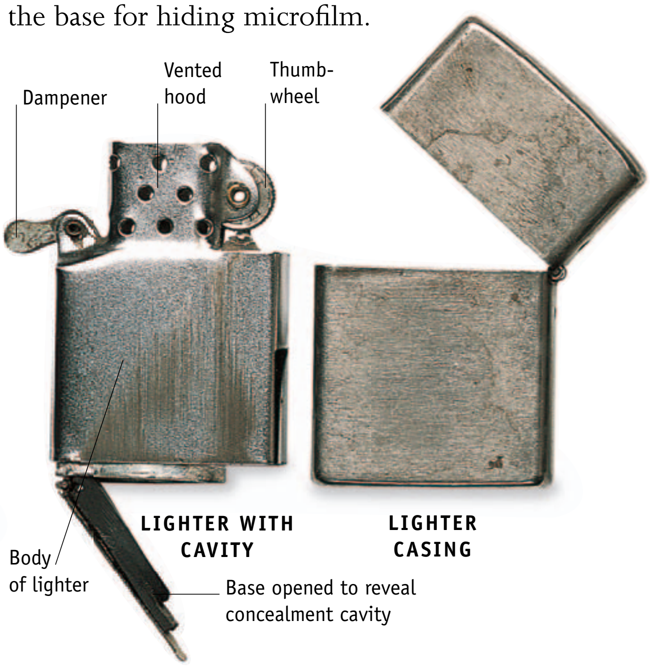
IRON



FRAME OF CONCEALMENT

Lighter concealment

Popular Zippo-style cigarette lighters could be transformed into effective concealments. This KGB modified lighter functioned normally but also contained a hidden cavity built into the base for hiding microfilm.

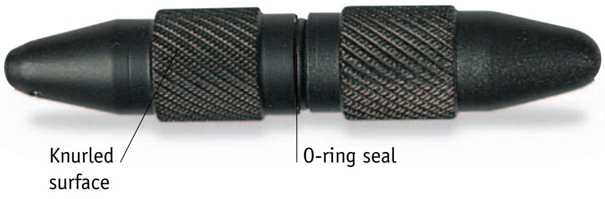


LIGHTER WITH CAVITY

LIGHTER CASING

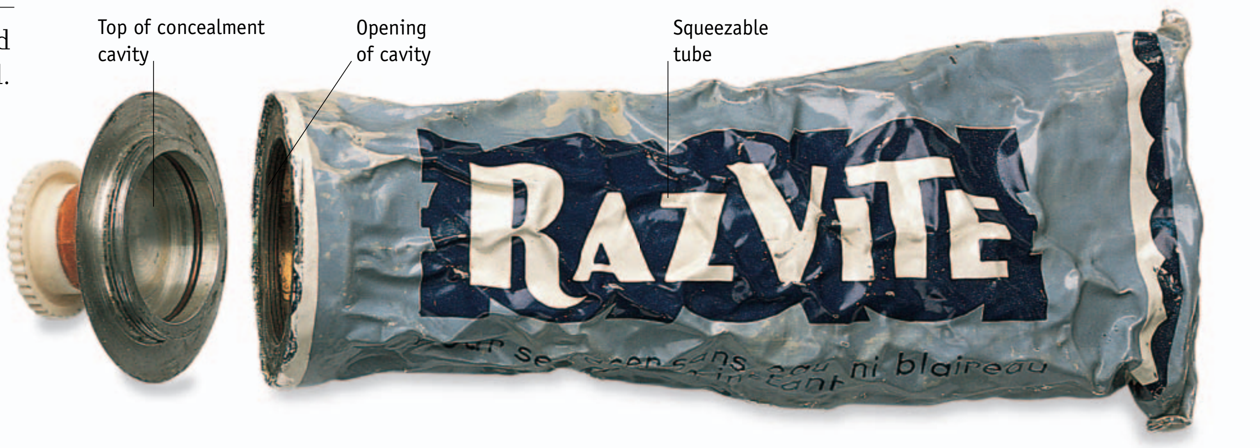
Rectal concealment

MI6, the British foreign intelligence service, produced this small concealment to store microfilm. It was designed to be hidden in the rectum and came with its own condom.



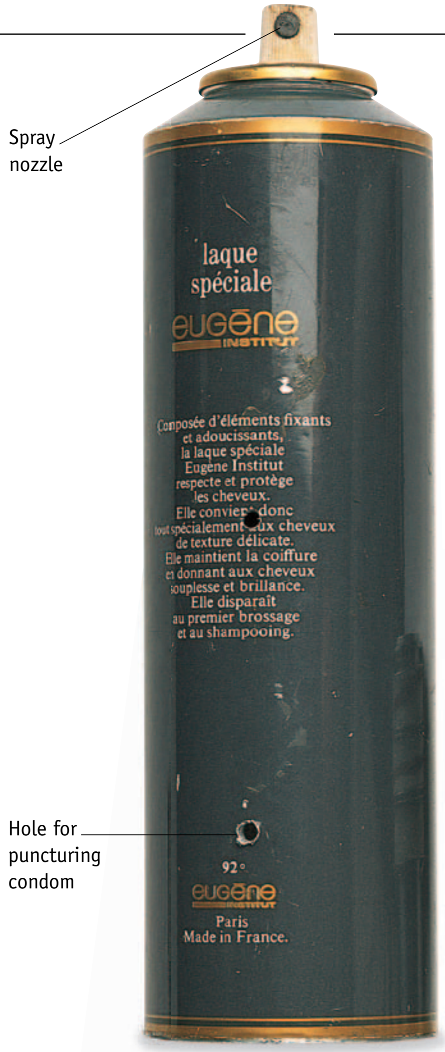
Tube concealment

This tube appears unmodified and is pliable when squeezed. Inside is an inner shell that creates a waterproof concealment cavity, accessed by unscrewing the upper portion of the tube. The cavity is large enough to conceal a rolled-up false passport for a KGB agent to make an escape.

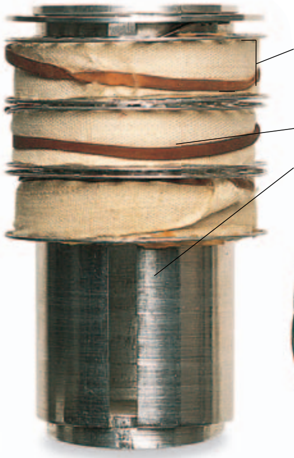


Aerosol concealment

This can was used by KGB couriers to transport undeveloped Minox film. Each roll of exposed film was spooled onto an outer ring, with each layer of film separated by a layer of cotton ribbon. The rings fit over an inner core containing an ammonia-filled condom. If danger was detected, the condom was punctured and the ammonia, absorbed by the cotton, destroyed the film.


Spray nozzle
laque spéciale
eugène INSTITUT
Composée d'éléments fixants et adoucissants, la laque spéciale Eugène Institut respecte et protège les cheveux. Elle convient donc tout spécialement aux cheveux de texture délicate. Elle maintient la coiffure et donnant aux cheveux souplesse et brillance. Elle disparaît au premier brossage et au shampooing.
Hole for puncturing condom
92°
eugène INSTITUT
Paris
Made in France.

AEROSOL CAN


Film and ribbon spooled onto ring
Rubber band securing film and ribbon
Inner core of can

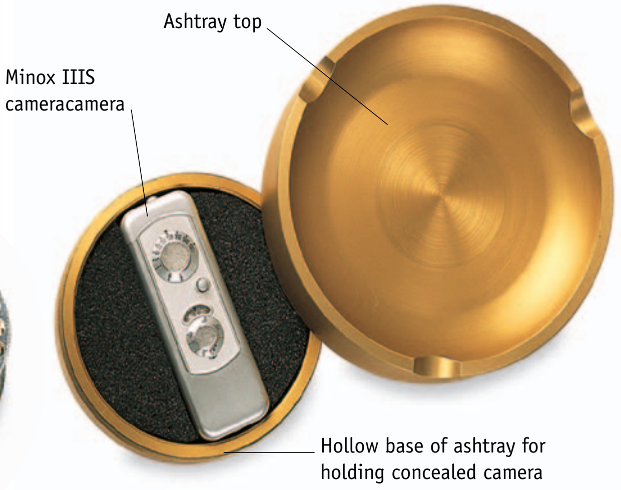
INNER CORE WITH RINGS

RING HOLDING MINOX FILM

BASE OF CAN

Ashtray concealment for Minox camera

The HVA designed this ashtray to conceal a Minox IIIS camera. The top unscrewed for quick access to the camera but had to be turned the "wrong" way because of its reverse thread mechanism. The ashtray was always left filled with cigarette ash, making it unlikely to be searched.



Hollow construction nail

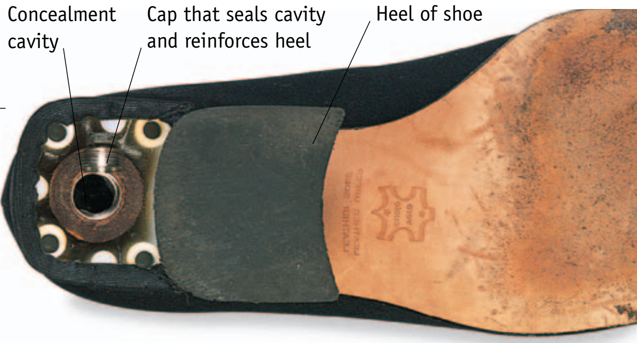
The KGB modified this construction nail to create a small cavity for hiding soft film (photographic emulsion that has been separated from its celluloid backing). The fragile, thin film could be easily rolled and hidden in the nail.

HOLLOW NAIL WITH HEAD SCREWED IN

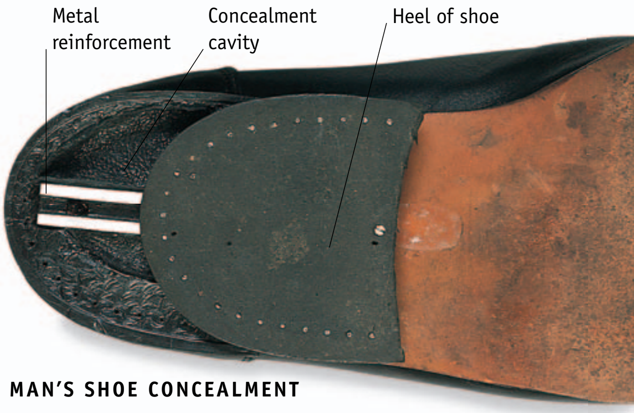
HEAD UNSCREWED

Stasi heel concealments

Shoe heels were used to create concealment cavities for transporting exposed, but undeveloped, film. The woman's shoe (top) has a cylindrical cavity in the heel large enough for rolled-up one-time pads and microfilm. In the man's heel (bottom), a metal reinforcement prevents indentations in the heel that might reveal the cavity, which was used to hide Minox film. After the introduction of metal detectors in airports, heel concealments could no longer be reinforced with metal.



WOMAN'S SHOE CONCEALMENT



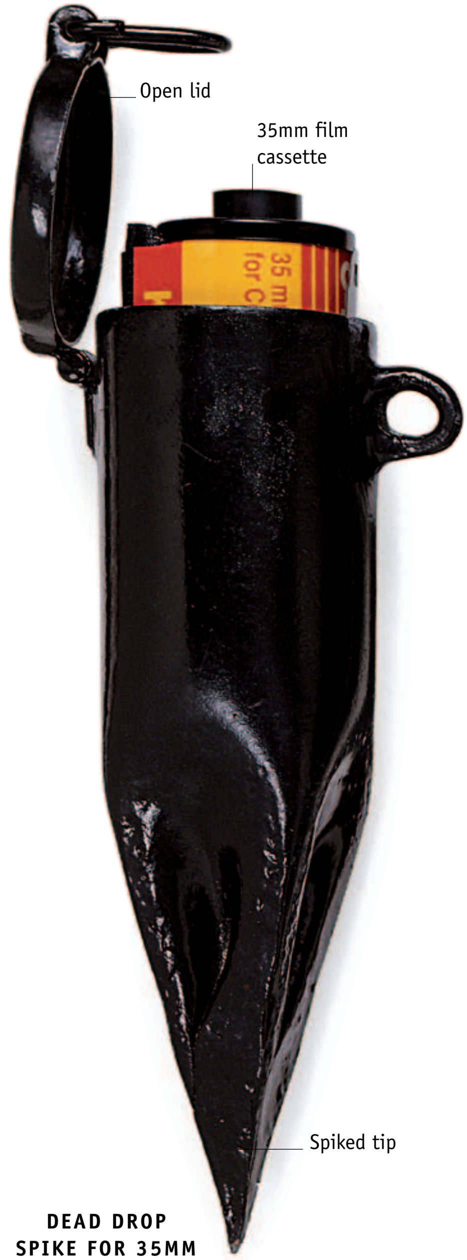
MAN'S SHOE CONCEALMENT

Dead drops I

A DEAD DROP IS A PREARRANGED location at which spies can leave information or from which they can collect instructions, cipher pads, microdot cameras, film, radio schedules, money, or any form of spying equipment. Items are usually placed in specially designed dead drop containers. Spies use dead drops because they are safer than personal meetings, which can jeopardize the safety of at least two links in a spy network. The sites used for dead drops must be inconspicuous, but easy for the agents to find. The procedure for making a dead drop involves a series of signals which the controller and the agent use to ensure that an enemy is not involved or watching.

CIA spikes

Shown full-size, these spikes are stuck in the ground; they are used to hold money, cipher pads, microdot cameras, and other items ready for collection at dead drop locations. One is designed to hold a 35mm film cassette.



DEAD DROP SPIKE FOR 35MM FILM CASSETTES

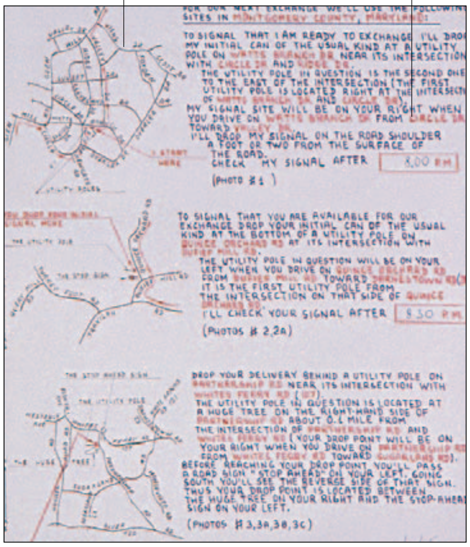
JOHN WALKER'S FINAL DEAD DROP

On the evening of May 17, 1985, John Walker, an American spy for the KGB (see p. 54), drove to a dead drop site on a country road in Maryland, some 25 miles (40 km) northwest of Washington, DC. Unknown to him, he was under surveillance by the FBI.

To signal to his KGB handler that he was in the area for the drop, Walker placed an empty soda can at the foot of a roadside utility pole. His secret documents were hidden inside a bag of garbage, and he placed this behind another utility pole.

The FBI, following Walker, saw him place the soda can and thought it might contain something of importance, so they removed it. The KGB officer, unable to find the can, terminated the procedure and returned safely to the Soviet embassy in Washington, where he was based.

The FBI retrieved the garbage bag, complete with the secret documents, and Walker was arrested later that night.


Annotated map
Instructions with place names in red
START HERE

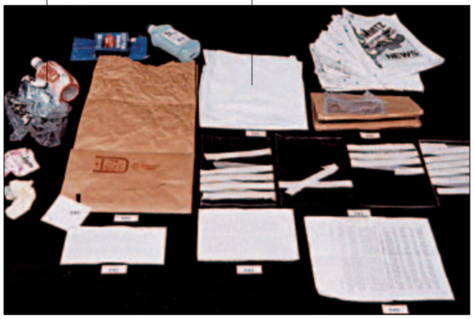
FOR OUR NEXT EXCHANGE WE'LL USE THE FOLLOWING SITES IN MONTGOMERY COUNTY, MARYLAND:

TO SIGNAL THAT I AM READY TO EXCHANGE I'LL DROP MY INITIAL CAN OF THE USUAL KIND AT A UTILITY POLE ON WATTS BRANCH DR NEAR ITS INTERSECTION WITH CIRCLE DR AND VALLEY DR.
THE UTILITY POLE IN QUESTION IS THE SECOND ONE TO THE EAST OF THE INTERSECTION (THE FIRST UTILITY POLE IS LOCATED RIGHT AT THE INTERSECTION OF WATTS BRANCH DR AND CIRCLE DR).
MY SIGNAL SITE WILL BE ON YOUR RIGHT WHEN YOU DRIVE ON WATTS BRANCH DR FROM CIRCLE DR TOWARD VALLEY DR.
I'LL DROP MY SIGNAL ON THE ROAD SHOULDER A FOOT OR TWO FROM THE SURFACE OF THE ROAD.
CHECK MY SIGNAL AFTER 8.00 PM
(PHOTO #1)

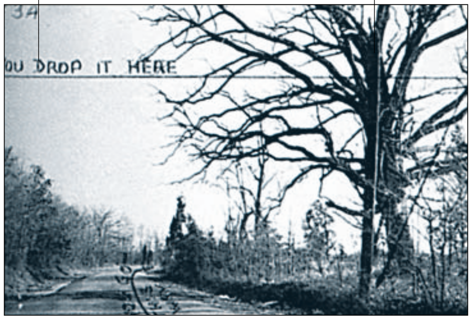
TO SIGNAL THAT YOU ARE AVAILABLE FOR OUR EXCHANGE DROP YOUR INITIAL CAN OF THE USUAL KIND AT THE BOTTOM OF A UTILITY POLE ON QUINCE ORCHARD RD AT ITS INTERSECTION WITH DUFIEF MILL RD.
THE UTILITY POLE IN QUESTION WILL BE ON YOUR LEFT WHEN YOU DRIVE ON QUINCE ORCHARD RD FROM DUFIEF MILL RD TOWARD DARNESTOWN RD(
IT IS THE FIRST UTILITY POLE FROM THE INTERSECTION ON THAT SIDE OF QUINCE ORCHARD RD.
I'LL CHECK YOUR SIGNAL AFTER 8.30 PM
(PHOTOS # 2,2A)

DROP YOUR DELIVERY BEHIND A UTILITY POLE ON PARTNERSHIP RD NEAR ITS INTERSECTION WITH WHITES FERRY RD (107).
THE UTILITY POLE IN QUESTION IS LOCATED AT A HUGE TREE ON THE RIGHT-HAND SIDE OF PARTNERSHIP RD ABOUT 0.1 MILE FROM THE INTERSECTION OF PARTNERSHIP RD AND WHITES FERRY RD (YOUR DROP POINT WILL BE ON YOUR RIGHT WHEN YOU DRIVE ON PARTNERSHIP RD FROM WHITES FERRY RD TOWARD SUGARLAND RD).
BEFORE REACHING YOUR DROP POINT YOU'LL PASS A ROAD SIGN "STOP AHEAD" ON YOUR LEFT. GOING SOUTH YOU'LL SEE THE REVERSE SIDE OF THAT SIGN. THUS YOUR DROP POINT IS LOCATED BETWEEN THE HUGE TREE ON YOUR RIGHT AND THE STOP-AHEAD SIGN ON YOUR LEFT.
(PHOTOS #3,3A,3B,3C)

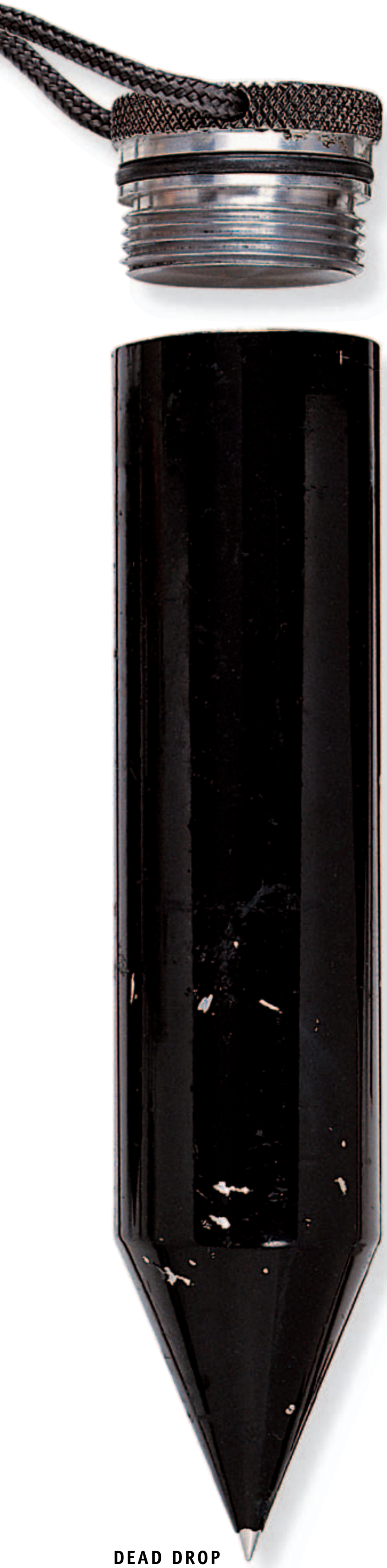
KGB'S INSTRUCTIONS TO GUIDE WALKER TO HIS DEAD DROP SITE



CONTENTS OF WALKER'S DEAD DROP



KGB PHOTOGRAPH OF THE DEAD DROP



DEAD DROP SPIKE

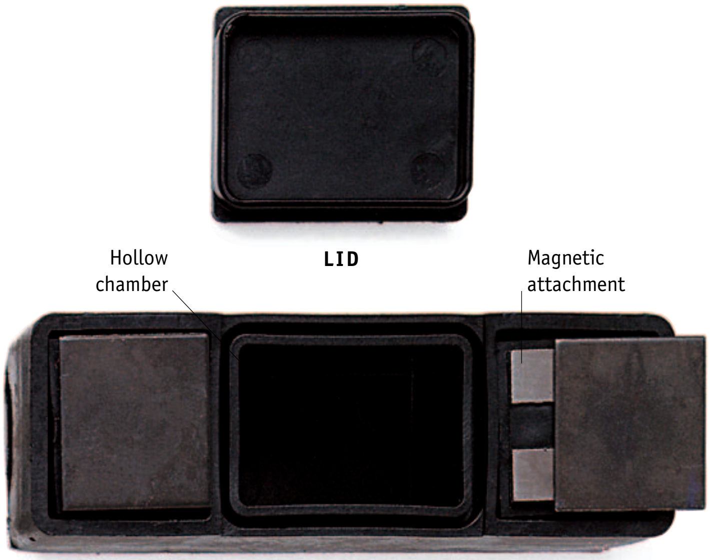
DEAD DROP EMIL

During the 1950s, Bruno Sniegowski spied for Poland in West Germany. The officers in charge of Sniegowski communicated with him using dead drops, one of which was codenamed Emil. A chalk mark at a prearranged place would inform Sniegowski that a message awaited him at Emil. The container used for dead drop Emil was a metal tube, which was hidden at the base of a wall, behind a brick.

SNIEGOWSKI AT DEAD DROP EMIL

CIA clam dead drop

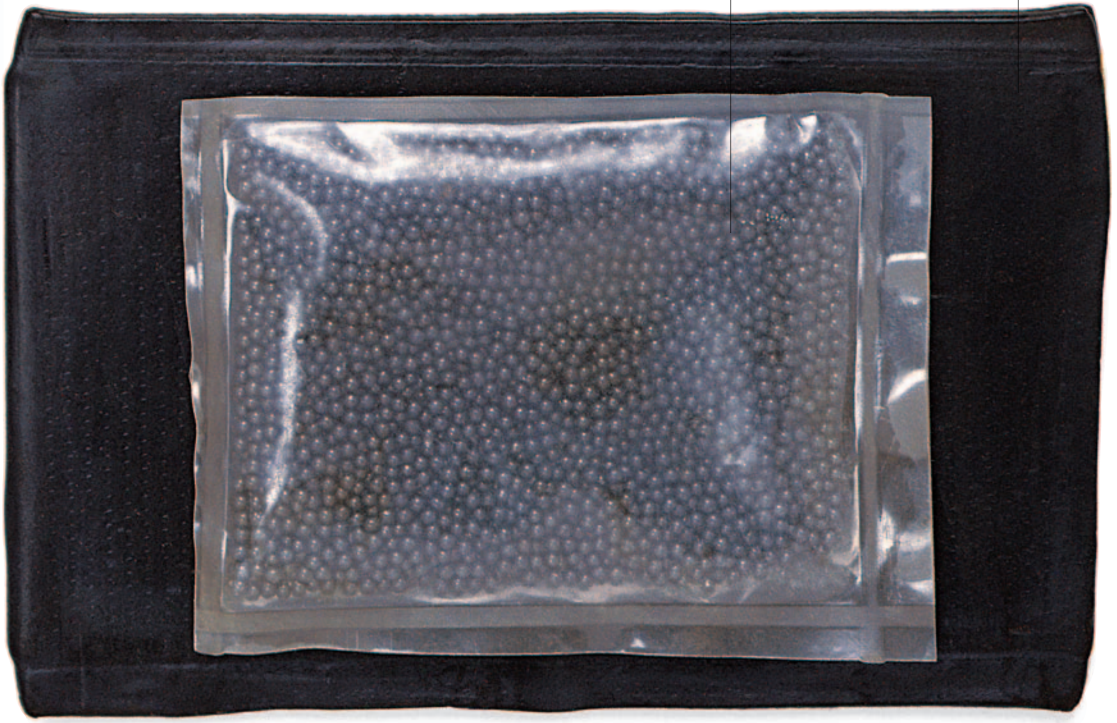
A magnet holds this dead drop container to a metal object at the location of the drop. A dead drop location need not be in the ground—the clam container can be used in many places; for example, under an abandoned car or metal park bench.



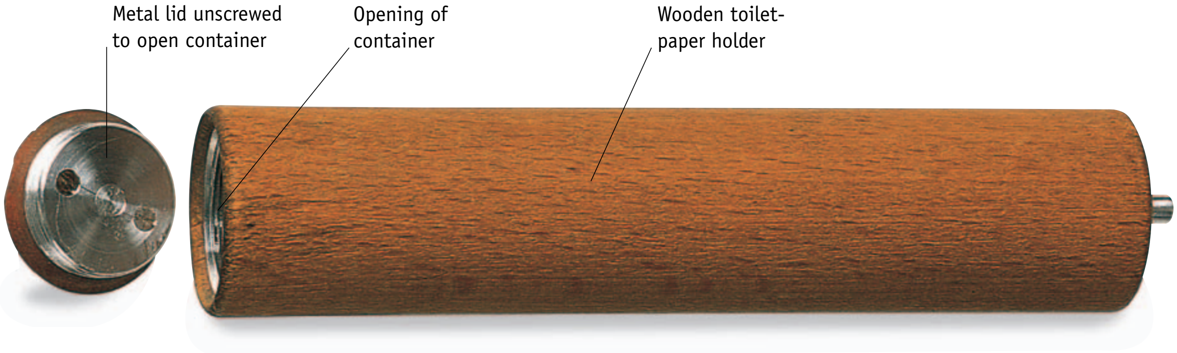
CLAM DEAD DROP CONTAINER

CIA waterproof pouch

The weights in this waterproof pouch allow it to be be used to conceal material in a roadside ditch, or beneath marked rocks in a shallow stream.



Dead drops II


Metal lid unscrewed to open container
Opening of container
Wooden toilet-paper holder

Toilet-roll holder dead drop

The HVA (see p. 56) used this hollow toilet-paper holder on trains that passed through East Germany from Western countries. The drop would be filled by an agent in the West and safely cleared by the HVA after the train crossed the border into East Germany.

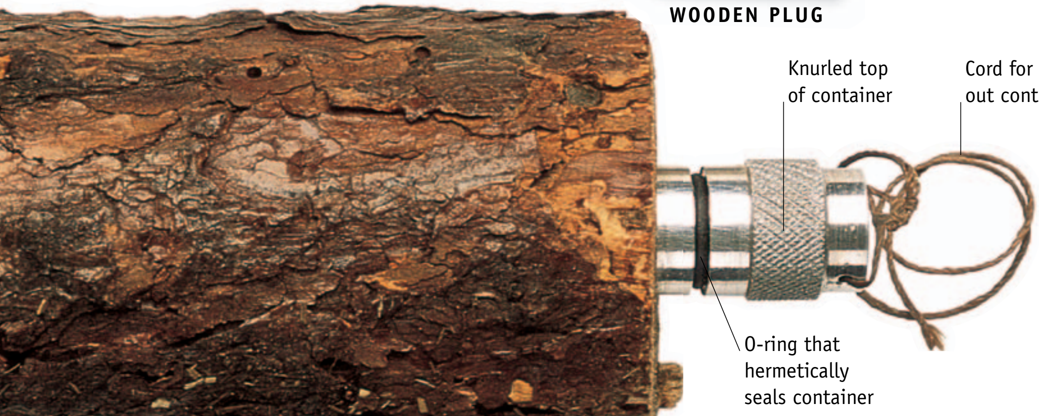
Log dead drop

This wooden log was used in Australia during the 1950s for secret communications between a KGB officer and the Australian Security and Intelligence Organization (ASIO). The log appears to be an ordinary piece of cut firewood with a protruding bent nail. When the nail is removed, a spring-loaded wooden plug pops out to reveal a cylindrical, hermetically sealed metal container.

LOG WITH HIDDEN CONTAINER

NAIL FOR SECURING HIDDEN CONTAINER

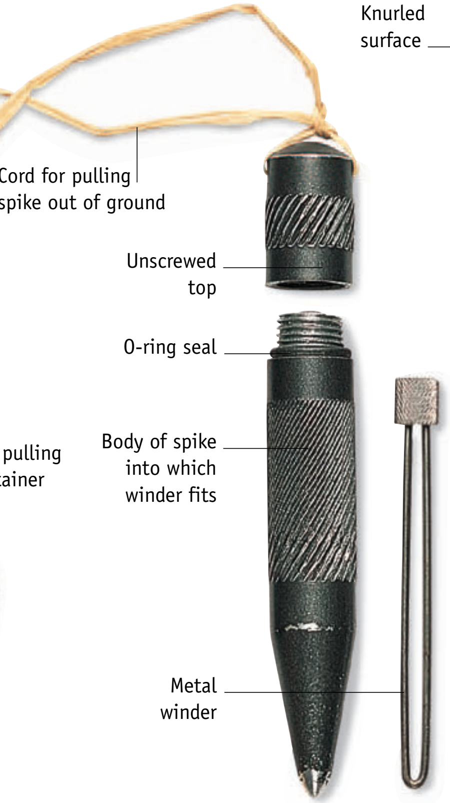
WOODEN PLUG


Knurled top of container
Cord for pulling out container
O-ring that hermetically seals container

CONTAINER REVEALED AFTER NAIL REMOVED

MI6 dead drops

Britain's MI6 (see p. 217) used metal spikes as containers for passing film and messages. The spikes were often buried in grassy areas near the base of a lamppost or bench. Messages written on paper were rolled around a metal winder inserted into the hollow spike.

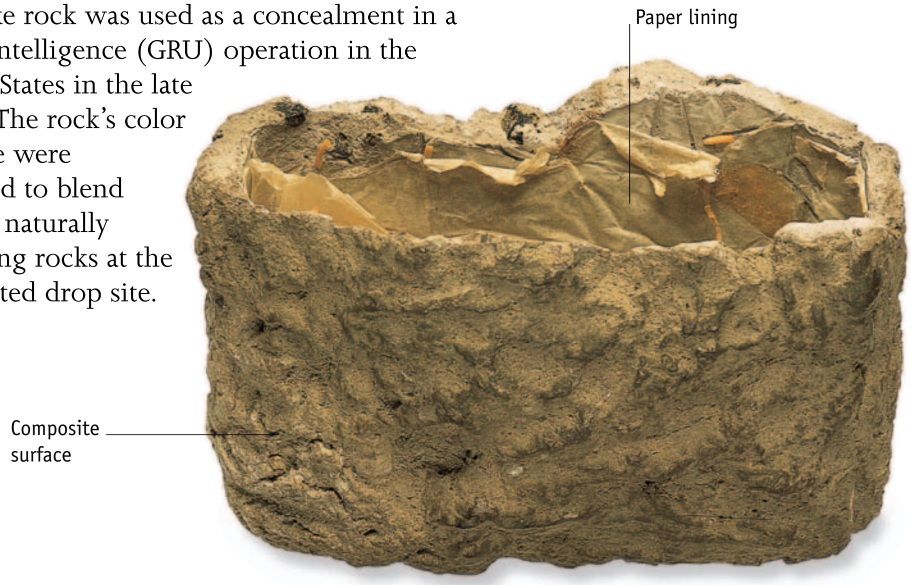

Cord for pulling spike out of ground
Unscrewed top
O-ring seal
Body of spike into which winder fits
Metal winder

SPIKE AND WINDER

SPIKE

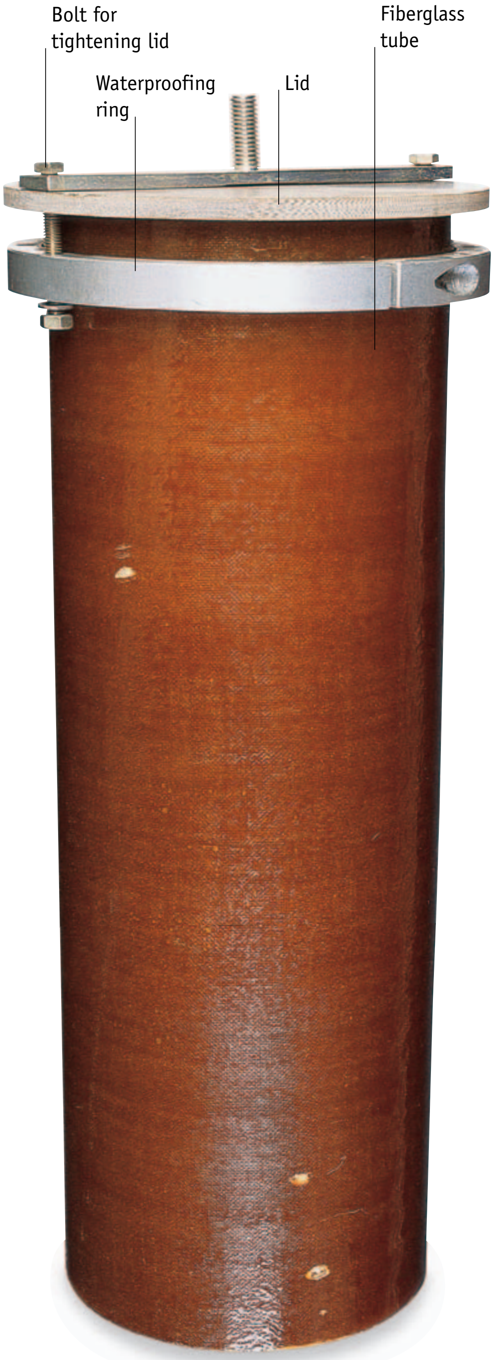
Rock concealment

This fake rock was used as a concealment in a Soviet intelligence (GRU) operation in the United States in the late 1970s. The rock's color and size were designed to blend in with naturally occurring rocks at the designated drop site.



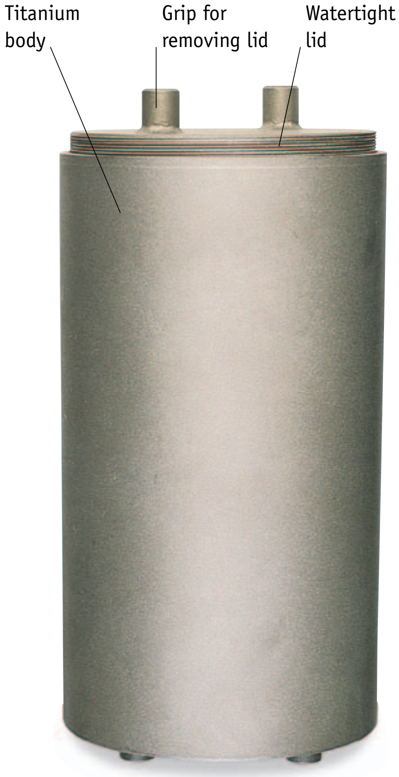
Underwater document holder

When the East German government began to collapse in 1989, its foreign intelligence service, the HVA, worked to safeguard the identities of its agents still operating around the world. The HVA did this by caching sensitive computer printouts listing the real names of the agents (known elsewhere only by their codenames) in underwater holders.



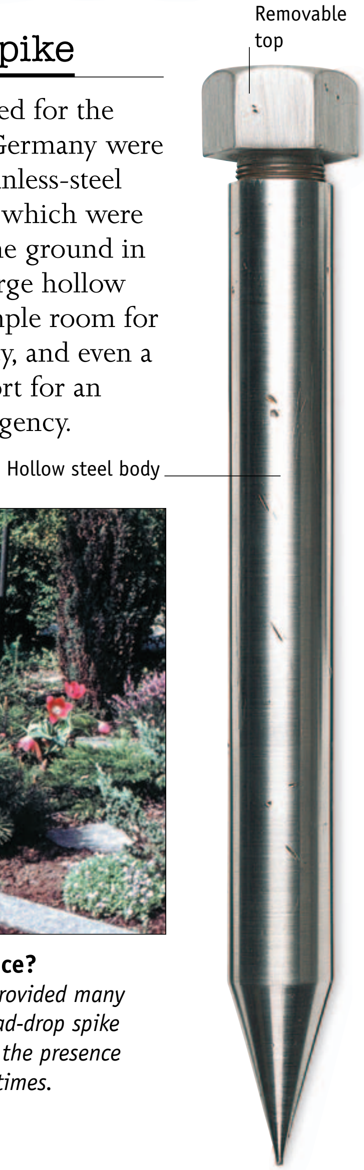
Metal cache

This titanium cylinder was used for long-term underground storage at a remote location. During the Cold War, the KGB secretly buried caches of spy equipment inside many Western European countries.



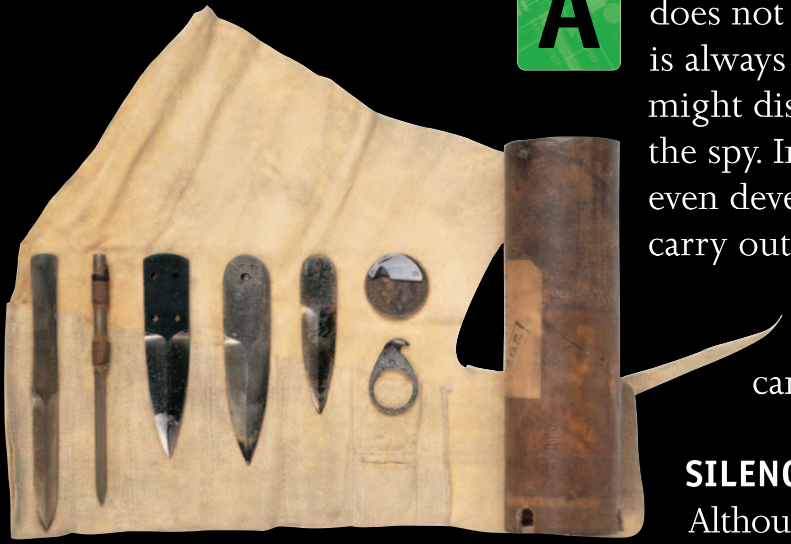
Cemetery spike

Agents who worked for the HVA inside West Germany were provided with stainless-steel dead-drop spikes, which were often hidden in the ground in cemeteries. The large hollow spike provided ample room for documents, money, and even a rolled false passport for an escape in an emergency.



A perfect hiding place?
The cemetery setting provided many places to conceal a dead-drop spike and could also explain the presence of visitors at irregular times.

WEAPONS



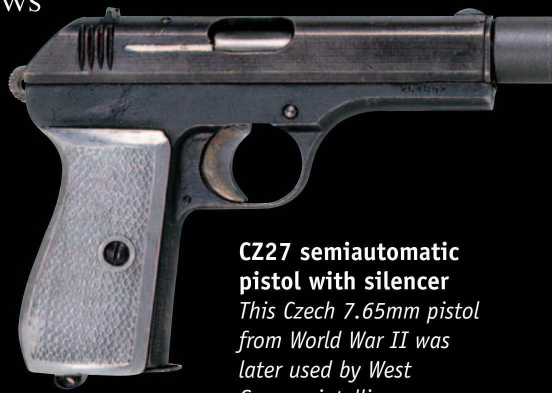
Concealed blades
During World War II, the British SOE developed a number of concealable edged weapons, as displayed in this knife roll.

A SPY WHOSE FUNCTION is purely to gather intelligence does not normally carry or own a weapon, since there is always a risk that an enemy counterintelligence force might discover the weapon, which would incriminate the spy. Intelligence agencies do, however, stock and even develop weapons for the use of personnel who carry out specialized roles: bodyguards, assassins, and other covert action personnel. In wartime, special forces operating behind enemy lines carry both conventional and specialized weapons.

SILENCED WEAPONS

Although the frequency of their use in espionage has been exaggerated by writers of spy fiction, silenced weapons do have a role in the work of intelligence agencies. Many were developed for special operations use during World War II. Because firearms can never be made completely silent or flashless, experiments were made with rossbows and with pistols adapted to fire arts.

Some of the silenced firearms employed in World War II, such as the Welrod (see p. 205) used by the SOE and the Hi-Standard pistol (see p. 181) of the OSS, remain part of the arsenals of major intelligence agencies.

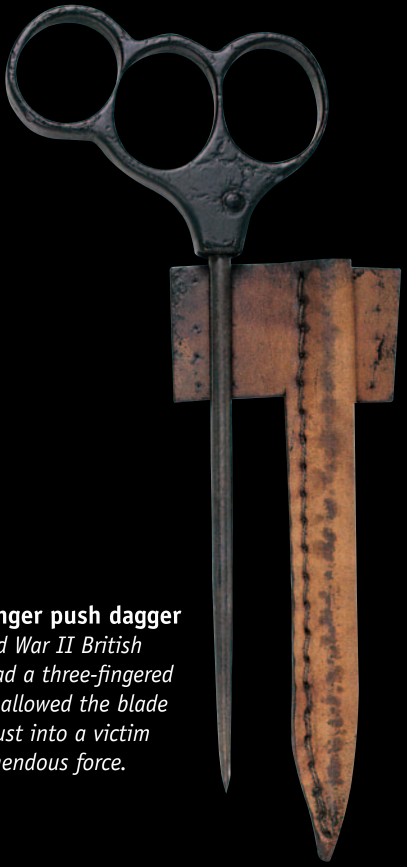


CZ27 semiautomatic pistol with silencer
This Czech 7.65mm pistol from World War II was later used by West German intelligence.

In some cases, silenced weapons are issued for survival use—for example, for hunting if stranded in a remote area. In other cases, they may be issued as a defense against guard dogs, rather than for attacking human opponents.

CLOSE-COMBAT WEAPONS

Specialized weapons made for fighting at close quarters are often carried in covert operations. A considerable degree of training is needed to use some types of close-combat weapons. The type of personnel who carry them are those ordered to attack individual targets by surprise, or those taking part in high-risk operations



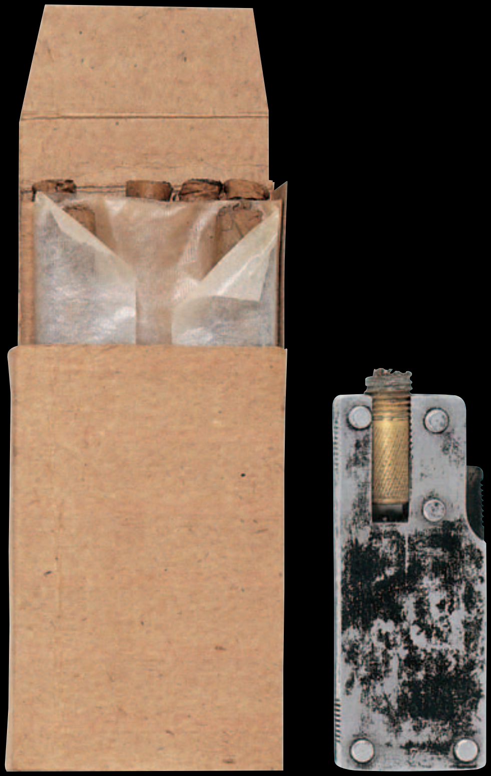
Three-finger push dagger
This World War II British dagger had a three-fingered grip that allowed the blade to be thrust into a victim with tremendous force.

who may need a last-resort weapon for self defense. They range from traditional "brass knuckles" to specially designed weapons such as the World War II Peskett Device, which is a combined dagger, garrotte, and cosh.

The spring cosh is often the weapon of choice for subduing opponents. It may be used with lethal force, or merely to give a knockout blow. Other coshes are used as a means of forcing an enemy to surrender or to disclose information.

Genrikh Yagoda
Yagoda (1891–1938) was head of the Soviet NKVD and set up a poison weapons workshop.

Knives are the classic close-combat weapons, and many different types have been developed for use in various situations. Small blades can be hidden under a jacket lapel for emergency use. However, the Fairbairn-Sykes fighting knife of World War II was designed for offensive use. It is so perfectly suited to its purpose that it continued in production and service into the 1990s.

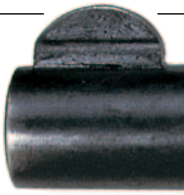

KGB assassination device
Hidden in a fake cigarette pack, this device fires acid that vaporizes into deadly cyanide gas in the victim's face, causing death within seconds.

CONCEALED WEAPONS

World War II saw the development of a number of concealed weapons. The main purpose of such weapons was to give an agent who had been detected some chance of escape. They included firing devices that could be worn on belts or carried up an agent's sleeve. Others were disguised as cigars, pipes, or pens. After the war, intelligence agencies continued to develop such weapons—a notable example being the 4.5mm caliber firing device issued by the KGB, which could be hidden in a variety of concealments, including a lipstick holder.

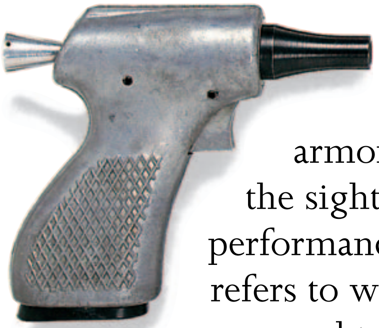
The KGB developed assassination weapons that could kill silently and in ways not detectable at autopsy; for example, by emitting poison gas or injecting poison pellets. These weapons have been disguised as canes or umbrellas, or concealed in newspapers.

Walther PPK pistol
Designed for German plainclothes police, the PPK is an easy weapon to hide. This makes it popular with intelligence agencies worldwide.



Special issue weapons

INTELLIGENCE AGENCIES prefer to equip their personnel with weapons that can be bought commercially, provided the performance is up to operational requirements. Such weapons are cheaper than specially developed ones and, if discovered, less incriminating as they cannot be traced to the agency. The only noticeable difference might be that the agency's armorers may have fine-tuned the sights and trigger to improve performance. The term "special issue" refers to weapons obtained in this way, and to such weapons as the dear gun, manufactured for the CIA for issue to Vietnamese agents in the Vietnam War (1959–75). This cheap, single-shot gun was intended to enable an agent to kill an enemy soldier in order to capture his or her weapon.



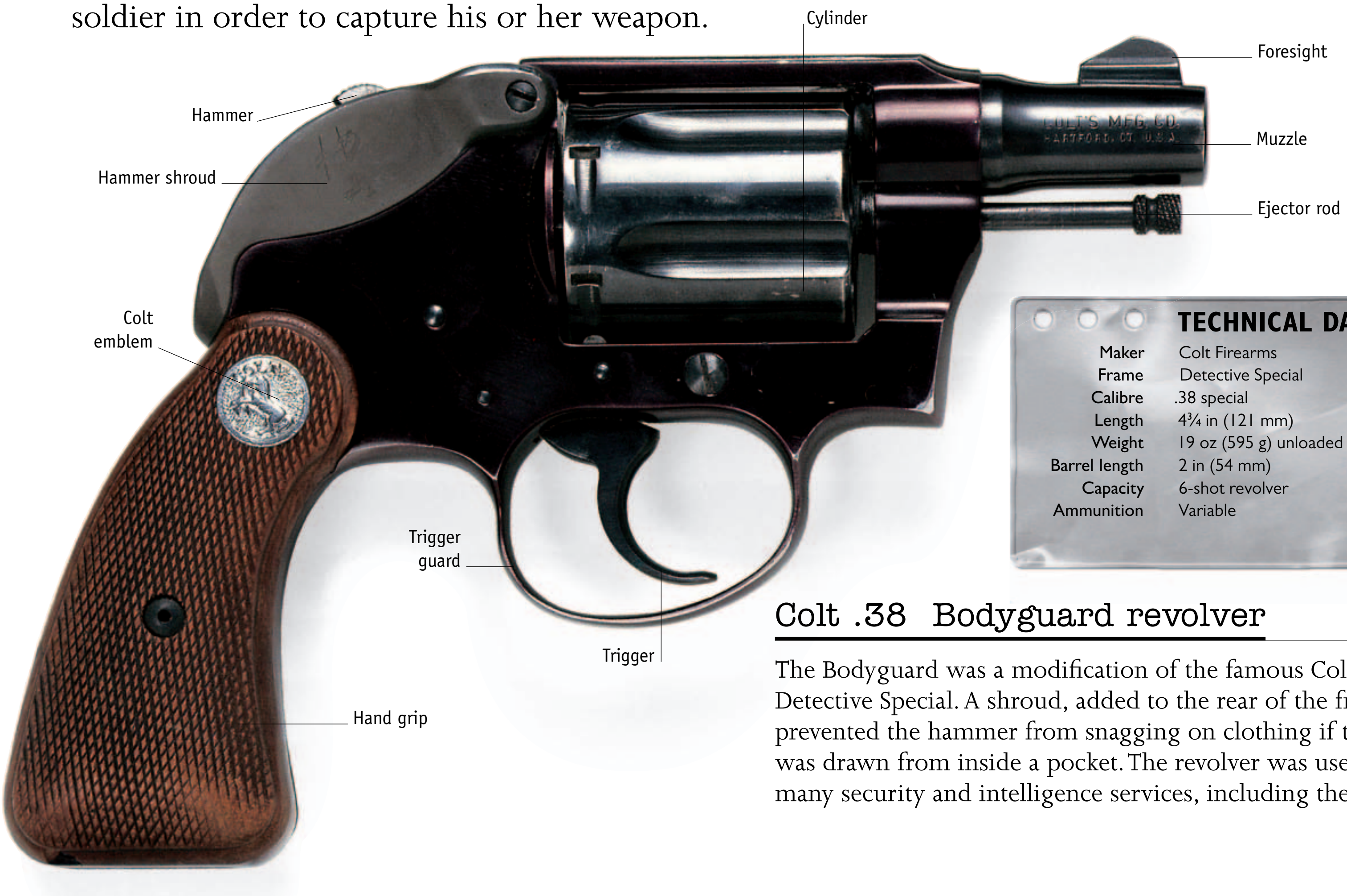
CIA DEAR GUN

ROYAL CANADIAN MOUNTED POLICE

Until 1981, counterintelligence and security in Canada were the responsibility of the security service of the Royal Canadian Mounted Police (RCMP). An RCMP "Red Squad" was set up in the 1920s to stop the spread of communism. Canadian intelligence realized the extent of infiltration by Soviet spies in 1945, when a Soviet defector informed the Canadians of wide-ranging espionage operations in their country. In 1984, the Canadian Security Intelligence Service (CSIS) was set up to take over in this field from the RCMP. The Colt Bodyguard shown below is an example of the wide variety of weapons available to CSIS officers.

CANADA
MAINTIENS LE DROIT
ROYAL CANADIAN MOUNTED POLICE

Crest of the RCMP
The members of the Royal Canadian Mounted Police are frequently known as Mounties.

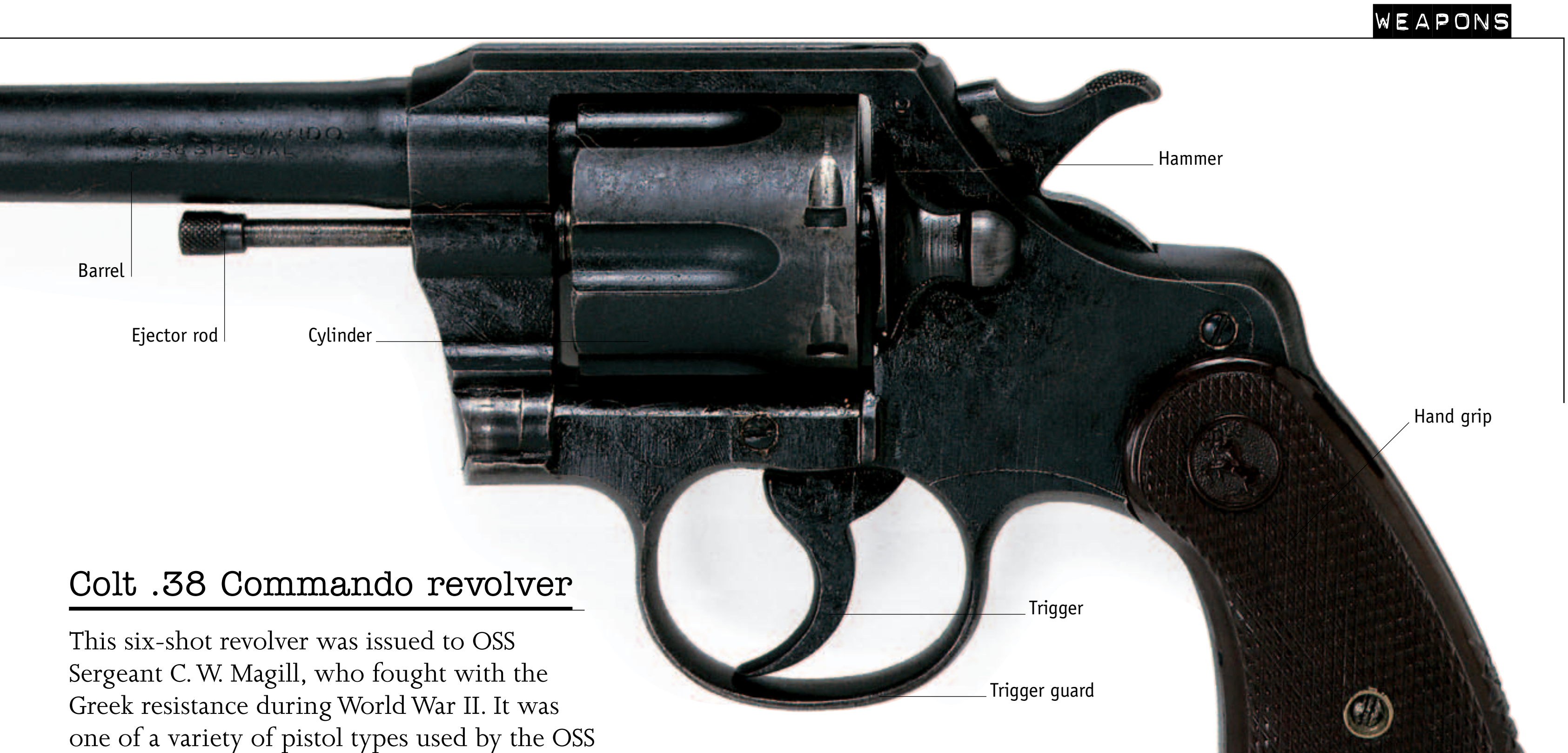


TECHNICAL DATA

Maker	Colt Firearms
Frame	Detective Special
Calibre	.38 special
Length	4¾ in (121 mm)
Weight	19 oz (595 g) unloaded
Barrel length	2 in (54 mm)
Capacity	6-shot revolver
Ammunition	Variable

Colt .38 Bodyguard revolver

The Bodyguard was a modification of the famous Colt Detective Special. A shroud, added to the rear of the frame, prevented the hammer from snagging on clothing if the pistol was drawn from inside a pocket. The revolver was used by many security and intelligence services, including the RCMP.



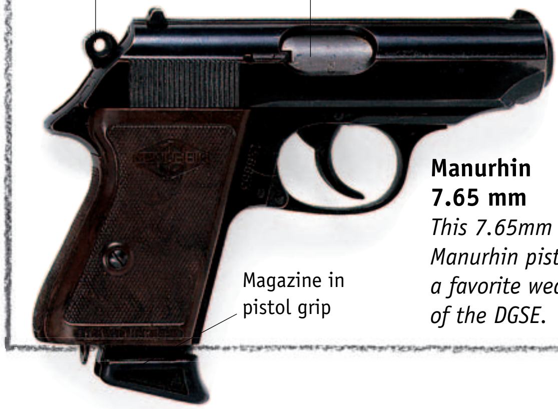
Colt .38 Commando revolver

This six-shot revolver was issued to OSS Sergeant C. W. Magill, who fought with the Greek resistance during World War II. It was one of a variety of pistol types used by the OSS (see p. 32) and was also supplied to American and Allied troops. The Commando was too large for covert operations that depended on concealment, but served well in resistance support operations.

Sergeant C. W. Magill
This World War II photograph shows Sergeant Magill at the age of 28, when he was serving with the OSS in Greece. His role was to work with Greek resistance units. The location here is the mountain village of Kastania.

THE FRENCH SECRET SERVICE

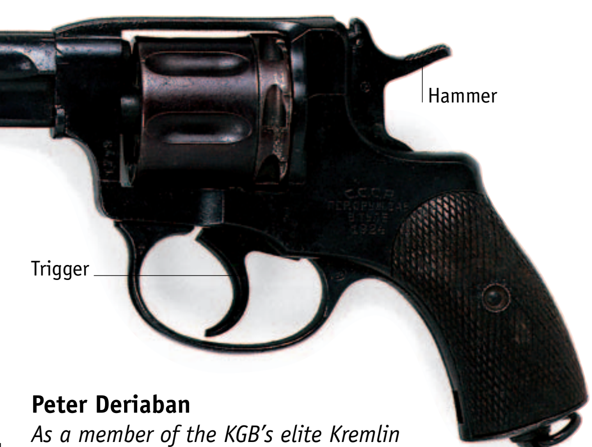
Formerly known as the SDECE, the French secret service was reconstituted in 1981 and called the DGSE. French operatives have been involved in many high-profile operations, including attempts to assassinate and abduct foreign political leaders. They made several attempts to assassinate President Gamal Abdel Nasser of Egypt during the 1950s, despite the fact that he was being supported by the CIA.



Manurhin 7.65 mm
This 7.65mm Manurhin pistol is a favorite weapon of the DGSE.

Nagant 7.62 mm secret police revolver

In the 1920s, a compact version of the standard Nagant service revolver was developed for the Soviet secret police. The 7.62mm Secret Police revolver was easily concealed. It was used until the 1940s, and armed the elite bodyguard unit that protected Stalin, the head of state, in Moscow.



Peter Deriaban
As a member of the KGB's elite Kremlin Guard Directorate, the defector Deriaban was issued with the Nagant.

Silenced weapons I

FIREARMS ARE NEVER totally silent, although they can be made quiet enough not to attract attention. A silencer eliminates most of the sound of the muzzle blast, but not the sound of the weapon's working parts. Ammunition that travels slower than the speed of sound is used, so avoiding the "crack" caused by supersonic bullets. Most silenced weapons were developed for assassinations or for special operations in armed conflicts. In peacetime, spies who are not on special assassination missions may carry silenced weapons for self-defense. The U-2 spy plane pilot Francis Gary Powers (see p. 52) was issued with the silenced Hi-Standard pistol for use as a hunting weapon in case his plane should be downed in remote enemy territory.

MOSSAD

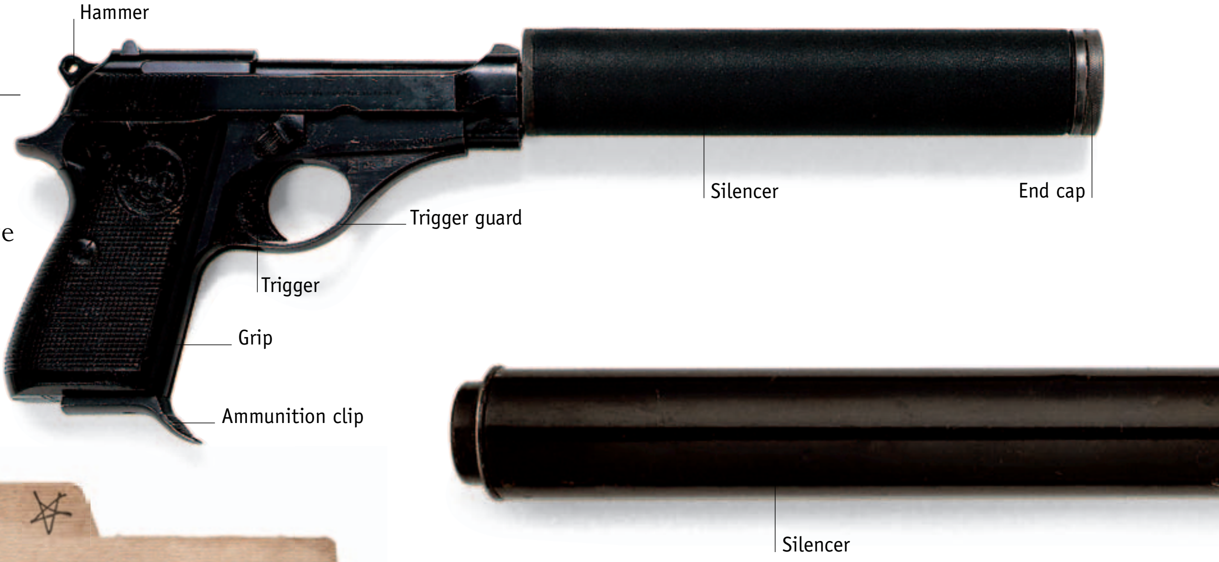
The Institute for Intelligence and Special Operations, or Mossad, was formed in 1951 as Israel's external intelligence service. It is the equivalent of the United States' CIA or Britain's MI6, but employs far fewer personnel: only 30–35 Mossad case officers are active in the whole world. However, the organization often also draws on local volunteers (see p. 209). Mossad is most active against hostile Arab states surrounding Israel and against Palestinian political organizations. One of its most prominent operations was the daring abduction of the Nazi war criminal Adolf Eichmann from Argentina in 1960 to stand trial in Israel. Eichmann was hanged two years later.

המוסד
למודיעין

MOSSAD CREST

Beretta 7.65 mm pistol with silencer

Italian Beretta pistols are often used by Mossad. The small Beretta is easy to conceal and can be loaded with reduced-charge cartridges in order to increase the effectiveness of the silencer. This adaptation of a Beretta Model 70 was issued to members of Mossad's assassination teams (known as *kidon*).



PETER MASON

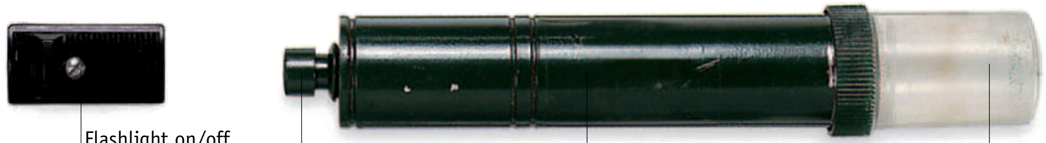
SPY PROFILE

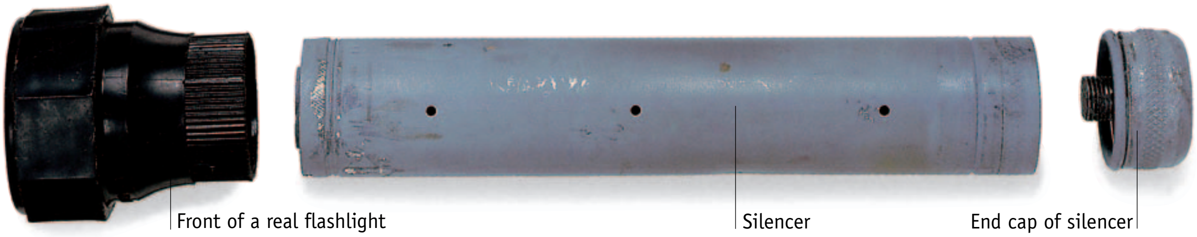
Former Defense Intelligence Staff Captain Peter Mason (b.1927) is one of the leading experts on special weapons and close-combat shooting. In 1946 he joined a British Special Air Service (SAS) "Hunter Team." Using captured enemy weapons, such as the Beretta used by the OVRA (see opposite), these three-man teams hunted down and secretly killed those guilty of murdering SAS or SOE members (see p. 30) during World War II.

SS Colonel Otto Skorzeny
Otto Skorzeny (1908–75) was the commander of Germany's Brandenburg commando detachment in World War II. He mounted a number of audacious operations, including the dramatic rescue of the Italian leader Mussolini from Italian resistance forces. Skorzeny often used a captured British silenced Sten submachine gun for his operations.

Silencers disguised as flashlights

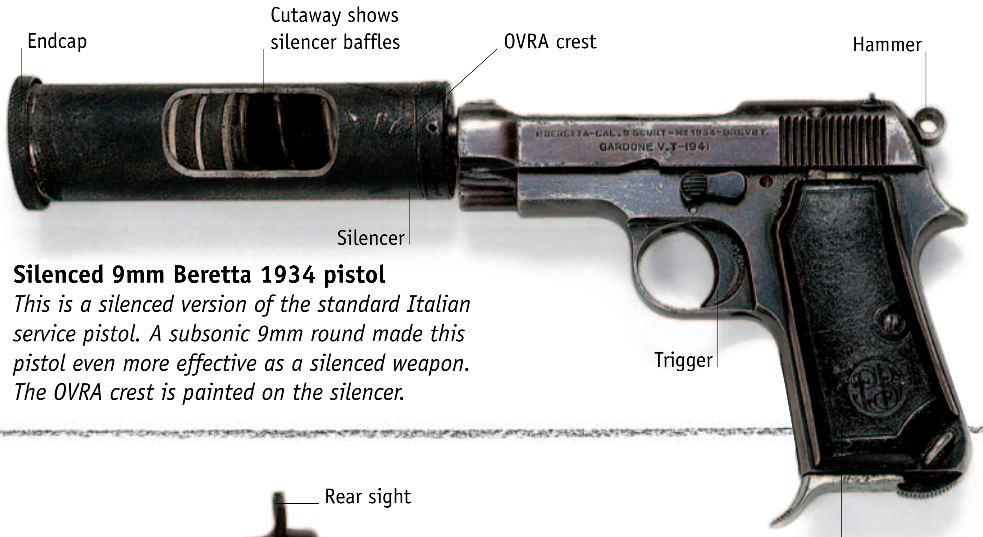
These two British special forces silencers were disguised as flashlights so that they could be transported secretly without arousing any suspicion. Although the flashlights did not work, the disguise was effective when the flashlights were packed with other ordinary workshop tools. The parts added for disguise were easily removable, enabling the the silencers to be converted rapidly for their real purpose.


Flashlight on/off switch (glued to side of silencer)
False end plug
Silencer
Cap from a real flashlight

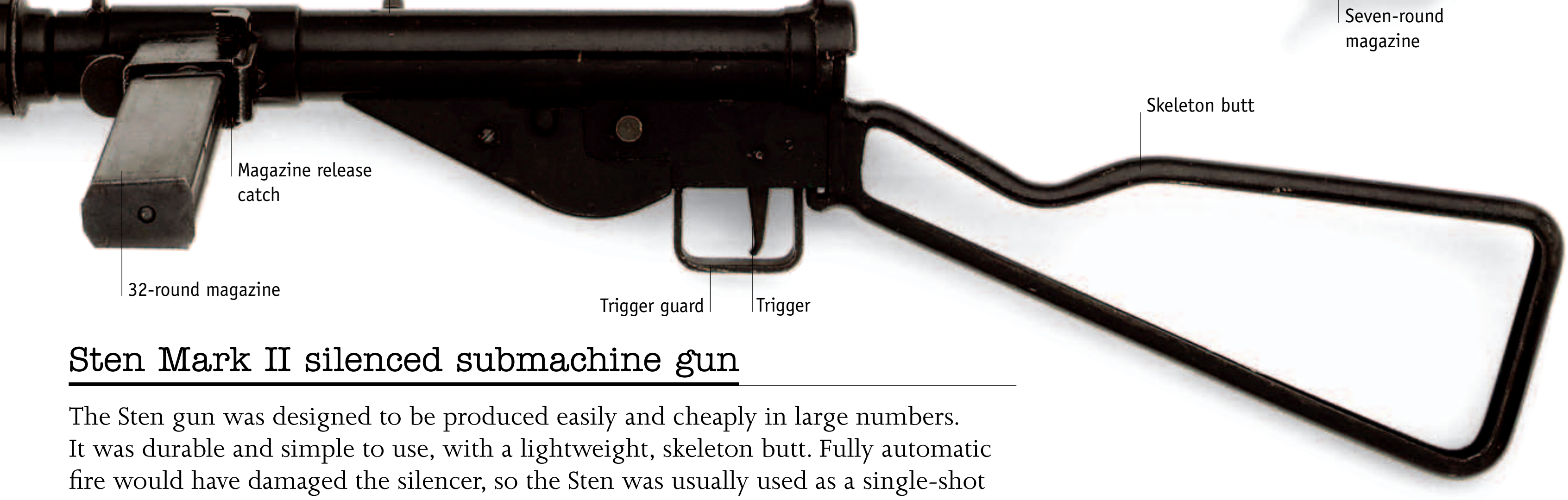


ITALIAN FASCIST SECRET POLICE

Italy's Organizzazione di Vigilanza e Repressione dell'Antifascismo (OVRA) was formed in 1926 to suppress opposition to the Italian fascist government. During World War II, the OVRA operated against resistance groups in the French Alps and in the Balkans. The OVRA also recruited a number of double agents (see p. 216), who spied on the activities of Britain's SOE in Italy. Some OVRA members remained loyal to the Italian fascist regime until the closing stages of the war. The pistol shown here was carried in 1945 by an OVRA team led by a German officer.



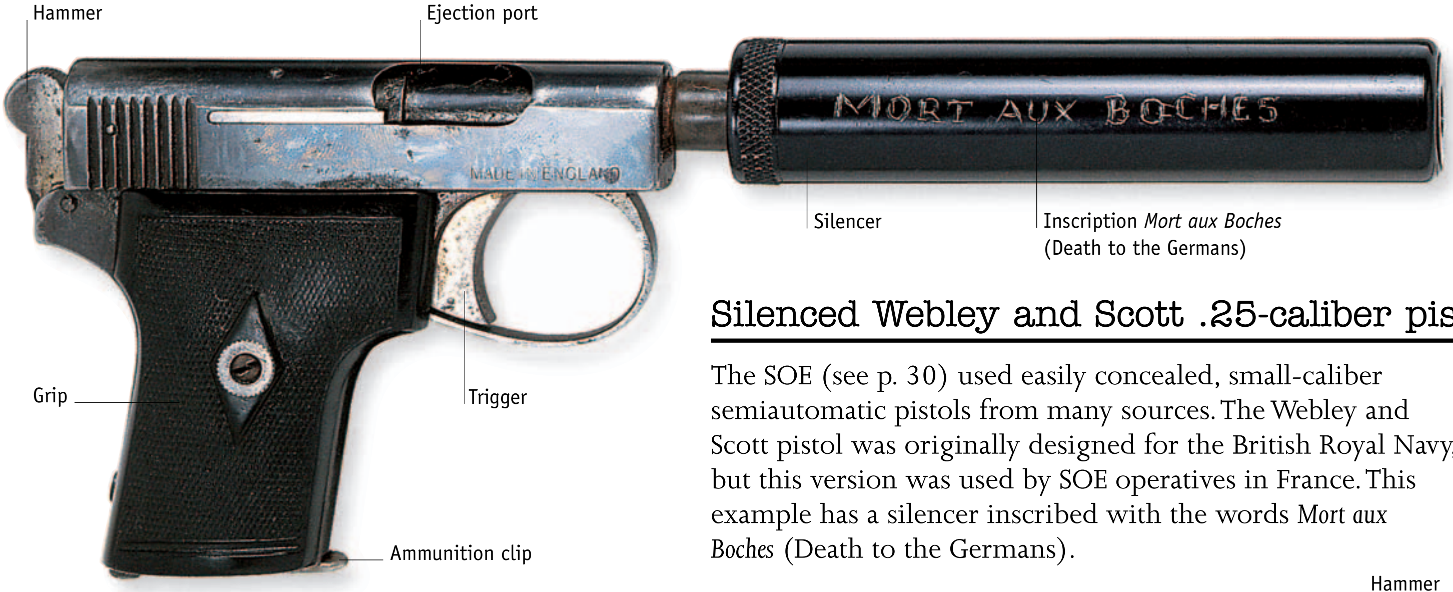
Silenced 9mm Beretta 1934 pistol
This is a silenced version of the standard Italian service pistol. A subsonic 9mm round made this pistol even more effective as a silenced weapon. The OVRA crest is painted on the silencer.



Sten Mark II silenced submachine gun

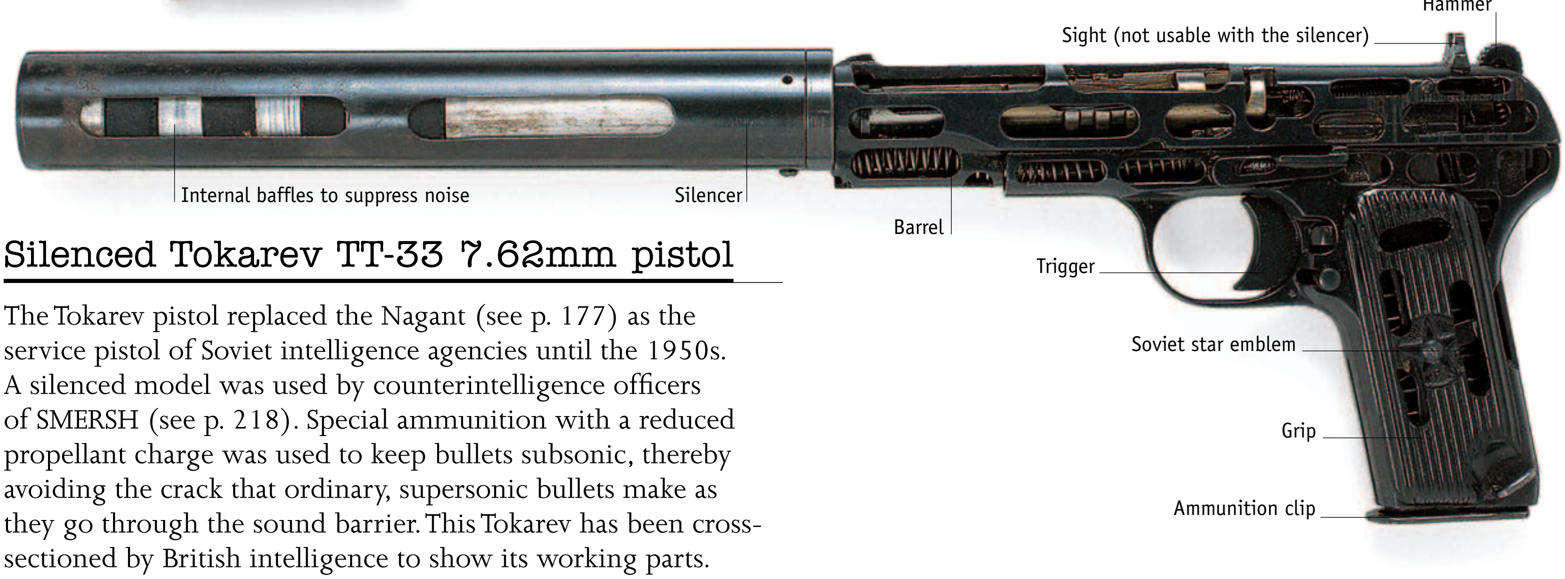
The Sten gun was designed to be produced easily and cheaply in large numbers. It was durable and simple to use, with a lightweight, skeleton butt. Fully automatic fire would have damaged the silencer, so the Sten was usually used as a single-shot weapon. This silenced model was used by British commandos, but another version known as the Mark IIS was developed by the SOE.

Silenced weapons II



Silenced Webley and Scott .25-caliber pistol

The SOE (see p. 30) used easily concealed, small-caliber semiautomatic pistols from many sources. The Webley and Scott pistol was originally designed for the British Royal Navy, but this version was used by SOE operatives in France. This example has a silencer inscribed with the words *Mort aux Boches* (Death to the Germans).


Hammer
Sight (not usable with the silencer)
Internal baffles to suppress noise
Silencer
Barrel
Trigger
Soviet star emblem
Grip
Ammunition clip

Silenced Tokarev TT-33 7.62mm pistol

The Tokarev pistol replaced the Nagant (see p. 177) as the service pistol of Soviet intelligence agencies until the 1950s. A silenced model was used by counterintelligence officers of SMERSH (see p. 218). Special ammunition with a reduced propellant charge was used to keep bullets subsonic, thereby avoiding the crack that ordinary, supersonic bullets make as they go through the sound barrier. This Tokarev has been cross-sectioned by British intelligence to show its working parts.

Winchester Model 74 .22-caliber rifle

American Winchester 74 sporting rifles were purchased for the British Home Guard Auxiliary Units and modified by the addition of British-made accessories: a Parker Hale silencer and an Enfield telescopic sight. The rifles were intended for use against German soldiers and tracker dogs if the Germans invaded Britain—which never happened. However, during tests simulating the rough conditions of operating from underground shelters that would be likely in the event of an invasion, the rifles proved unsuitable for use because their sights were easily knocked out of alignment.

HOME GUARD AUXILIARY UNITS

The Home Guard was a locally based army in Britain during World War II, composed of spare-time soldiers who also continued to work in their normal civilian jobs. The Auxiliary Units were an elite force drawn from its ranks. Units were trained to wage guerrilla warfare behind German lines in case of an invasion of Britain and were issued with secret stocks of weapons and explosives.

AUXILIARY UNIT BADGE

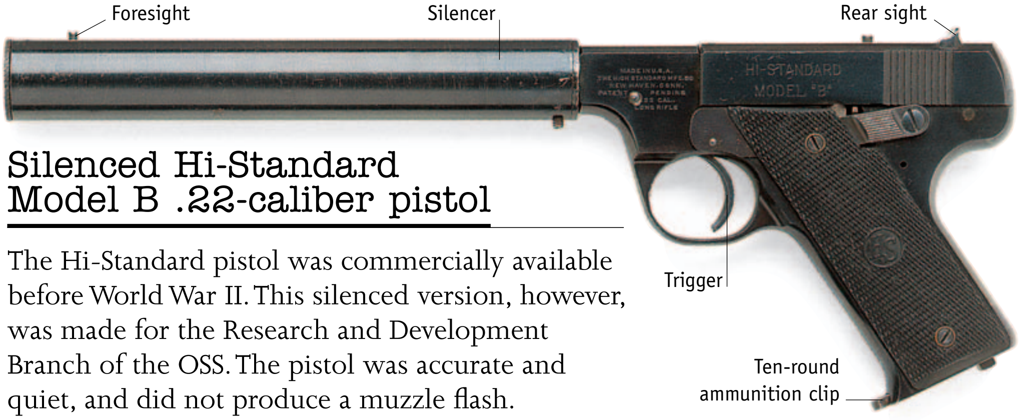
COLBY'S JEDBURGH TEAM

The World War II Jedburgh teams were made up of three men from the SOE or OSS (see p. 32), and Free French units (see p. 31). Teams were sent to France in 1944 to coordinate resistance activities supporting the Allied invasion of France. OSS Major William Colby, later to become head of the CIA (see p. 33), was a member of a Jedburgh team codenamed Bruce. His two Free French team-mates are shown.

JACQUES FAVEL:
CODENAME GALWAY

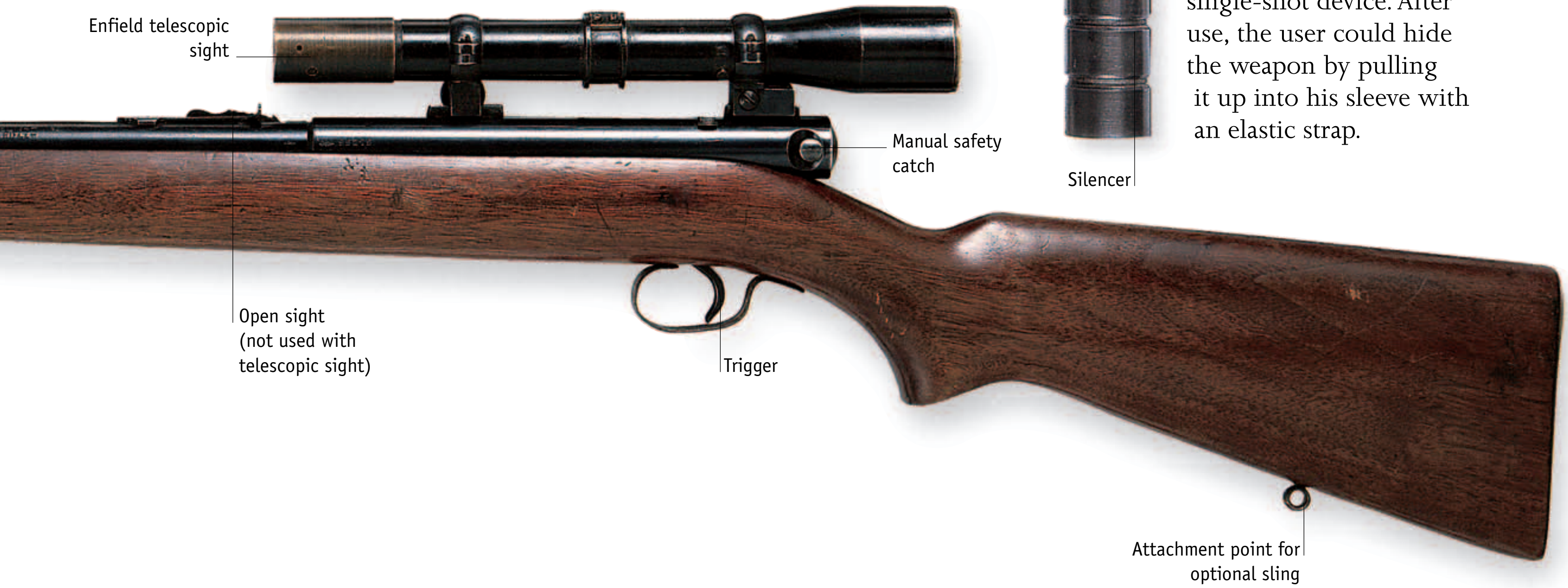
LOUIS GIRY:
CODENAME PIASTRE

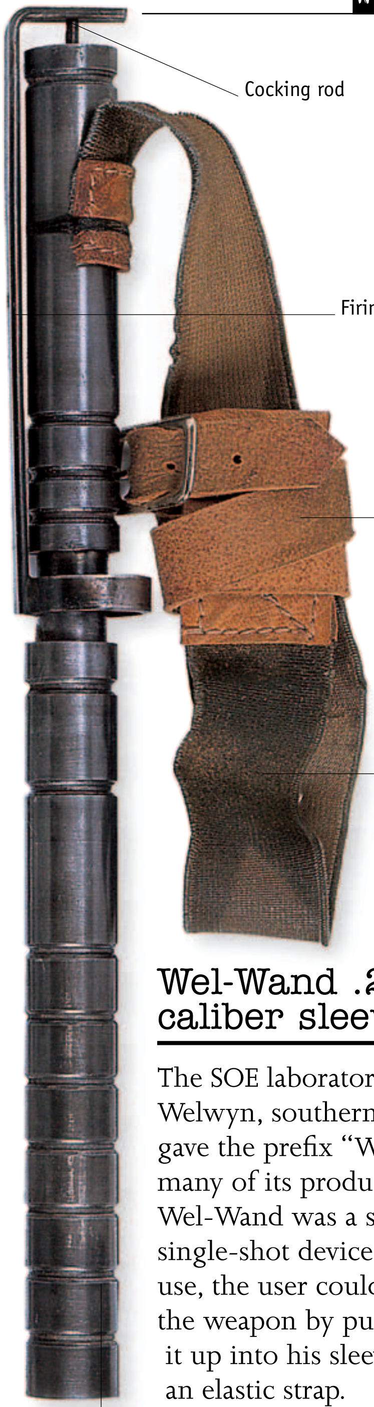
WILLIAM COLBY:
CODENAME BERKSHIRE



Silenced Hi-Standard Model B .22-caliber pistol

The Hi-Standard pistol was commercially available before World War II. This silenced version, however, was made for the Research and Development Branch of the OSS. The pistol was accurate and quiet, and did not produce a muzzle flash.


Enfield telescopic sight
Manual safety catch
Open sight (not used with telescopic sight)
Trigger
Attachment point for optional sling



Wel-Wand .25-caliber sleeve gun

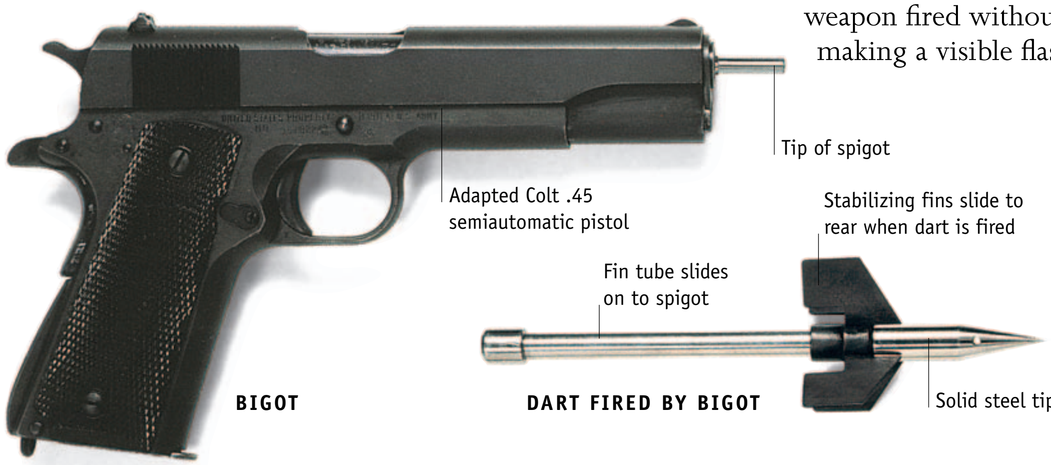
The SOE laboratory in Welwyn, southern England, gave the prefix "Wel-" to many of its products. The Wel-Wand was a silenced single-shot device. After use, the user could hide the weapon by pulling it up into his sleeve with an elastic strap.

Crossbows and darts

MANY INTELLIGENCE AGENCIES have tried to develop weapons capable of firing silently and without emitting a muzzle flash. During World War II, some designs were based on earlier weapons: medieval crossbows and slingshots were the inspiration for the Big Joe 5 crossbow, while a close-range weapon called the bigot was a pistol adapted to fire a dart. But, after tests proved that these weapons were less effective than the newly improved silenced guns, they were not adopted. Weapons invented since World War II include a steel crossbow developed for British special forces.

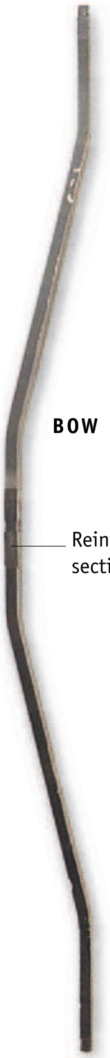
Dart-firing pistol

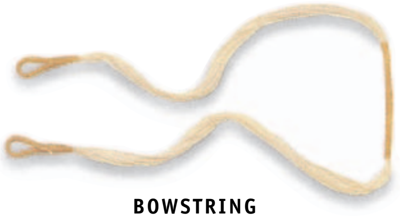
Invented in the United States in 1944, the bigot was a pistol adapted to fire a dart. This was launched from a structure known as a spigot, which protruded from the gun's muzzle. The dart's flight was powered by the blast from a blank cartridge located inside the forward end of the fin tube. The weapon fired without making a visible flash.

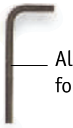

Tip of spigot
Adapted Colt .45 semiautomatic pistol
Stabilizing fins slide to rear when dart is fired
Fin tube slides on to spigot
BIGOT
DART FIRED BY BIGOT
Solid steel tip

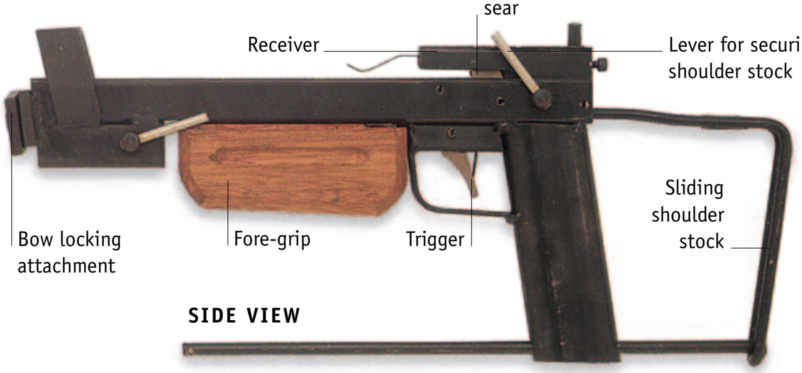
Steel crossbow

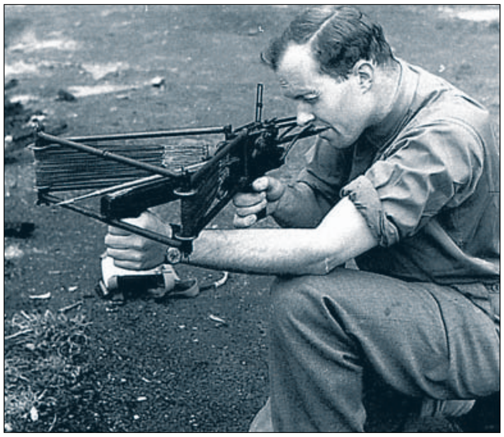
This lightweight British weapon from the 1970s has a powerful metal bow. It shoots either a normal steel bolt or a knife blade. Originally meant for use in assassinations or combat missions, in practice the crossbow has mainly been used for killing guard dogs.







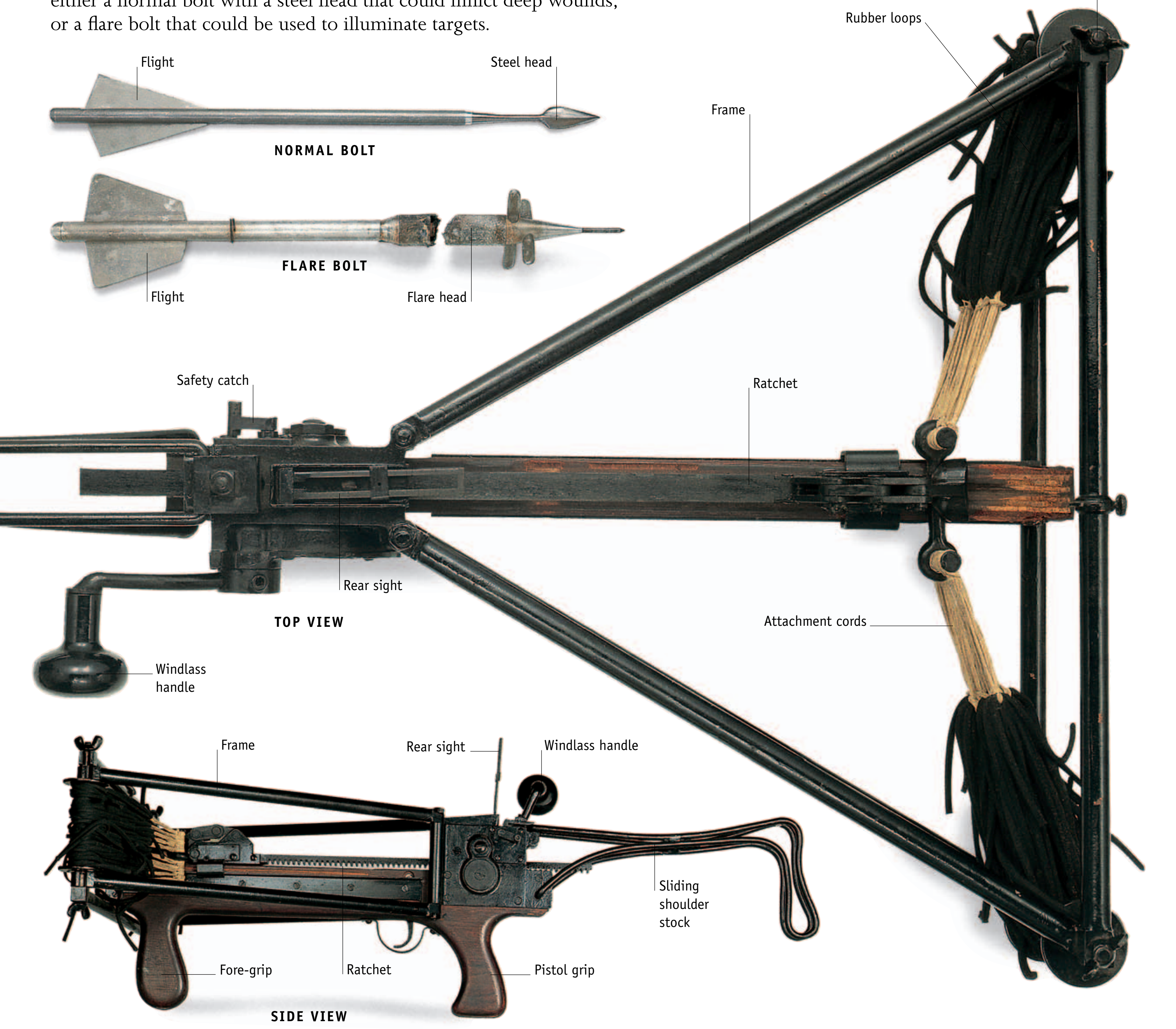




Testing the Big Joe 5 crossbow
Trials showed that the crossbow had a maximum range of 200 yd (180 m), but in practical terms it was less useful than the new silenced firearms.

Big Joe 5 crossbow

This American design was tested during World War II by the SOE (see p. 30) and the OSS (see p. 32), but was not used in action. The crossbow was powered by rubber loops, which were tensioned by a windlass before firing. The front frame and shoulder stock could be folded for easier transportation and concealment. Ammunition was either a normal bolt with a steel head that could inflict deep wounds, or a flare bolt that could be used to illuminate targets.


NORMAL BOLT

FLARE BOLT

TOP VIEW

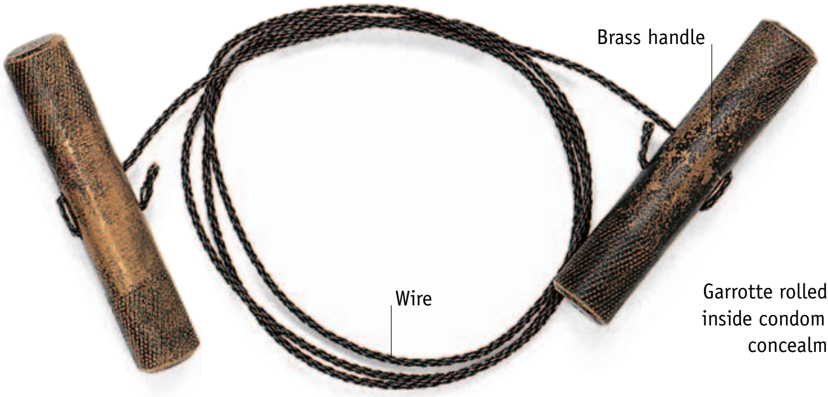
SIDE VIEW

Close-combat weapons I

CLOSE COMBAT is something for which all special operations personnel must be trained and equipped. Specialized close-combat weapons—such as blades, knives, coshes, and garrottes—enable them to overcome an opponent in a swift, silent attack, or to defend themselves in an emergency and hopefully escape alive. The weapons tend to be used as a last resort, perhaps when a silenced firearm is unavailable. Those who are likely to face the dangers of close combat make their own preparations and often buy weapons privately, although some are issued officially.

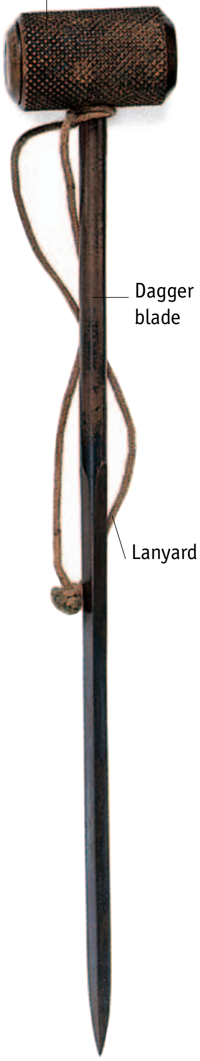
British special forces garrotte

The most common use of a garrotte is to strangle sentries. The wire is looped over the victim's head, around the neck, and pulled tight from behind until the target is dead. Other garrottes have serrated wires that double as escape saws.



Thrust weapon

The brass pommel of this weapon rested in the palm of the hand to add force to a thrusting movement. The lanyard was twisted around the hand to prevent the blade from being lost in action. British marine special forces used this weapon in World War II. Small items (suicide tablets, for instance) could be carried in the pommel.



THRUST WEAPON

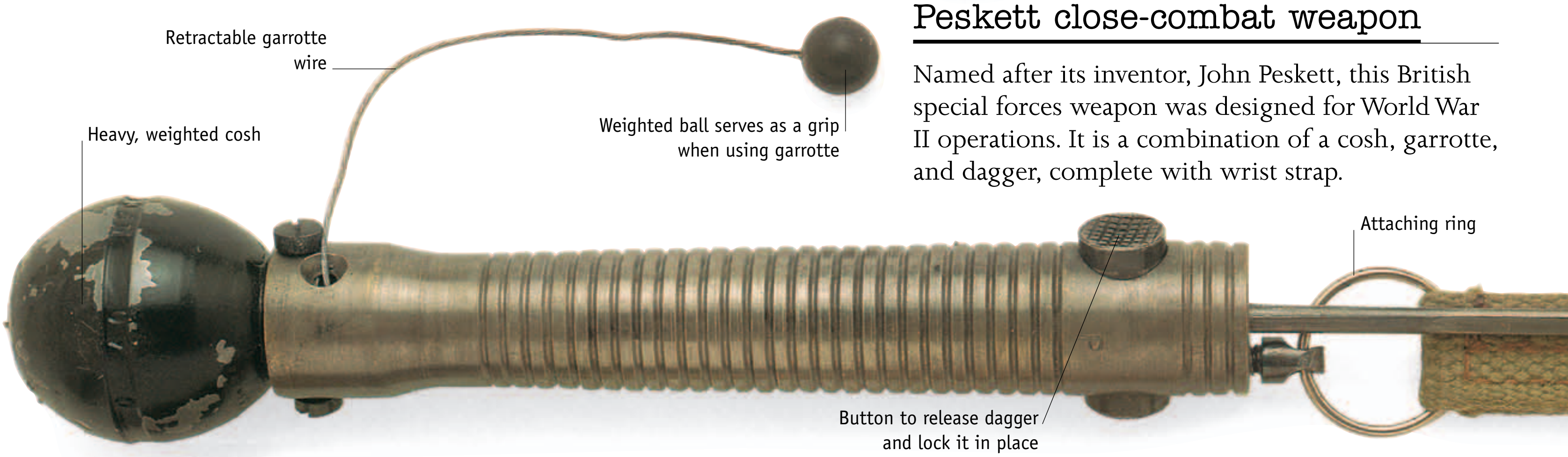
LEATHER SHEATH

Hidden garrotte

Some British special forces in World War II used a condom to conceal a garrotte. It also prevented rust by sealing out moisture. Because condoms were commonly carried, the garrotte might be overlooked if the person carrying one was searched by the enemy.

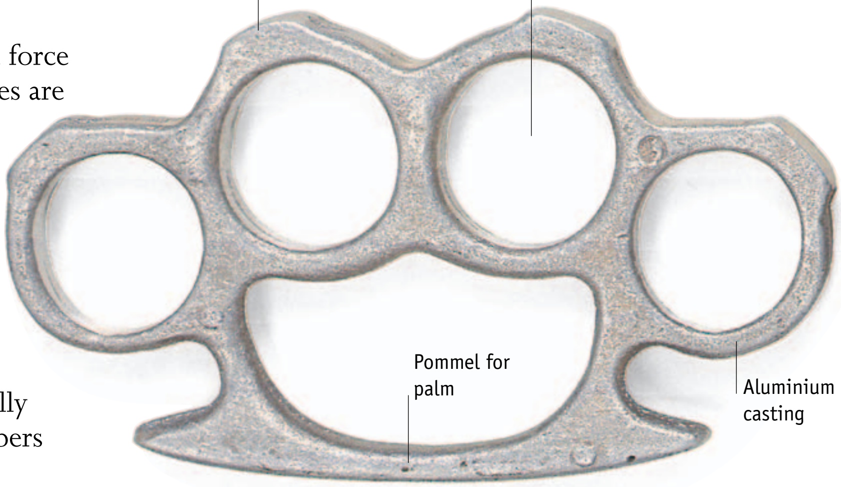
Peskett close-combat weapon

Named after its inventor, John Peskett, this British special forces weapon was designed for World War II operations. It is a combination of a cosh, garrotte, and dagger, complete with wrist strap.


Retractable garrotte wire
Heavy, weighted cosh
Weighted ball serves as a grip when using garrotte
Attaching ring
Button to release dagger and lock it in place

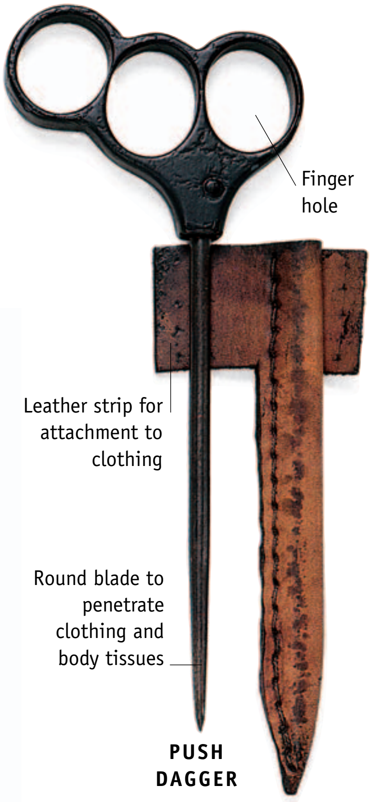
Brass knuckles

Brass knuckles serve as a metal brace to give extra force to a punch. Brass knuckles are bought privately by some intelligence personnel as protection from street crime in some of the rough areas where they operate. During World War II, brass knuckles were occasionally issued officially to members of covert action units.



Push dagger

The three-finger grip of this British weapon from World War II allowed the operator to exert tremendous force at close range.


Finger hole
Leather strip for attachment to clothing
Round blade to penetrate clothing and body tissues
PUSH DAGGER
LEATHER SCABBARD

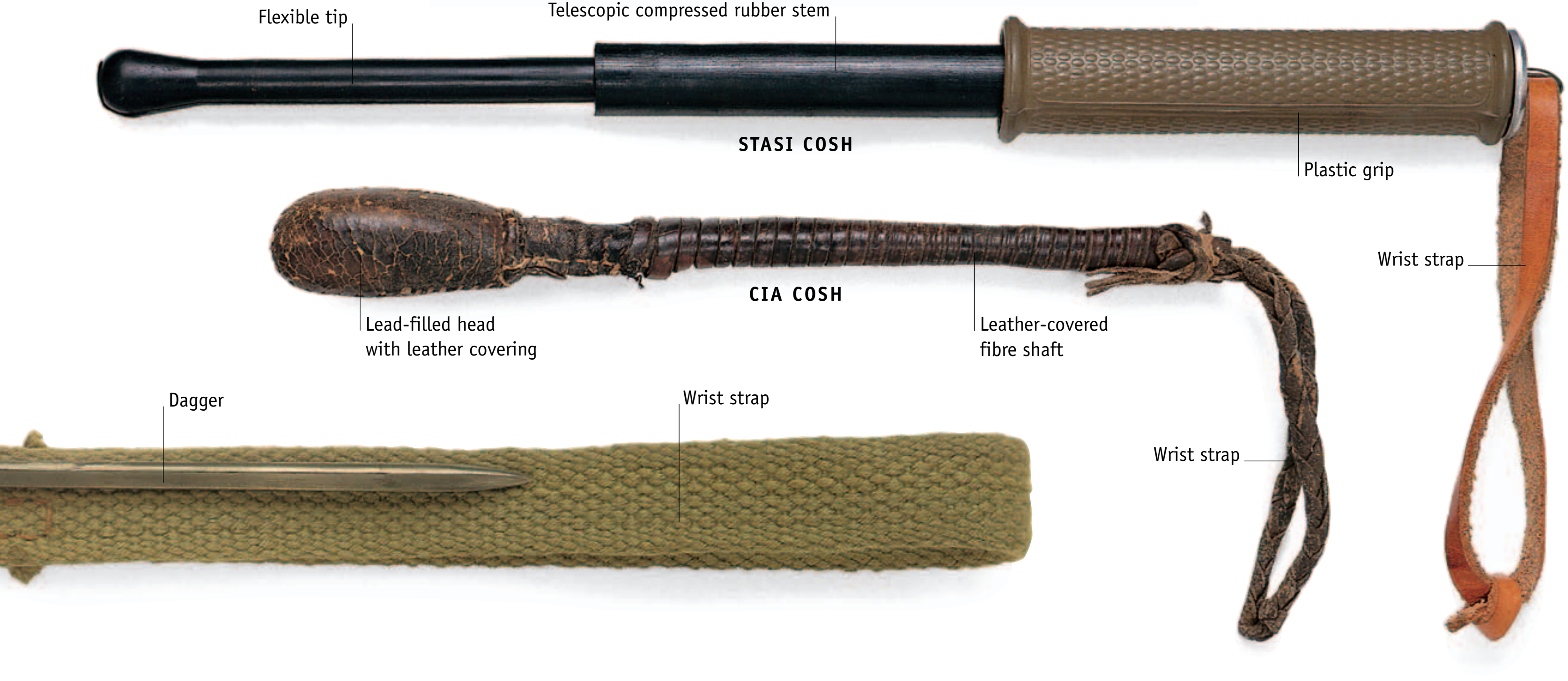
Coshes

Coshes are often used to stun or injure, but a hard blow to the temple or the back of the head can be fatal. The upper cosh was used by the East German Stasi (see p. 99) as a method of crowd control during demonstrations. The lower one was carried by CIA officers operating in Europe during the 1960s as a means of self-defense.

WILLIAM STANLEY-MOSS

SPY PROFILE

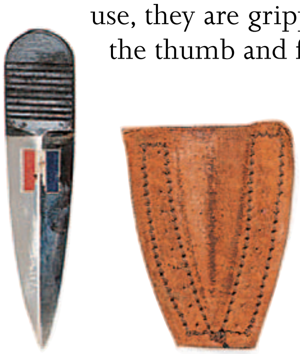
During World War II, Captain Stanley-Moss (1921–65) served in British special operations. In 1944 he was in a team sent to Crete (then under German occupation) to capture General Kreipe, the German commander of the island. The team planned to kidnap the general by ambushing his car, and was issued with coshes for this purpose. They succeeded, although in the event coshes were not used. The general was smuggled to Egypt by submarine.


Flexible tip
Telescopic compressed rubber stem
STASI COSH
Plastic grip
Wrist strap
CIA COSH
Lead-filled head with leather covering
Leather-covered fibre shaft
Wrist strap
Dagger
Wrist strap

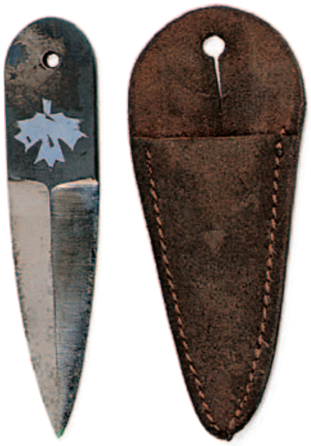
Close-combat weapons II

Thumb knives and scabbards

Thumb knives (these are from World War II) are tiny knives that can be hidden in clothing or a uniform. In use, they are gripped with the thumb and forefinger.



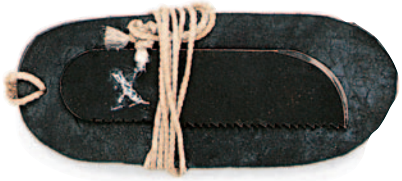
KNIFE WITH FRENCH TRICOLOR



KNIFE WITH CANADIAN MAPLE LEAF

X-TROOP

10 Commando was a British army unit made up of foreign nationals in World War II. Its No. 3 troop, also called X-troop, was made up of anti-Nazi Germans, many of them Jewish. X-troop personnel performed a variety of roles in front-line service. As German speakers, they were specially helpful in intelligence work. But they risked being executed as traitors if captured. Many carried escape aids such as the knife shown here.

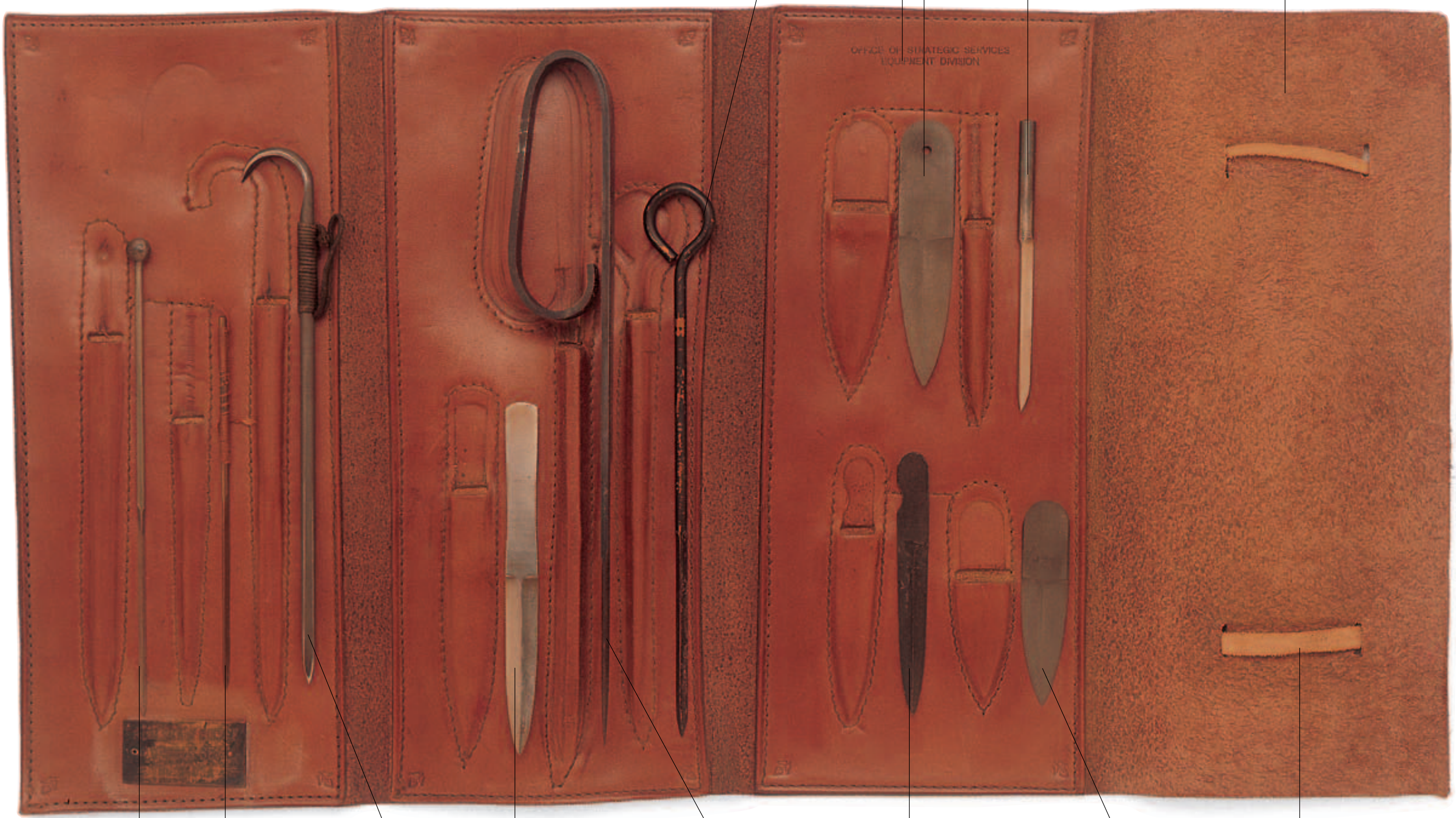


X-TROOP ESCAPE KNIFE

X-TROOP DETACHMENT

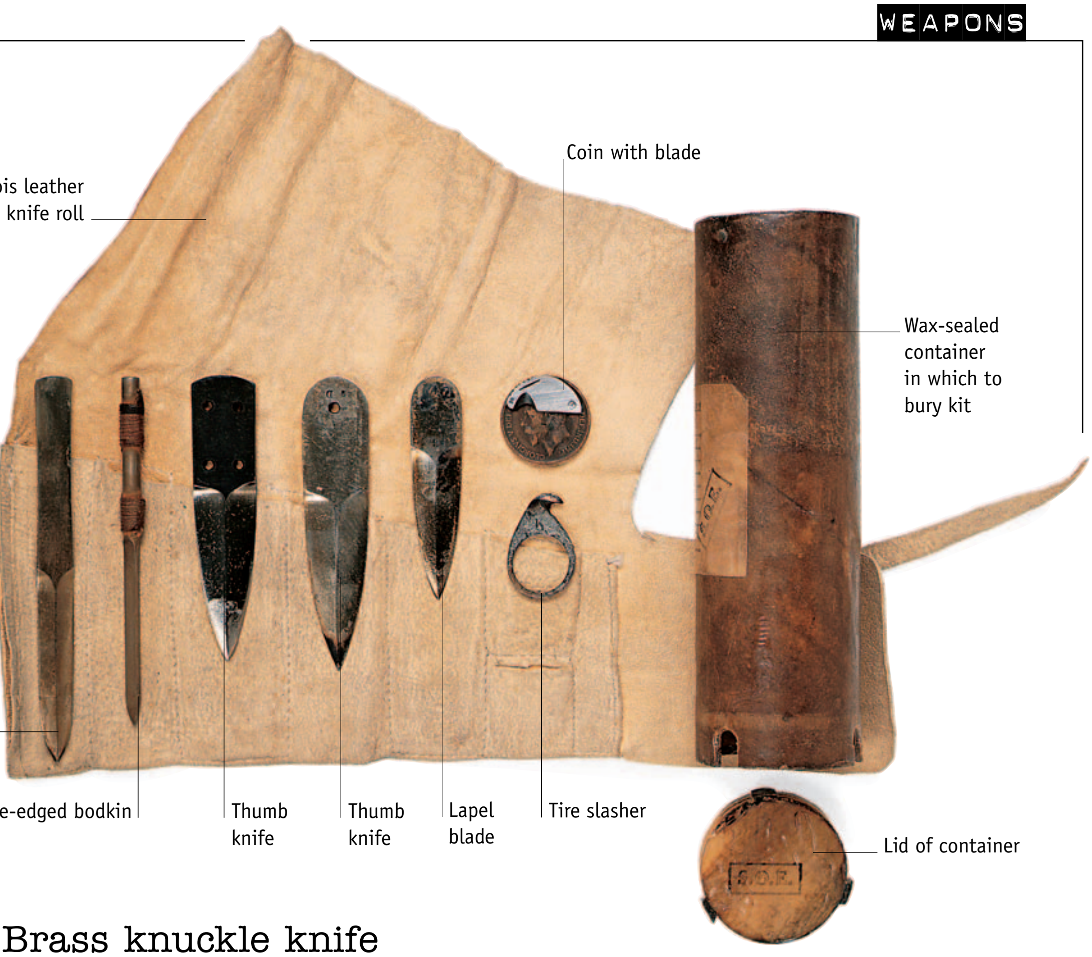
Clandestine blade kit

During World War II, the SOE (see p. 30) sent this blade kit to the OSS (see p. 32) for evaluation, but it was not accepted there for official issue. However, many OSS personnel acquired the blades privately, while attending SOE training schools in Britain.



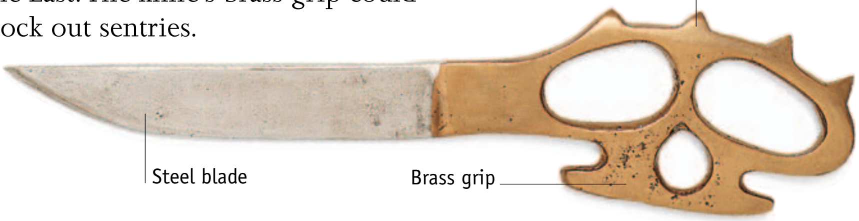
Instructor's blade kit

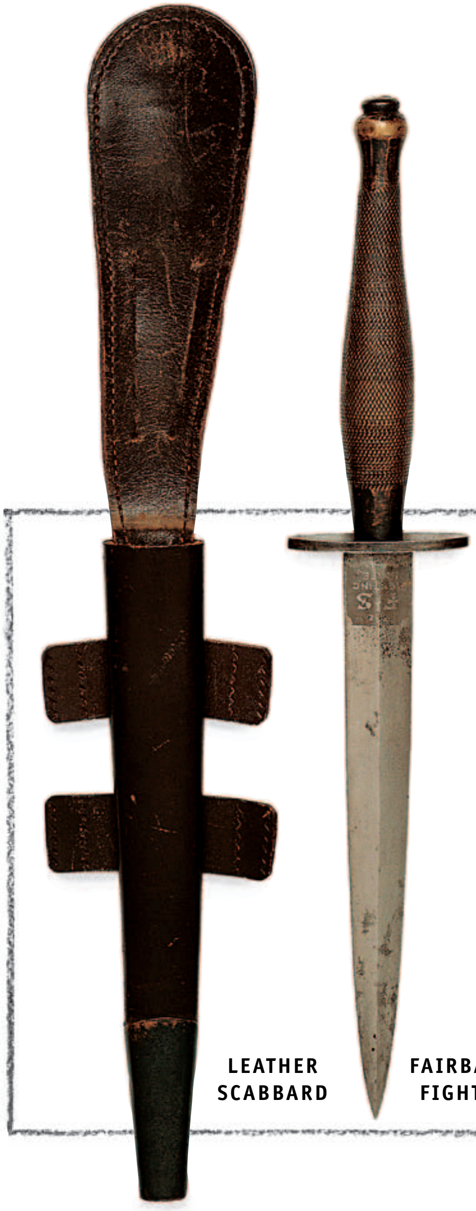
SOE instructors used an assortment of blades for training new personnel during World War II. Packed in wax-sealed containers and wrapped in chamois leather, the kit could also be buried for recovery and use during an operation. This example, buried in the 1940s, was recovered during the 1980s in perfect condition. The blade pack includes thumb and bodkin knives, and a tire-slasher for sabotaging vehicles.



Brass knuckle knife

During World War II, a knife was designed for British commandos operating in North Africa and the Middle East. The knife's brass grip could be used to knock out sentries.





LEATHER SCABBARD

FAIRBAIRN–SYKES FIGHTING KNIFE

FAIRBAIRN–SYKES FIGHTING KNIFE

This weapon was designed in 1940 by two British officers, Captain W. E. Fairbairn and Captain E. A. Sykes (1883–1945). They had gained experience in close combat while serving with the Shanghai Police. Their knife was designed so that a trained user could strike at the vulnerable points of an opponent's body and attack the vital organs, killing the target quickly. The first knives were made in 1941 and were quickly accepted. They were issued to British commando units and used on raids in Norway in 1941. Fairbairn was later loaned as an instructor to the OSS, for which he created a special version of the knife. Successive versions continued to be produced into the 1990s.

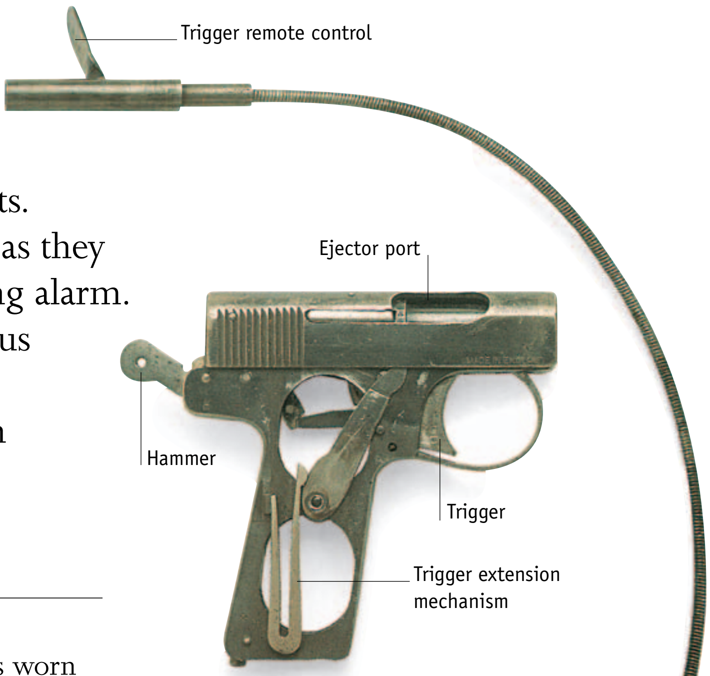
Instructor and inventor
W. E. Fairbairn (1885–1960) in the uniform of a lieutenant colonel, a rank he attained in August 1944.

Concealed weapons I

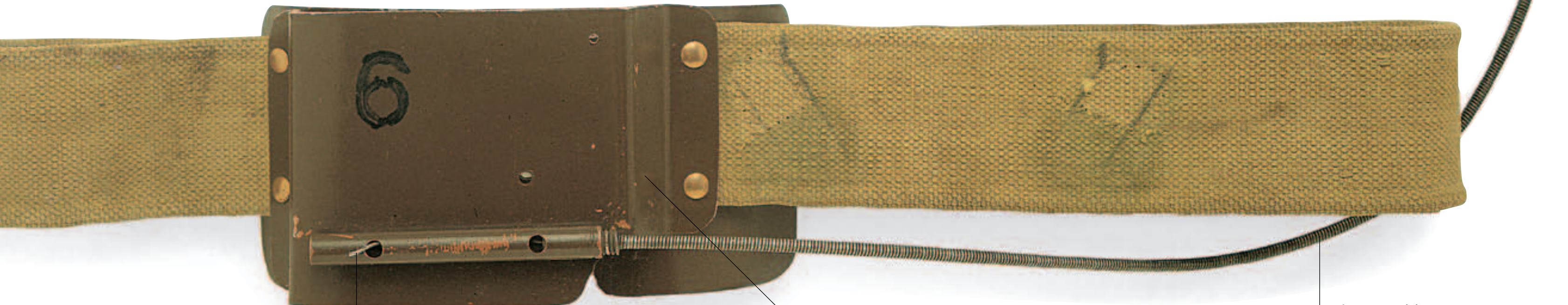
IN CLANDESTINE WARFARE, situations arise in which hidden weapons, perhaps of an unconventional or unexpected kind, may tilt the balance between success and failure. Because concealment generally means limited size, such weapons are likely to be very basic, without refinements such as silencers or magazines of extra bullets. Weapons of this type can also be used for assassinations, as they allow the killer to get close to the victim without arousing alarm. These weapons are issued only to people who have serious need of them and are not carried by those engaged in normal intelligence work. Anyone found in possession of them would be suspected of covert activity.

Belt pistol

This belt and pistol were developed for use by British special operations personnel during World War II. A modified .25-caliber Webley pistol was worn on the belt on the user's right side, facing forward, hidden under the clothing. The trigger was activated by a length of cable that ran to the user's hand.



MODIFIED WEBLEY PISTOL

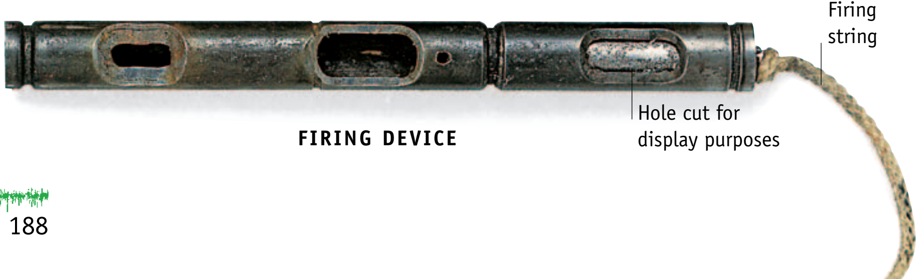

Cable end attached to trigger extension mechanism
Attachment plate for pistol
Trigger cable

BELT WITH PISTOL PLATE

Single-shot cigar pistol

A .22-caliber firing device was disguised as a cigar for use by SOE personnel (see p. 30). It was fired by pulling on the string. Its effective range was just 3 ft (1 m).

FALSE CIGAR

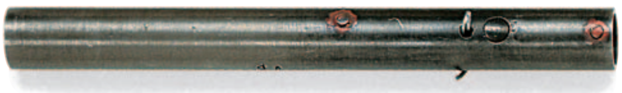


FIRING DEVICE

Single-shot cigarette pistol

This .22-caliber device disguised as a cigarette was developed at the SOE's Welwyn laboratory. The device was fired when the user pulled on a string with his teeth. Because of its short barrel it had a range of only about 3 ft (1 m) and was very loud.

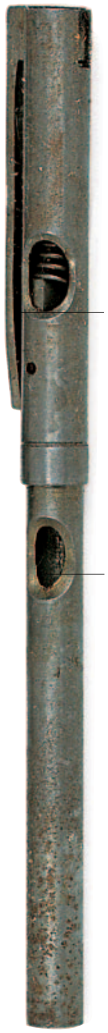
FALSE CIGARETTE



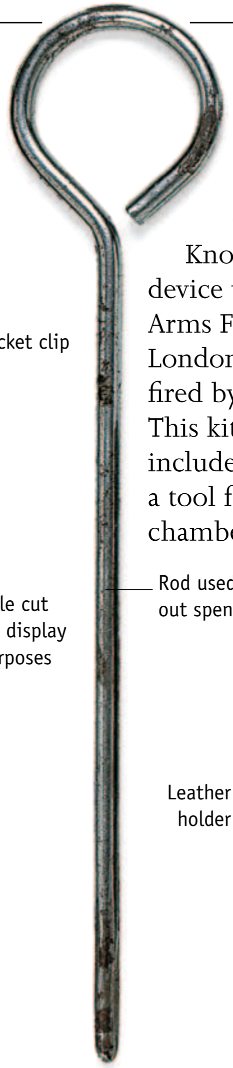
FIRING DEVICE

Single-shot pen gun

Known as the En-Pen, this 22-caliber device was made at the Royal Small Arms Factory at Enfield, north of London, for the SOE. The gun was fired by pulling back the pocket clip. This kit, issued to SOE instructors, included a cartridge ejector rod and a tool for cleaning out wax left in the chamber after firing blanks.



CROSS-SECTIONED VIEW OF GUN



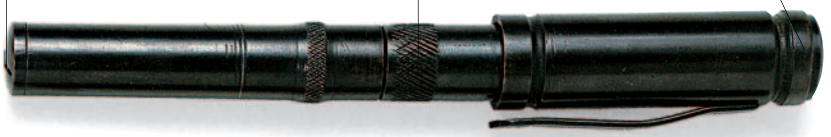
CARTRIDGE EJECTOR ROD

SET OF BLANK CARTRIDGES

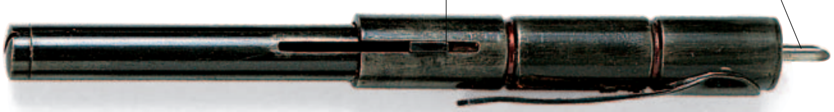
CLEANING TOOL

Single-shot gas and poison pens

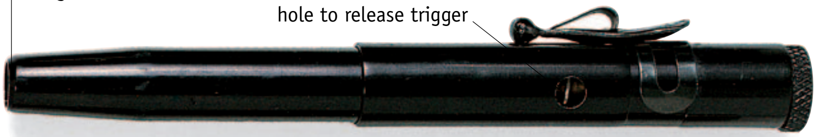
The KGB assassination pen fired a small charge that shattered an ampoule of hydrocyanic acid. This was then projected from the pen as a lethal gas. The pellet pen (also KGB) was used to inject a small pellet impregnated with ricin poison into a victim. The tear gas pen was developed for the SOE during World War II. It had a range of up to 6 ft (2 m).


Gas projection slit
Knurled surface for gripping
Weapon activated by snapping the cap back and releasing

GAS ASSASSINATION PEN



POISON PELLET PEN



TEAR-GAS PEN

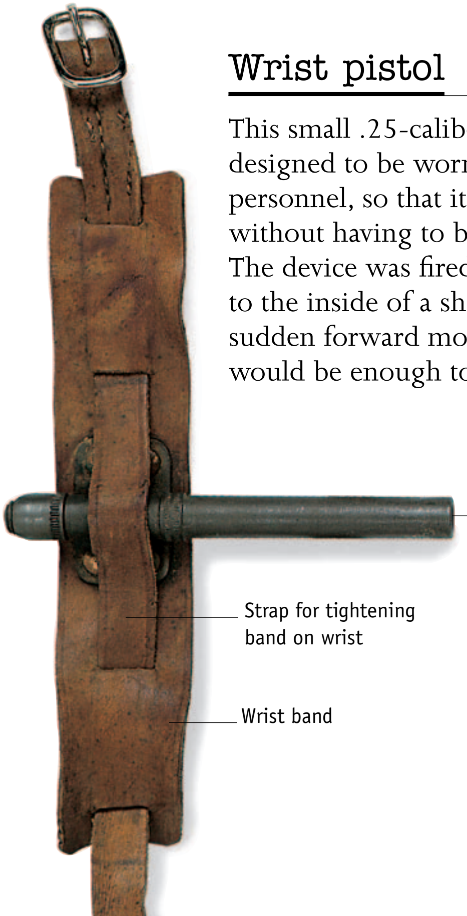
STANLEY LOVELL

During World War II, the OSS (see p. 32) began the practice of using industrial resources and the universities to develop new clandestine technology, an innovative approach that came to be widely adopted during the later Cold War years.

Stanley Lovell (1890–1976) was recruited from an academic background. He was personally selected by the OSS chief William Donovan (see p.33) to be OSS director of research and development. Under Lovell's direction, the OSS developed a number of devices for use in clandestine warfare. Among these were the Hi-Standard pistol (see p. 181), the Beano grenade (see p. 126), and the Matchbox camera (see p. 91). Other ideas included an explosive disguised as flour, which could even be baked without exploding, and a plan (never implemented) to attack Japanese cities by releasing bats to which incendiary bombs had been attached (see p. 133).

Wrist pistol

This small .25-caliber firing device was designed to be worn on the wrist of SOE personnel, so that it was readily available without having to be held in the hand. The device was fired by a string attached to the inside of a shirt or jacket. Any sudden forward movement of the arm would be enough to fire the device.


Barrel points in same direction as the outstretched fingers
Strap for tightening band on wrist
Wrist band

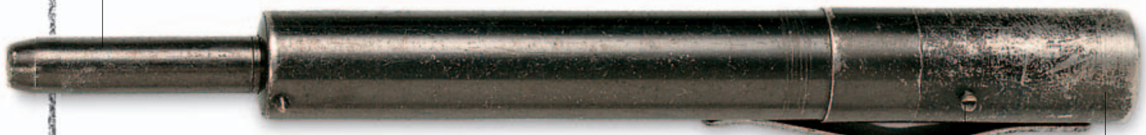
Concealed weapons II

CLAYTON HUTTON WITH M19 DEVICES

MAJOR CHRISTOPHER CLAYTON HUTTON

During World War II, Christopher Clayton Hutton (1893–1965) worked in MI9 (see p. 124), a British organization set up by the armed forces to help British prisoners of war escape, and to assist special forces behind enemy lines. He created numerous weapons, concealments, and escape and evasion aids. One of his inventions was a clandestine airstrip beacon that was only faintly luminous so that it could be seen by an approaching pilot, but was hard to spot at ground level.

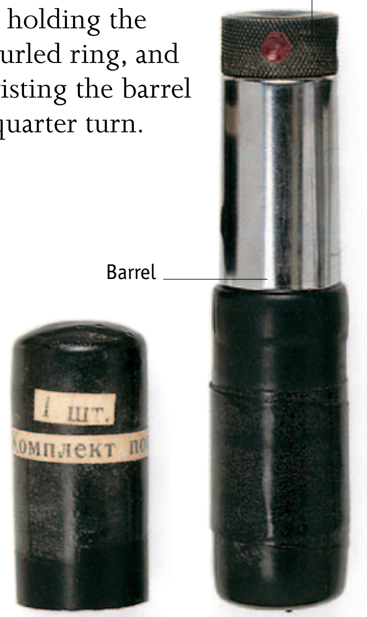
Major Clayton Hutton designed an air-powered firing device for the French resistance in Paris. The device was disguised as a pen and fired a gramophone needle. Although this weapon was unlikely to be lethal, the resistance would be able to spread a rumor among the Germans that the needles were poisoned. French units expressed interest in the weapon, but MI9 was unable to supply the quantity required.



Needle-firing pen
This pneumatic weapon was devised by Clayton Hutton for use by French resistance fighters during World War II.

Single-shot rectal pistol

This KGB 4.5mm firing device is packaged in a rubber sheath to facilitate concealment in the rectum. This is a common way of hiding items from cursory searches. The device was fired by holding the knurled ring, and twisting the barrel a quarter turn.

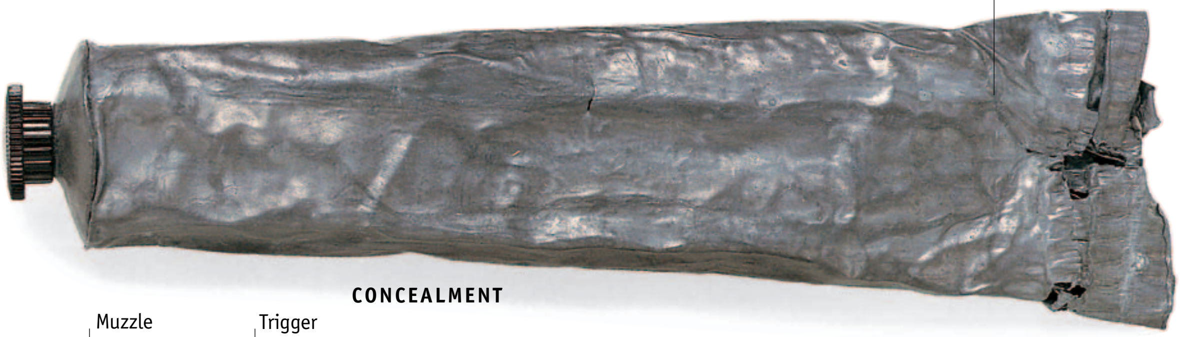


SAFETY COVER

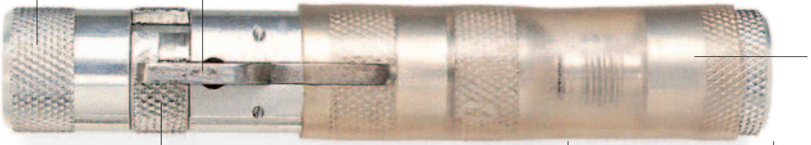
FIRING DEVICE

Single-shot firing device (stinger)

The Stinger was developed for the CIA during the post-World War II years. A reloadable .22-caliber device, the Stinger was issued with a spare barrel and seven rounds of ammunition in a camouflaged lead foil tube.



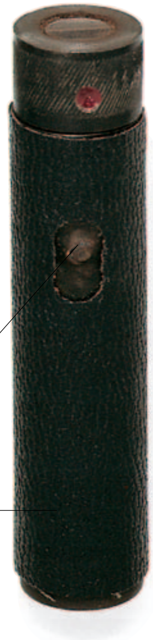
CONCEALMENT



SINGLE-SHOT FIRING DEVICE

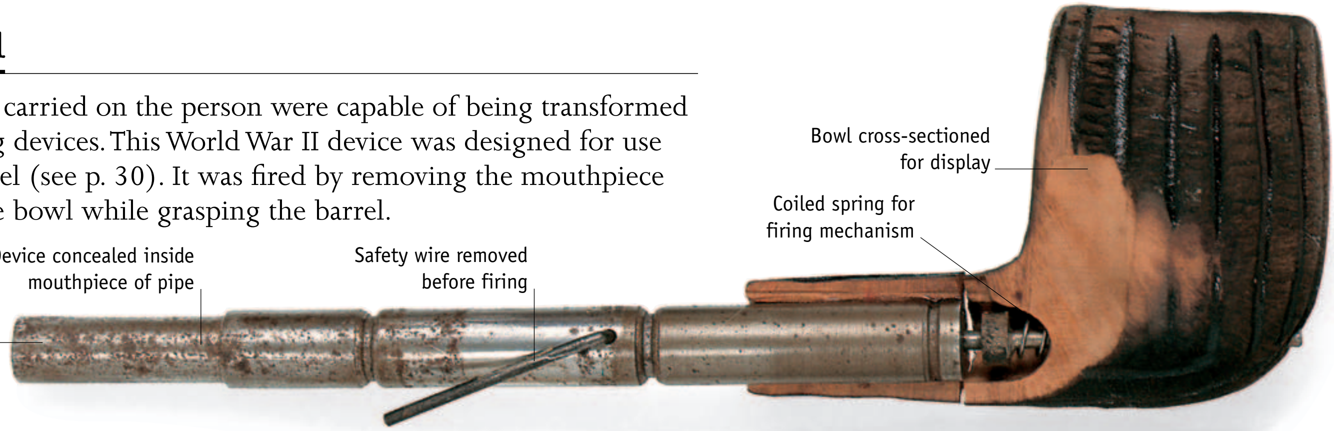
Single-shot pocket flashlight pistol

This 4.5mm device, disguised as a pocket flashlight, was used by the KGB in the 1950s and 1960s. Its mechanism was the same as in the pistol above. This example was seized at a British airport from the pilot of a Soviet civil aircraft.



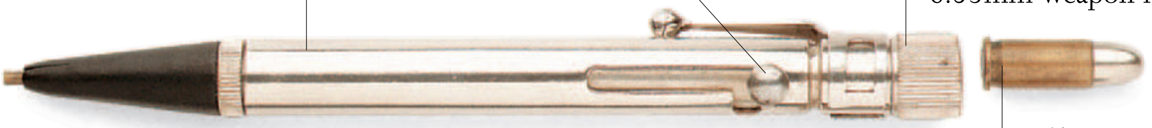
Pipe pistol

Common items carried on the person were capable of being transformed into lethal firing devices. This World War II device was designed for use by SOE personnel (see p. 30). It was fired by removing the mouthpiece and twisting the bowl while grasping the barrel.


Bowl cross-sectioned for display
Coiled spring for firing mechanism
Device concealed inside mouthpiece of pipe
Safety wire removed before firing
Muzzle

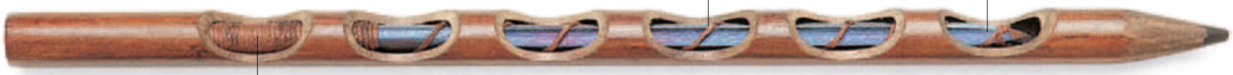
Mechanical pencil pistol

Unusual in that it functioned without a barrel, this 6.35mm weapon fired its bullet straight from the cartridge, which was loaded into the top section of the pencil. The device was sold commercially in Europe at the time of World War II.


Casing contains spring-loaded hammer
Button pulled back and released to fire
Tip unscrewed to load cartridge
Cartridge

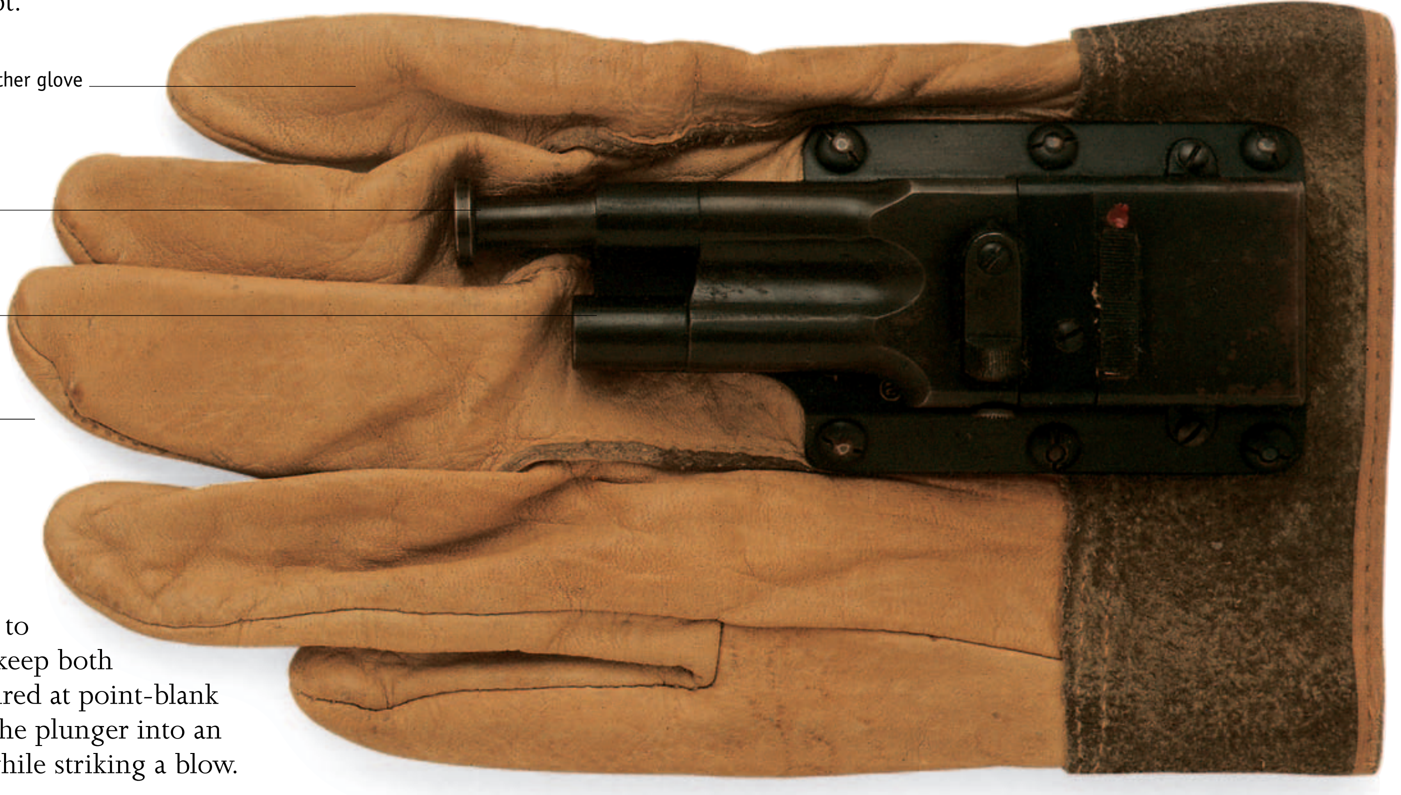
Pencil concealment for thrusting weapon

MI9 designed a variety of small thrusting weapons that could be concealed inside pencils and pens. The intention was that the device would pass unnoticed through an initial search and could then be used in an escape attempt.



Glove pistol

Devised in World War II by the US Office of Naval Intelligence, this .38-caliber device allowed the wearer to be armed and still keep both hands free. It was fired at point-blank range by pressing the plunger into an opponent's body while striking a blow.

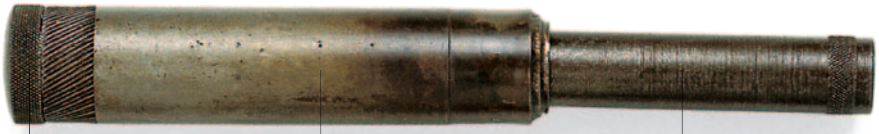


Assassination devices I

INTELLIGENCE AGENCIES are sometimes ordered to assassinate individuals who are considered by their governments to be a threat to national interests. In most cases, such killings have to be discreet, quiet, and untraceable to the assassins. Sometimes they are performed in such a way as to give the impression that the victim died of natural causes. Some killings, however, can serve as warnings, and might be done more blatantly. The need for discretion has led to the development of many types of assassination device, some of which are shown here. Secret services of the Soviet bloc countries used to specialize in assassinations. They devised a variety of methods, and even established a special workshop to experiment with poisons.

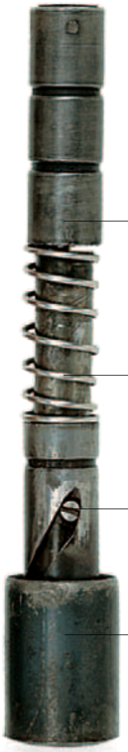
Single-shot assassination device

Developed during World War II by the technical department of the Abwehr (see p. 34), this device could be used for assassinations or for suicides. It fired a single 4.5mm bullet a short distance, and worked by pulling back and then releasing the rear section of the device. It is shown here at its actual size.



Poison pellet cane

The KGB developed this cane in the 1950s. It is operated by pressing the tip against a body. The pressure rotates the tip to extend a large needle. When the needle is extended, a poison pellet is fired through it and into the victim, with fatal effect.


Powder charge and poison pellet
Spring
Rotating cam
Tip through which large needle protrudes

TIP OF POISON PELLET CANE

POISON PELLET CANE

BULGARIAN SECRET SERVICE CREST

THE BULGARIAN UMBRELLA

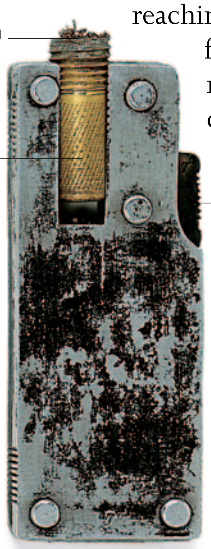
In 1978 Georgi Markov (b.1929), a Bulgarian dissident living in London, was killed on the orders of the Bulgarian leadership. The Bulgarians had asked the KGB to give technical assistance in devising an assassination method, and the KGB offered three choices: poisoned food; poisonous jelly to be smeared on Markov's skin; or a poison pellet.

A pellet filled with the lethal poison ricin was chosen. This was injected into Markov's thigh by means of a device disguised as an umbrella, which was jabbed at Markov as he stood on Waterloo Bridge, in London (see p. 197). He died soon afterward. At first his death was a mystery, as no one understood how it had happened. Eventually, however, murder began to be suspected, and Markov's corpse was exhumed. The pellet was found in the course of an autopsy, and the cause of his death understood.

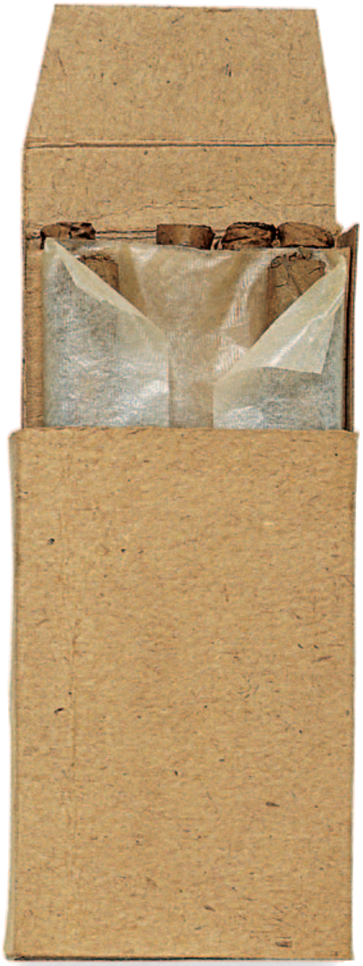
GEORGI MARKOV

Cigarette pack with gas-firing device

The KGB adapted a Soviet cigarette pack to conceal this poison-gas device, which is removed for firing. The single-shot weapon fires a cartridge containing a glass vial of acid. When fired, the vial is crushed and the acid vaporizes in the victim's face. A mesh screen stops glass splinters from reaching the victim's face and thus revealing the cause of death.



GAS-FIRING DEVICE



CIGARETTE PACK

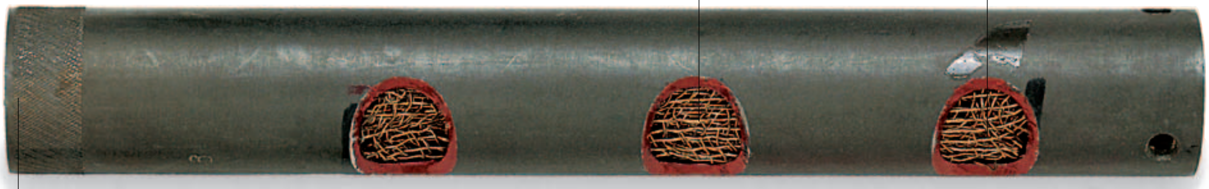
THE FOILED ASSASSINATION

Soviet assassin Nicolai Khokhlov (1922–2007) was sent to Frankfurt, West Germany, in 1954 to kill anti-Soviet agitator Georgi Okolovich. But before departing on his mission, Khokhlov married and converted to his wife's Christian beliefs. Because of these new beliefs, Khokhlov felt unable to carry out the assassination. When he arrived in Frankfurt, he warned Okolovich of the plot to kill him. Khokhlov defected with information about Soviet assassination devices, including the poison-pellet cigarette pack that was meant to kill Okolovich (see p. 196).

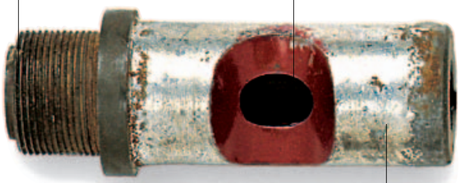
An assassin meets his intended victim
Soviet assassin Nicolai Khokhlov (right), defected rather than attempt to kill his intended victim, Georgi Okolovich, whom he warned of the assassination plot.

Silenced assassination gun

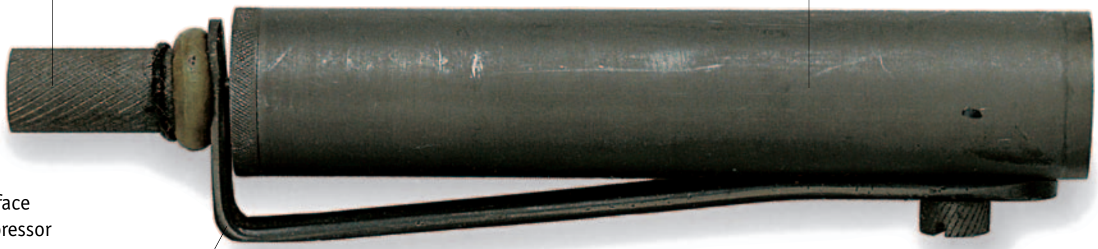
This Soviet weapon is designed to be carried in and fired from a rolled-up newspaper. It is a single-shot device, fired by squeezing the external lever on the rear section of the weapon. It is silenced by an internal suppressor, and further muffled by being pressed up against the victim as it is fired. A later adaptation of this gun, which fires gas, is shown on p. 194.


Mesh inside tube to muffle sound
Hole cut for display purposes
End connected to firing chamber

INTERNAL SUPPRESSOR


Thread screws into rear section of weapon
Hole cut for display purposes
Recessed surface receives suppressor

FIRING CHAMBER

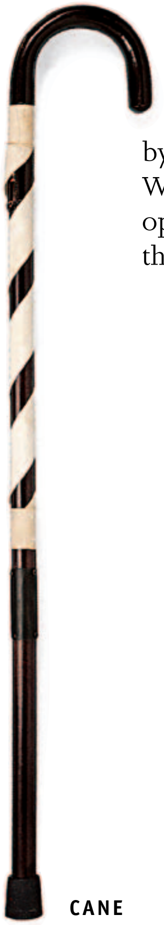


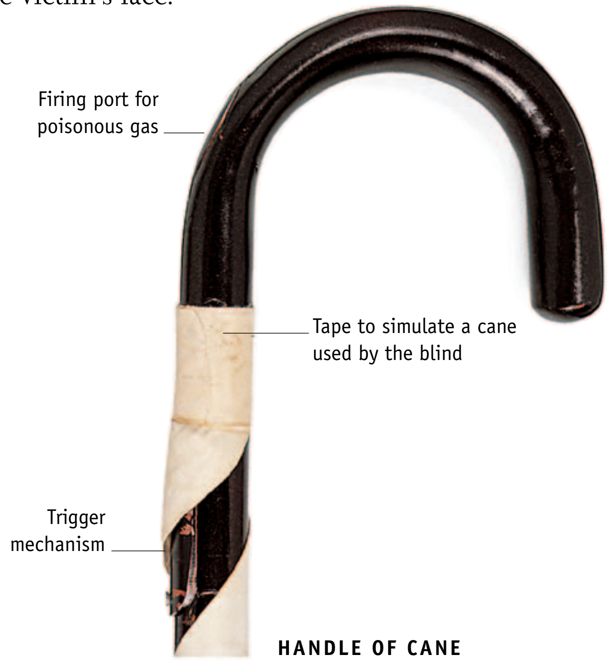
REAR SECTION OF WEAPON

Assassination devices II

Poison gas assassination cane

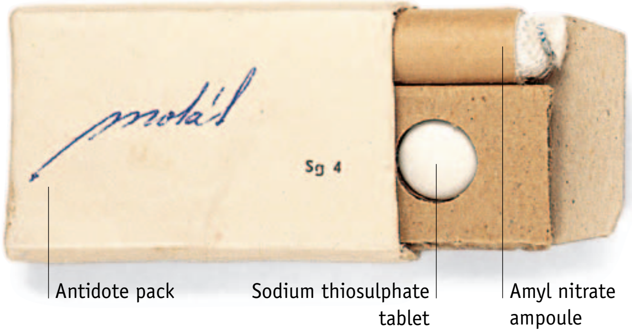
The KGB hid a gas assassination device inside this cane for the blind. The trigger is concealed by the white tape, which was peeled back for use. When the device was fired, it emitted gas from an opening in the handle, which was held close to the victim's face.


CANE


Firing port for poisonous gas
Tape to simulate a cane used by the blind
Trigger mechanism
HANDLE OF CANE

Antidotes for poison gas

KGB personnel who used gas assassination weapons were equipped with antidotes, which they took as a precaution against accidental inhalation of the lethal gas. The tablet of sodium thiosulphate was swallowed 30 minutes before an attack, and the ampoule of amyl nitrate was broken and inhaled immediately after the assassination had taken place.

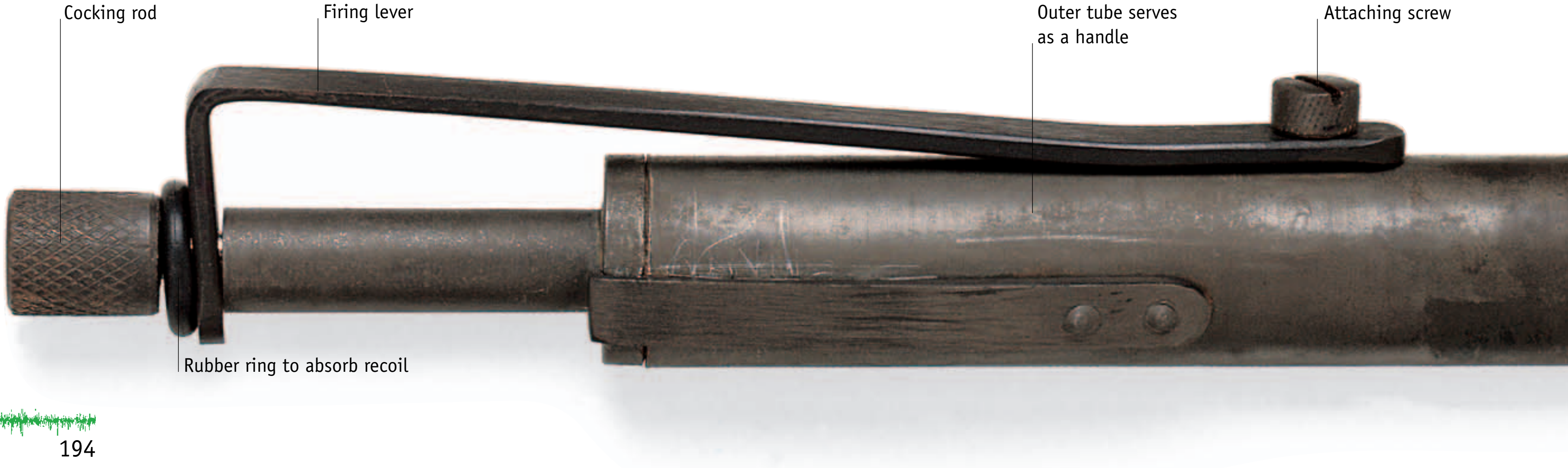


BOGDAN STASHINSKY

In 1957, KGB officer Bogdan Stashinsky (b.1931) killed the Ukrainian dissident leader Lev Rebet in Munich, using a gas assassination gun concealed in a newspaper. Rebet's death was ascribed to a heart attack. In 1959, Stashinsky assassinated the Ukrainian dissident Stefan Bandera, using an improved gas gun. The cause of death was correctly identified this time. Stashinsky defected to West Germany in 1961. He was convicted of the murders but received a short sentence.

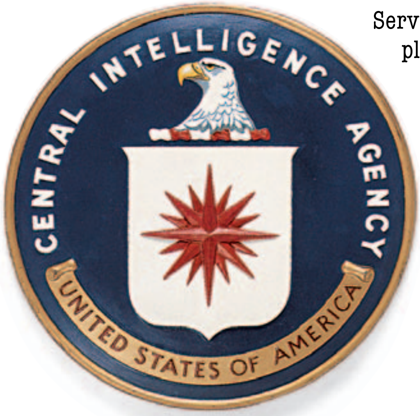
Poison gas assassination gun

This Soviet weapon had the capability to kill almost instantly if fired directly into the victim's face. It is a gas-firing version of the gun shown on p. 193 and, like that gun, was hidden in a rolled-up newspaper. The firing lever activated a firing pin, which detonated a percussion cap, rupturing an ampoule of acid. The acid vaporized into poisonous gas and was propelled out of a small hole. The gas gun is just 7 in (18 cm) long.



PLOTS TO ASSASSINATE FIDEL CASTRO

Between 1960 and 1965, the CIA was involved in eight White House-authorized plots to assassinate Fidel Castro, leader of communist Cuba. (Communist Cuba was considered a particular threat to the United States due to its close proximity.) Equipment and such materials as poisons were provided by the CIA Technical Services Division. Some plots went no further than the planning stage; others progressed further, but none resulted in a serious assassination attempt. One plot twice reached a point at which poison pills were sent to Cuba and agents were despatched to carry out the task. In another plot, weapons were furnished to a Cuban dissident. There was even a plan to impregnate one of Castro's cigars with deadly botulism bacilli. Non-lethal attacks were planned, aimed at destroying Castro's credibility with the Cubans. Such projects included putting thallium salts in his boots to make his beard fall out, and spraying him with hallucinatory drugs while he made a broadcast to the Cuban nation.

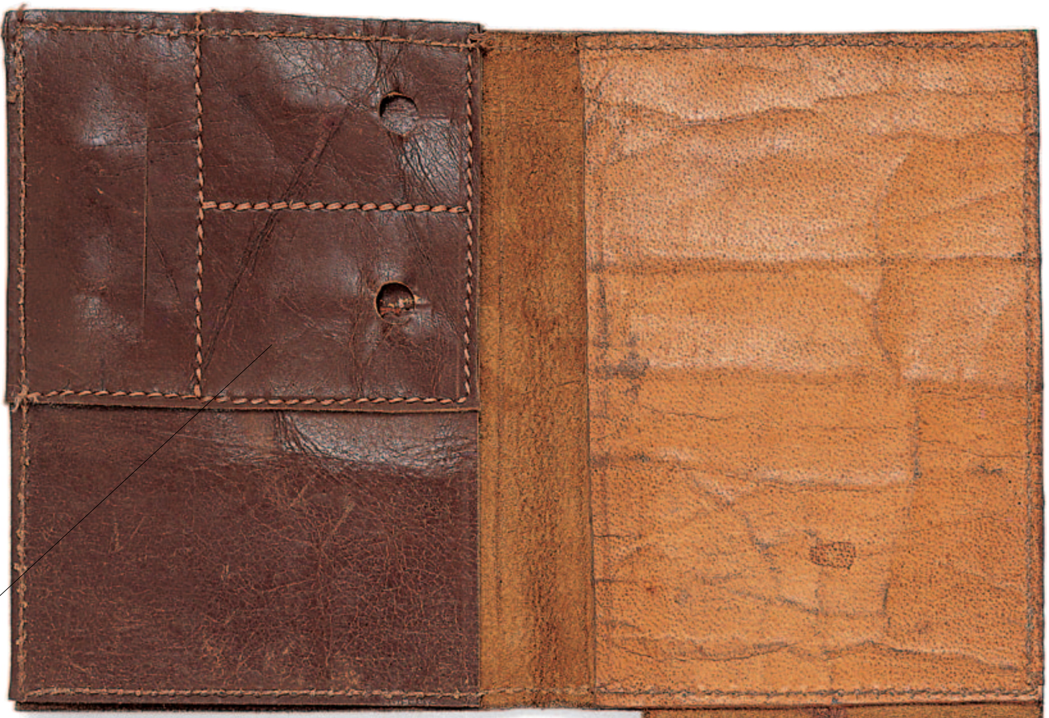


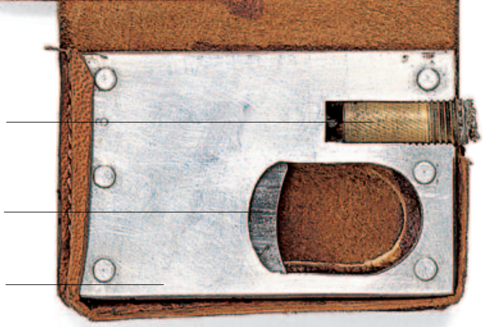
CREST OF THE CIA

FIDEL CASTRO

Gas-firing cartridge assassination wallet

A poison-gas firing device is concealed in this KGB wallet, which also has compartments for gas antidotes to protect the assassin. When the trigger was fired, the primer charge crushed a glass ampoule of poisonous acid that turned into a vapor and killed the victim. A screen over the cartridge prevented shards of glass from the ampoule embedding in the victim and so revealing the cause of death.



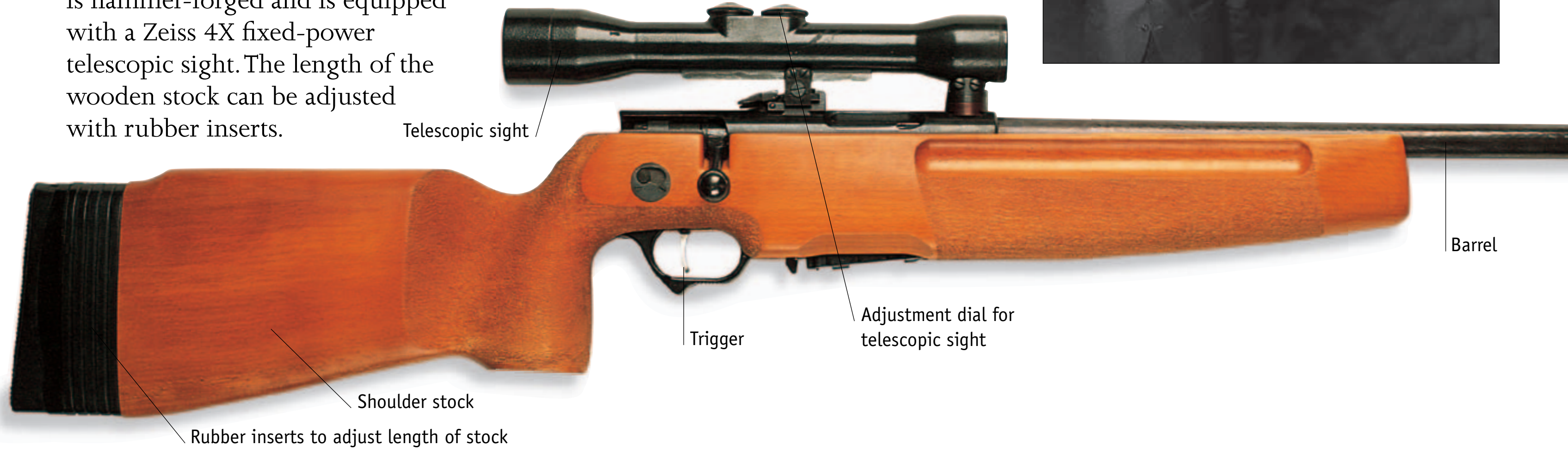


Assassination devices III

SSG-82 sniper rifle

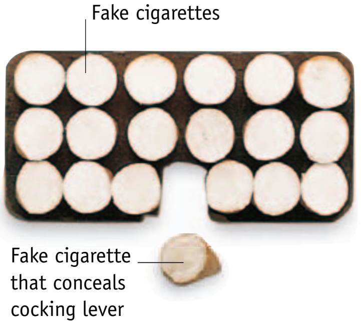
The East German Ministry for Security (MfS) recognized the need for a precision sniper rifle capable of delivering a lethal round with pinpoint accuracy for use by airport antiterror units and other security forces. The rifle is a bolt-action, manual repeater with a five-round detachable box magazine. The barrel is hammer-forged and is equipped with a Zeiss 4X fixed-power telescopic sight. The length of the wooden stock can be adjusted with rubber inserts.

General Erich Mielke
Mielke (1907–2000) headed the East German Ministry for State Security from 1957 to 1989. Here he is showing how the SSG-82 is held and aimed.

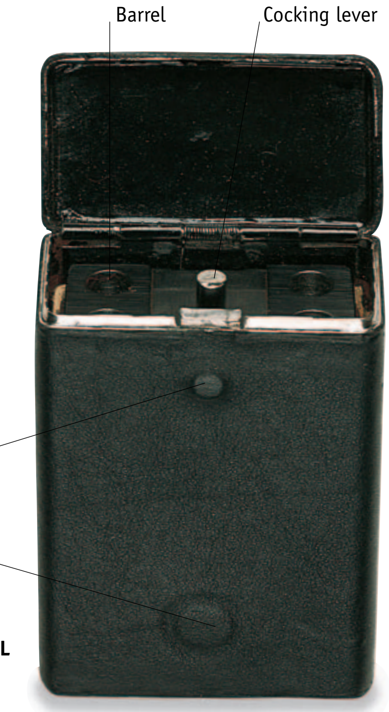

Telescopic sight
Barrel
Trigger
Adjustment dial for telescopic sight
Shoulder stock
Rubber inserts to adjust length of stock

Cigarette-case pistol

In 1954, the KGB's Operational–Technical Department (OTU) issued a cigarette-case pistol to Nikolai Khokhlov, an internal police officer. The pistol, which fired poison-filled bullets through a fake-cigarette insert, was for the assassination of the anti-Soviet émigré Georgi Okolovich. The assassination plan failed because Khokhlov defected to the West (see p. 193).



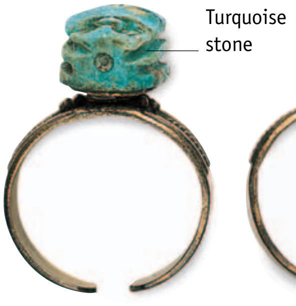
INSERT WITH FAKE CIGARETTES



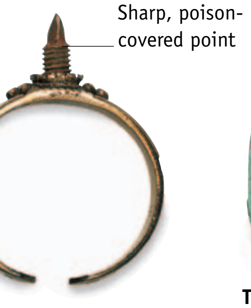
CIGARETTE-CASE PISTOL

Assassination ring

In the 1940s and 1950s, Special Laboratory No. 12 of the KGB's Operational–Technical Department (OTU) employed chemists, doctors, and technologists to make a variety of poisons and assassination devices. The turquoise stone of this assassination ring unscrewed to reveal a sharp point covered with poison.

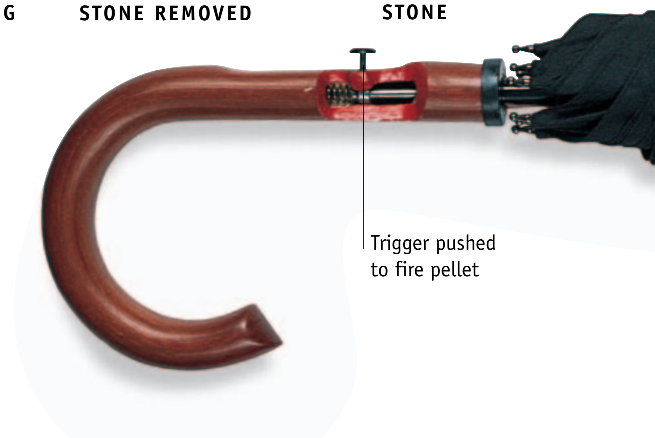


ASSEMBLED RING



STONE REMOVED

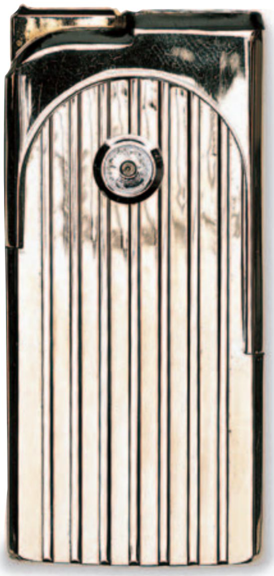
TURQUOISE STONE



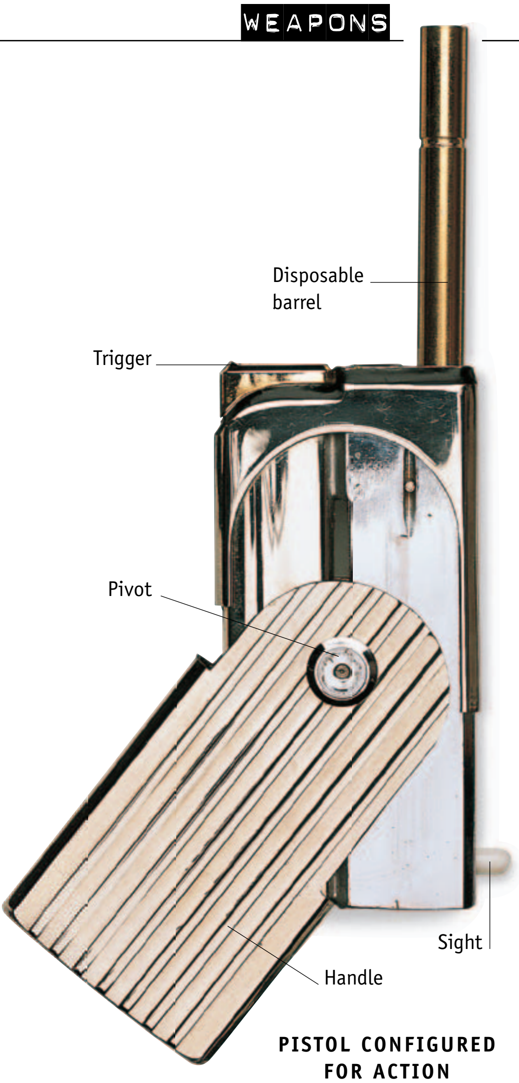
US intelligence cigarette-lighter pistol

This European-style lighter appears functional and unmodified and could be carried without suspicion in a pocket or purse. However, it converts into an electrically fired pistol with a disposable barrel, which slots into the top of the lighter. The action of pulling back and rotating the rear of the lighter to form the handle automatically raises the rear sight into position. When the trigger is pressed, an internal electric magneto sends an impulse that fires the pistol.

BARREL



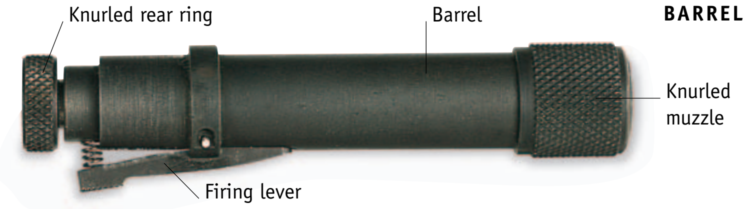
PISTOL CAMOUFLAGED AS LIGHTER



PISTOL CONFIGURED FOR ACTION

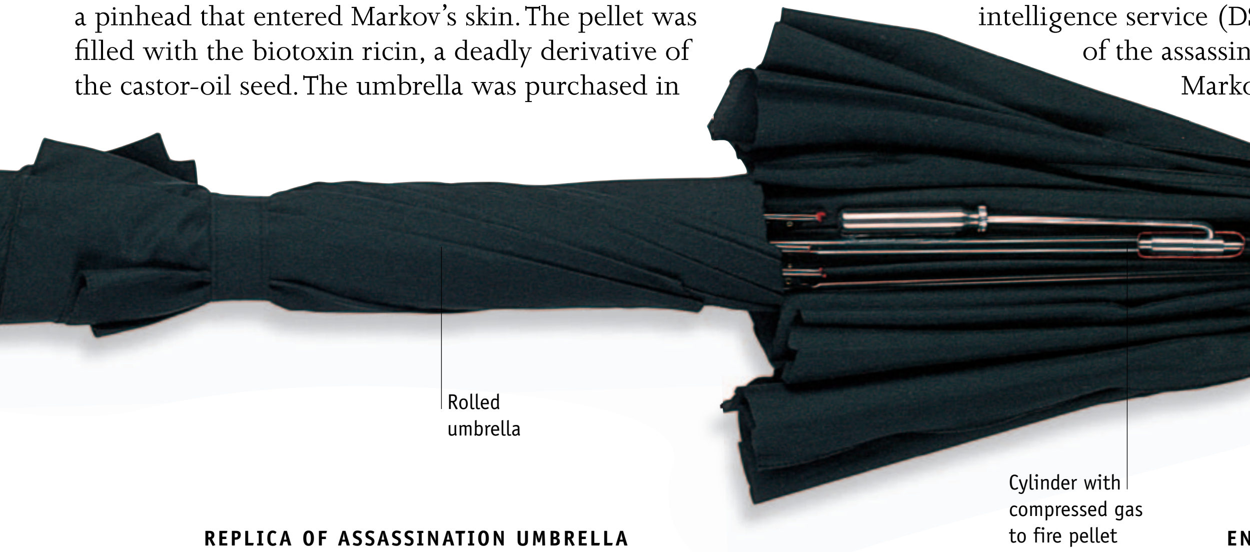
.22-Caliber firing device

Slighter longer than a cigarette, this US firing device is easy to conceal in a purse or pocket. It is cocked by pulling on the knurled ring at the rear and fired by depressing the raised firing lever.

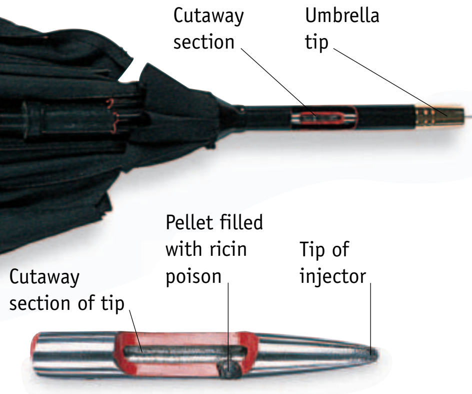


Assassination umbrella

On September 7, 1978, dissident Georgi Markov (see p. 192), an outspoken critic of the regime of Todor Zhivkov in Bulgaria, was assassinated in London. His attacker used an umbrella that had been converted into a pneumatic weapon. When the tip was jabbed into Markov's thigh, it fired a pellet the size of a pinhead that entered Markov's skin. The pellet was filled with the biotoxin ricin, a deadly derivative of the castor-oil seed. The umbrella was purchased in Washington, D.C., by the KGB but modified in Moscow at Laboratory No. 12 of the Central Scientific Investigation Institute for Special Technology (TsNIIST). Throughout the Cold War, the KGB orchestrated assassinations globally as a way of stifling outspoken dissidents. The files of the Bulgarian intelligence service (DS) have revealed the codename of the assassin as Piccadilly and that of Markov as Traveler.



REPLICA OF ASSASSINATION UMBRELLA



ENLARGED MODEL OF UMBRELLA TIP

Modern assassinations

HIGHLY TECHNICAL means of assassination are devised by certain intelligence services all the time. Alleged cases in recent years include the remote detonation of an explosive device concealed in a Palestinian terrorist's cell phone, and slipping a deadly radioactive substance into a Russian troublemaker's afternoon tea. Sometimes the crudest methods of assassination are still the most effective, however, as may have been the case with the Egyptian spy who mysteriously "fell" to his death from the fourth-floor balcony of his London apartment in 2007. High-tech or low-tech, modern assassinations require extremely careful planning and timing.

ATTEMPTED POISONING?

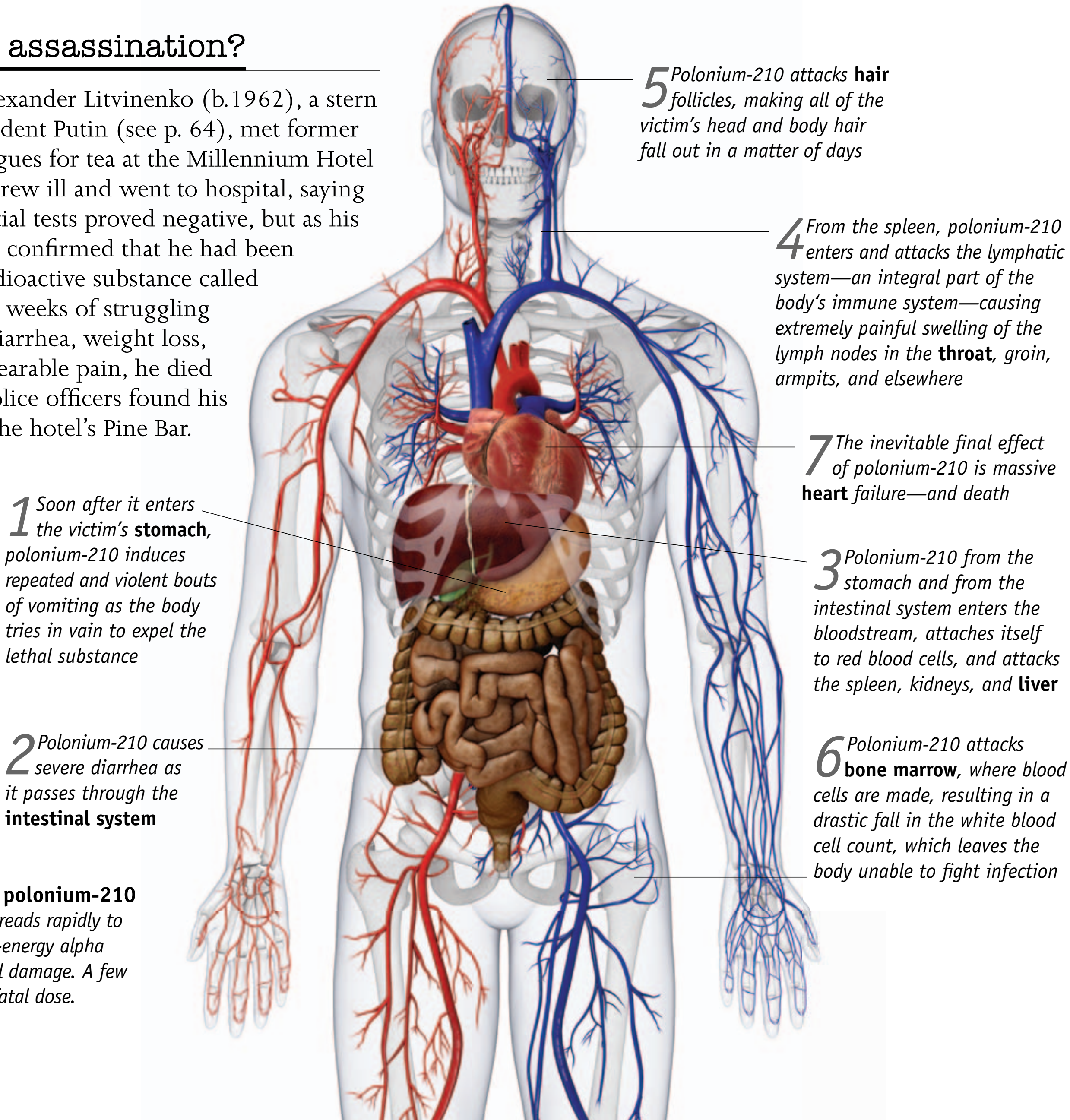
On September 5, 2004, Ukrainian opposition leader Viktor Yushchenko (b.1954) dined with the chairman of the Ukrainian Security Service (SBU) and his deputy. Yushchenko had soup. The next day he began feeling unwell, and five days later he entered an Austrian clinic with severe stomach pains, and blisters all over his face. A toxicologist found 6,000 times the normal level of dioxin in his blood. Though scarred for life (right), he lived, and in 2005 was elected Ukraine's president.

VIKTOR YUSHCHENKO

The first nuclear assassination?

On November 1, 2006, Alexander Litvinenko (b.1962), a stern critic of then Russian President Putin (see p. 64), met former Russian intelligence colleagues for tea at the Millennium Hotel in London. That night he grew ill and went to hospital, saying he had been poisoned. Initial tests proved negative, but as his condition worsened it was confirmed that he had been poisoned with a deadly radioactive substance called polonium-210. After three weeks of struggling with hair loss, vomiting, diarrhea, weight loss, kidney problems, and unbearable pain, he died on November 23. Later, police officers found his still-radioactive teacup at the hotel's Pine Bar.

ALEXANDER LITVINENKO

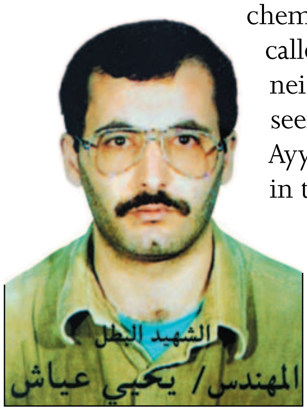


1 Soon after it enters the victim's **stomach**, polonium-210 induces repeated and violent bouts of vomiting as the body tries in vain to expel the lethal substance
2 Polonium-210 causes severe diarrhea as it passes through the **intestinal system**
3 Polonium-210 from the stomach and from the intestinal system enters the bloodstream, attaches itself to red blood cells, and attacks the spleen, kidneys, and **liver**
4 From the spleen, polonium-210 enters and attacks the lymphatic system—an integral part of the body's immune system—causing extremely painful swelling of the lymph nodes in the **throat**, groin, armpits, and elsewhere
5 Polonium-210 attacks **hair** follicles, making all of the victim's head and body hair fall out in a matter of days
6 Polonium-210 attacks **bone marrow**, where blood cells are made, resulting in a drastic fall in the white blood cell count, which leaves the body unable to fight infection
7 The inevitable final effect of polonium-210 is massive **heart** failure—and death

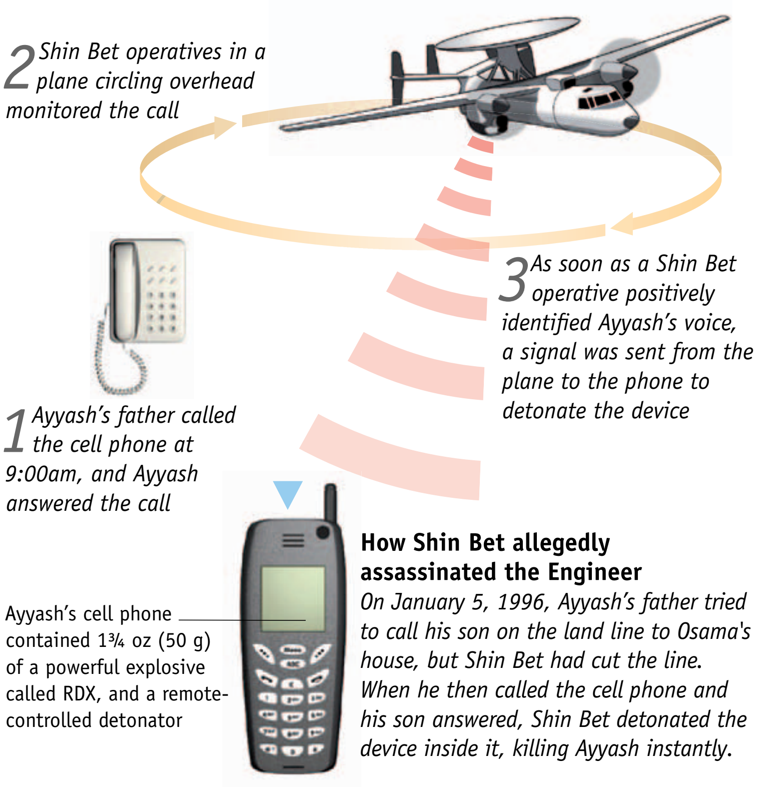
The fatal effects of ingesting polonium-210
When swallowed, polonium-210 spreads rapidly to all parts of the body, emitting low-energy alpha particles that cause irreversible cell damage. A few micrograms of the substance is a fatal dose.

The high-tech death of the Engineer

Yahya Ayyash (b.1966) of the Palestinian group Hamas was the terrorist "most wanted" by Shin Bet, the Israeli security service. Known as the Engineer, he designed suicide bombs that killed nearly 100 Israelis. His speciality was using common household chemicals to make a powerful explosive called "Mother of Satan." The Israelis have neither confirmed nor denied it, but it seems that in 1995 they learned that Ayyash sometimes stayed in Beit Lahiya in the Gaza Strip with a friend, Osama Hamad, whose uncle, Kamil, had previously cooperated with them. They told Kamil they would expose him if he did not pass a rigged cell phone to Osama to give to Ayyash. Hidden inside the cell phone was a remote-controlled explosive device.



YAHYA AYYASH


2 Shin Bet operatives in a plane circling overhead monitored the call
3 As soon as a Shin Bet operative positively identified Ayyash's voice, a signal was sent from the plane to the phone to detonate the device
1 Ayyash's father called the cell phone at 9:00am, and Ayyash answered the call
Ayyash's cell phone contained 1¾ oz (50 g) of a powerful explosive called RDX, and a remote-controlled detonator

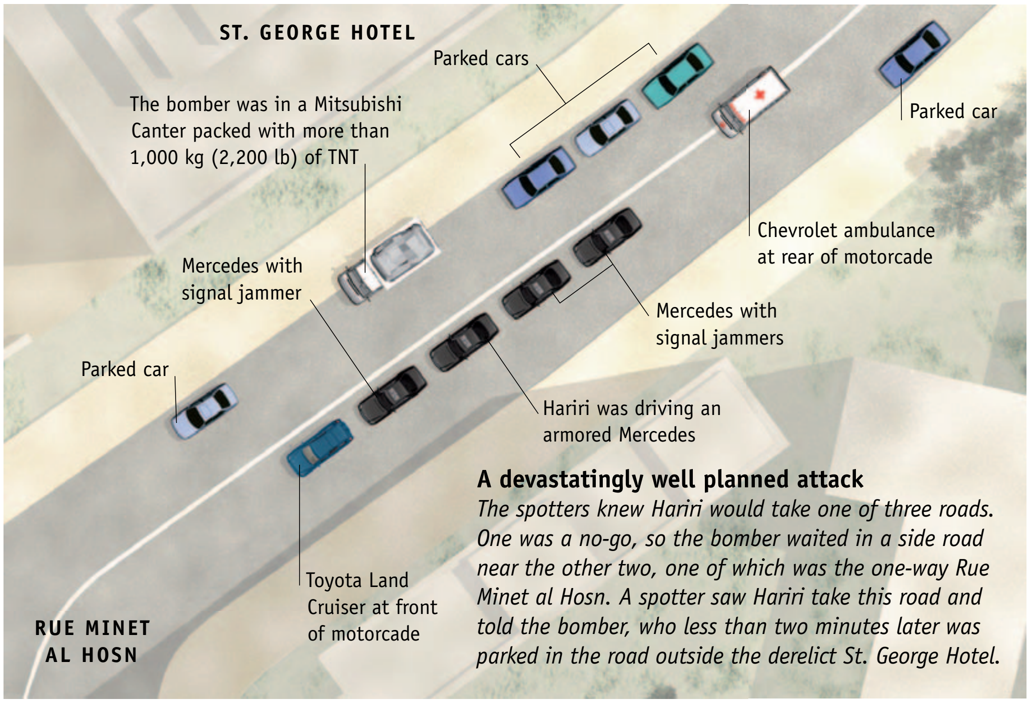
How Shin Bet allegedly assassinated the Engineer

On January 5, 1996, Ayyash's father tried to call his son on the land line to Osama's house, but Shin Bet had cut the line. When he then called the cell phone and his son answered, Shin Bet detonated the device inside it, killing Ayyash instantly.

Brute force and deadly timing

On February 14, 2005, former Lebanese Prime Minister Rafik Hariri (b.1944)—a thorn in the sides of both the Lebanese and the Syrian authorities—drove home through Beirut in an armored car between other cars fitted with devices to jam any signal sent remotely to set off a roadside bomb. A suicide bomber detonated a TNT-packed truck as Hariri drove past. The huge blast killed 21 people, including Hariri, and injured 225. The United Nations Security Council concluded that the Syrian and Lebanese security services most likely jointly approved the attack, and that spotters with cell phones directed the bomber.

RAFIK HARIRI


ST. GEORGE HOTEL
Parked cars
The bomber was in a Mitsubishi Canter packed with more than 1,000 kg (2,200 lb) of TNT
Parked car
Chevrolet ambulance at rear of motorcade
Mercedes with signal jammer
Mercedes with signal jammers
Parked car
Hariri was driving an armored Mercedes
Toyota Land Cruiser at front of motorcade
RUE MINET AL HOSN

A devastatingly well planned attack

The spotters knew Hariri would take one of three roads. One was a no-go, so the bomber waited in a side road near the other two, one of which was the one-way Rue Minet al Hosn. A spotter saw Hariri take this road and told the bomber, who less than two minutes later was parked in the road outside the derelict St. George Hotel.

A LOW-TECH ASSASSINATION?

On June 27, 2007, Egyptian billionaire Ashraf Marwan (b.1944) plunged to his death from the fourth-floor balcony of his apartment in London. Bystanders reported seeing two "Mediterranean" men in suits leaning over the balcony as he fell. The son-in-law of former Egyptian president Abdel Nasser, Marwan supplied Israel with Egyptian political and military secrets in the 1970s after volunteering to spy for Israel in 1969. Egyptian revenge is suspected as a motive for his death.

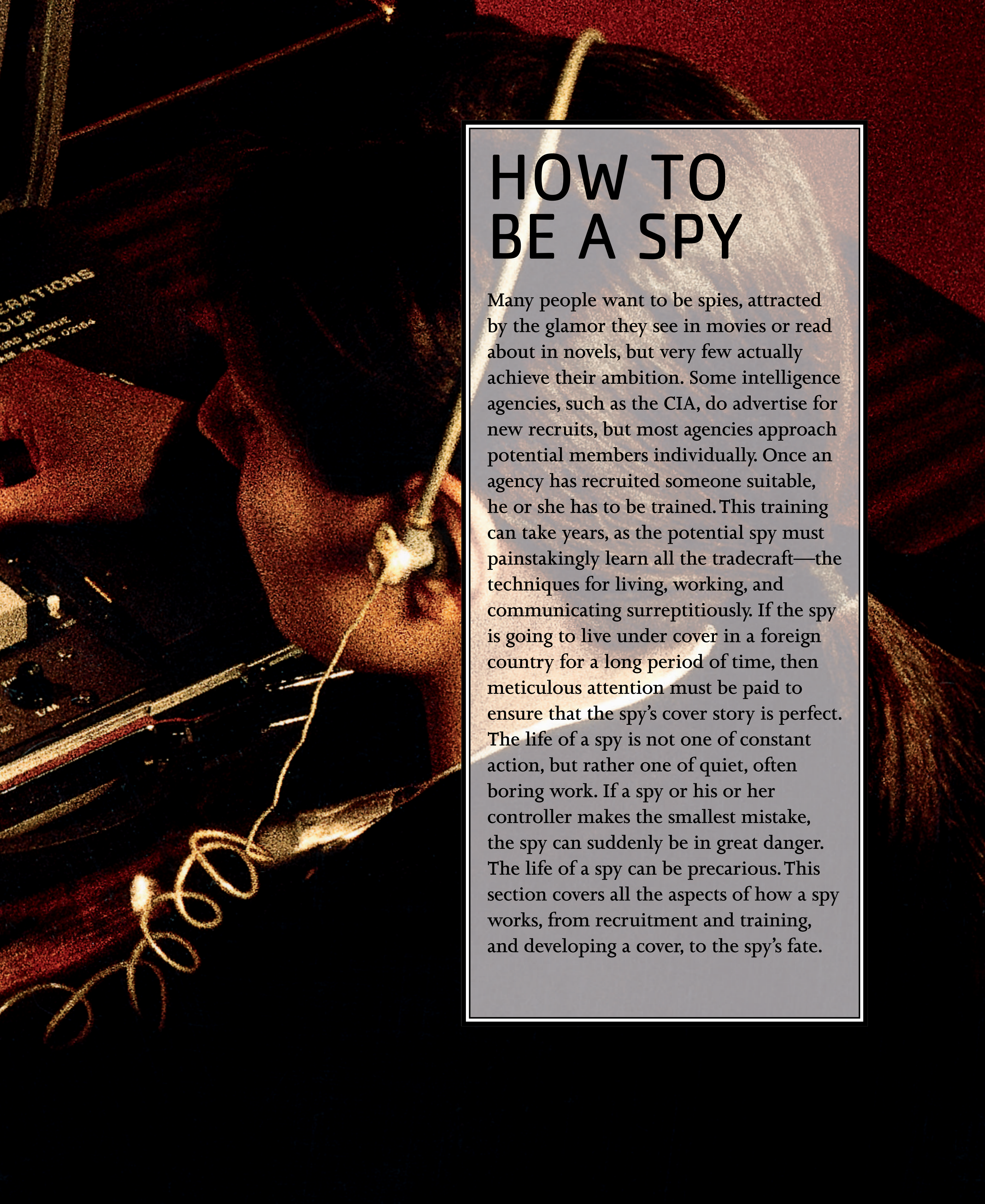
The funeral of Ashraf Marwan

Top Egyptian officials attended the funeral of Ashraf Marwan in the country's capital, Cairo.

SPECIAL OP
GRO
165 T
WALTH

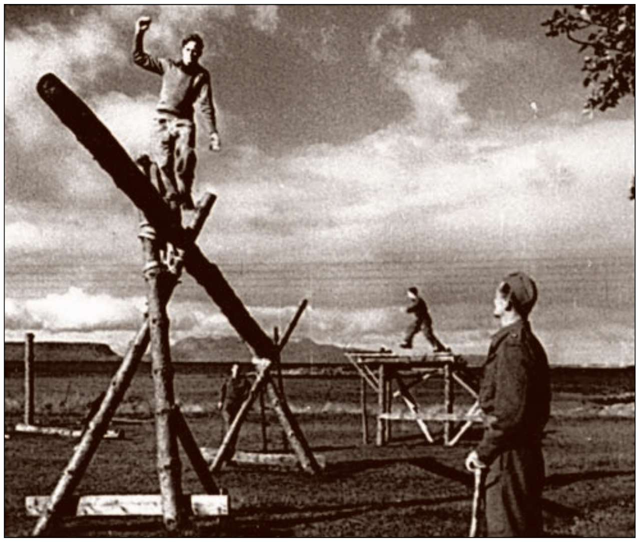
HOW TO BE A SPY

Many people want to be spies, attracted by the glamor they see in movies or read about in novels, but very few actually achieve their ambition. Some intelligence agencies, such as the CIA, do advertise for new recruits, but most agencies approach potential members individually. Once an agency has recruited someone suitable, he or she has to be trained. This training can take years, as the potential spy must painstakingly learn all the tradecraft—the techniques for living, working, and communicating surreptitiously. If the spy is going to live under cover in a foreign country for a long period of time, then meticulous attention must be paid to ensure that the spy's cover story is perfect. The life of a spy is not one of constant action, but rather one of quiet, often boring work. If a spy or his or her controller makes the smallest mistake, the spy can suddenly be in great danger. The life of a spy can be precarious. This section covers all the aspects of how a spy works, from recruitment and training, and developing a cover, to the spy's fate.



Training and recruitment I

SPIES ARE RECRUITED by different means according to the skills or abilities required. Personnel needed by the technical support branch of an intelligence service, for example, can often be recruited simply by advertising for people with the required expertise. If scientific knowledge is required, in computing or nuclear physics, for instance, it may be possible to recruit directly from universities. Linguists can also be acquired in this way. Thousands of specialists are employed by the big intelligence agencies, though few of the recruits will play active roles in intelligence-gathering overseas.



Physical training
Intelligence officers, particularly those expected to engage in clandestine warfare like these wartime SOE agents, undergo rigorous physical training.

Fairbairn-Sykes training knives
Fotr training agents in World War II, these knives (see p. 187) had ball tips for safety (right). Now it is more urgent for agents to acquire computer skills.

Intelligence-gathering is the preserve of career intelligence officers, known as case officers, and agents recruited by them. When working abroad, case officers are usually attached to the staff of embassies. They operate there under the guise of diplomatic personnel, often making stringent efforts to disguise their role in intelligence work. Their primary task is the recruitment and control of agents, through whom intelligence can be gathered. When seeking potential recruits, case officers usually target the personnel of foreign intelligence services and foreign embassy employees. Intelligence officers are of obvious value if they can be recruited as moles, but anyone who has access to information can prove useful. Chauffeurs, secretaries, or maintenance staff can all provide information that may lead to the recruitment of more agents. For instance, they are likely to know which of their colleagues have personal problems, such as financial difficulties or alcoholism, and which may be having extramarital affairs. Such gossip can help intelligence officers identify the people who are vulnerable, and who might therefore be successfully recruited.

Friendly spies

Case officers who are responsible for recruiting agents need to have friendly, likeable personalities. They must be affable and socially adaptable, and appear open to other people's points of view. Soviet case officers with these qualities were known to spend much time in clubs and bars around Washington, DC,

ALDRICH AMES

SPY PROFILE

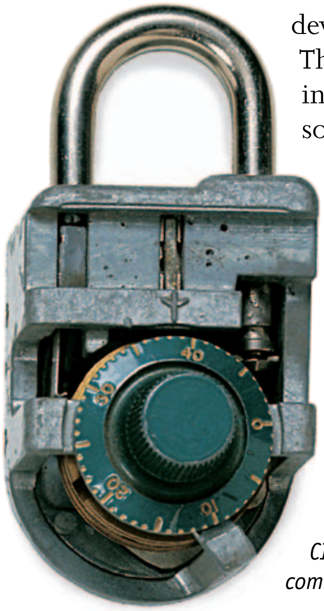
Finding himself in debt, CIA officer Ames (b.1941) offered his services to the KGB in 1985. He became the Counterintelligence Branch Chief in the Soviet Division of the Directorate of Operations and betrayed every secret that came his way, leading to the deaths of at least 10 CIA agents. For the information that Ames gave them, the KGB paid a total of $2.7 million. Ames was arrested in 1994 and was convicted and sentenced to life imprisonment.

GEORGE BLAKE

SPY PROFILE

Communist Party member George Blake (b.1922) was a British citizen recruited by MI6 (see p. 217) because of his linguistic skills. Sent to Korea as Head of Station during the Korean War (1950–53), he was taken prisoner by the North Koreans. On his return to England in 1953, he started to pass secrets to the KGB, badly affecting British intelligence. In 1961 Blake was arrested and jailed for 42 years. After six years, he escaped to the Soviet Union.

hoping to fall into the company of US government staff, military personnel, or business people. The case officer will typically form a friendship with a likely recruit. This friendship is often based on a supposedly shared interest; for example women, drinking, gambling, or even an innocent hobby such as fishing or stamp collecting. As the friendship develops, the case officer will subtly probe for any character weaknesses that can be used to control the new friend. At this point, the potential recruit is referred to as a developing agent. The first information sought from them may seem totally innocuous. But slowly, new recruits will be drawn closer into a web of deceit and espionage. Some will be persuaded to agree to clandestine activities in return for cash, and later made to sign a receipt for money received. Once they have gone this far, there is little chance that they will turn back. They will have become recruited agents. The threat of having their new activities revealed, coupled with the lure of money, will be enough to ensure their continued loyalty to their handler.



Training padlock
This special padlock was used for teaching CIA recruits to open combination locks.

Handlers, who may not be the same case officers who recruited the agent, will attempt to reinforce this loyalty by building strong bonds of friendship and trust with their agents. Even after his arrest, CIA traitor Aldrich Ames was able to talk of the great affection he still held for his former handlers.

Types of agent

Apart from those recruited specifically to procure intelligence, several other types of agent exist. Contact agents and access agents are used to identify and facilitate access to potential recruits. Agents of influence are used to affect public opinion or events. Support agents assist other agents by acting as couriers or maintaining safe houses, for example.

Double agents are those who work against their original intelligence services while under the control of another service. They may be driven by motives of money, ideology, compromise, or ego, or they may be trying to save their lives or to regain their freedom after capture by their original enemy.

Moles are intelligence personnel who are in the employment of one service while being controlled by another.

Sleeper agents are those who are sent into foreign countries to live apparently normal lives until activated, perhaps in time of national emergency or pending war, when their mission is likely to be one of sabotage or assassination.

"Illegals" (see p. 217) are spies who adopt elaborate false identities to work in foreign countries. They are difficult for the enemy to detect, but run the risk of heavy punishment as they operate without any diplomatic immunity. Apart from gathering information, their role may sometimes also be to spot potential new recruits or run other agents.

Instruction in tradecraft
Tradecraft is the word for the range of technical skills used in espionage. Here, SOE recruits (see p. 30) learn about methods of opening locks.

Training and recruitment II

Once recruited, new employees of an intelligence service may follow any one of a number of different paths. Major intelligence agencies, such as the CIA and the KGB (now partially replaced by the SVR), need large numbers of technical and analytical experts to support their operations. Personnel who have been recruited to take these roles will receive a general introduction to the various elements of intelligence work before being sent on for training in their individual specialties. They may continue to work within these specialized areas throughout their careers. A recruit who is destined for a career as an intelligence officer or case officer will go through a far more intensive and wide-ranging course of training. Many of the elements that have characterized Western intelligence training since 1945 have their origins in the early, wartime training programs that were devised for the British SOE (see p. 30) and the American OSS (see p. 32).

Communications training
The use of Morse code for radio communication can be one of the most intensive and time-consuming elements of intelligence training.

JOHN VASSALL

SPY PROFILE

Admiralty clerk John Vassall (1924–96) was working at the British Embassy in Moscow when he was recruited by the KGB, who used evidence of his homosexuality as blackmail. He was trained to use a Minox camera and started work for the KGB. He continued to spy on his return to London in 1956. After passing many naval secrets to Moscow, Vassall was arrested in 1962 and convicted of spying. He served 10 years of an 18-year sentence.

Wartime recruitment and training

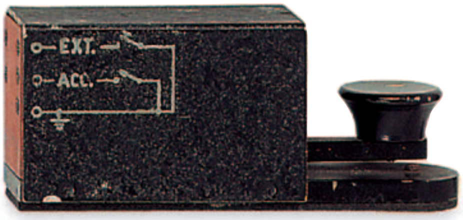
Originally, the SOE discovered many of its trainees through word-of-mouth recommendations and similar informal contacts. Individuals who had excellent foreign language skills, who were also willing to volunteer for unspecified service, were in demand. Besides this, the SOE received some of its recruits via the War Office Department MI1x, which also provided recruits for MI5 (see p. 208) and MI6. These agencies carried out their own direct recruiting, sometimes in competition with the SOE. The SOE preferred to recruit people from a middle-class background, who had no affiliations to extreme political groups. Less respectable individuals, such as forgers and burglars, were hired for their specialized skills.

The OSS also began by informal recruitment of personnel. By late 1943, however, its growing manpower needs led to a more systematic approach. The OSS joined with the SOE to set up a system of psychological assessment for sifting recruits; this system was combined with training programs designed in such a way that unsuitable trainees could be filtered out at various stages. In both organizations trainees would undergo a period of basic training. Subjects included fieldcraft (survival skills), communications, sabotage, and the various forms of combat. After that, more advanced courses followed to prepare agents for specialized tasks or work in specific countries.

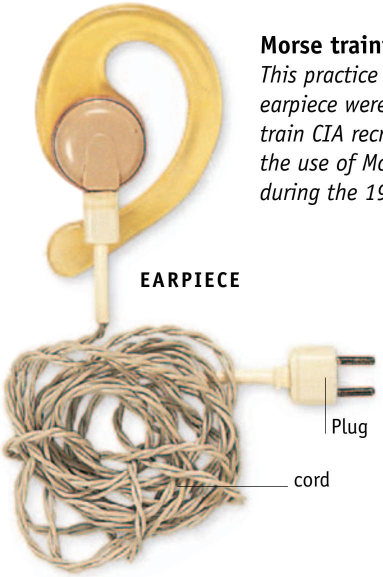
HUGH HAMBLETON

SPY PROFILE

Hugh Hambleton (b.1922) was recruited in 1947 by the MGB (later KGB), lured by their intellectual flattery and his craving for adventure. From 1956 to 1961 he worked for Nato and supplied secrets to Moscow. He returned to Canada, became a professor, and continued to pass secrets. The RCMP security service (see p. 176) discovered his espionage equipment in 1979. He was later sentenced to 10 years in prison in Britain.



TRAINING KEY



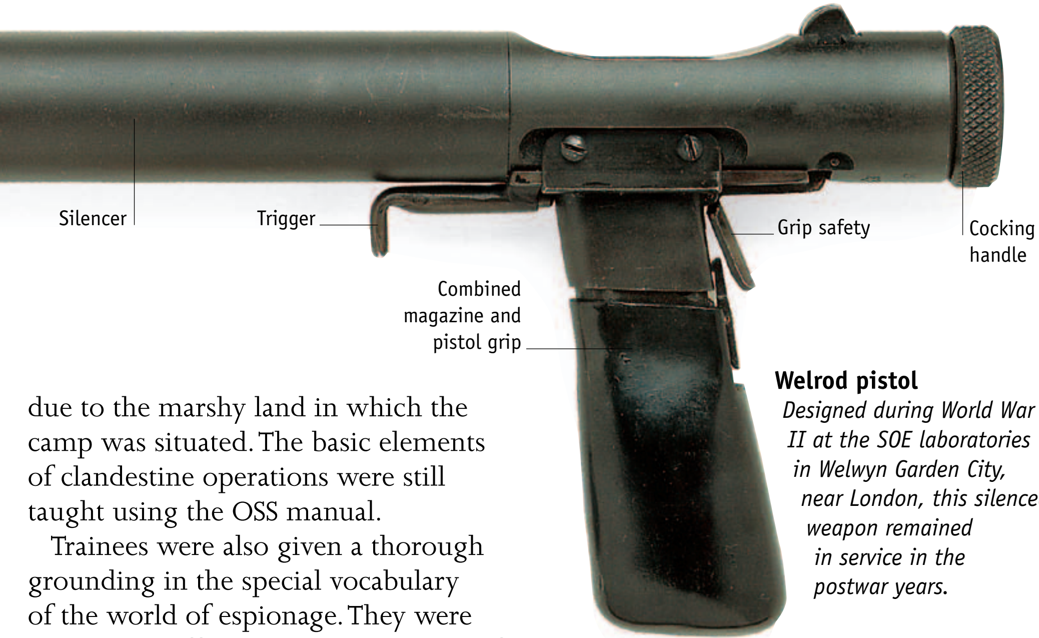
Morse training key
This practice key and earpiece were used to train CIA recruits in the use of Morse code during the 1960s.

Firearms training
Intelligence services may train their officers to use a variety of firearms, choosing weapons that will best meet the anticipated operational needs.

CIA training

The system of training instituted by the OSS had a strong influence over the methods adopted by the CIA. During the 1950s, trainee CIA officers received basic training at a camp codenamed Isolation. This former naval base in Virginia was also known to recruits as Camp Swampy, due to the marshy land in which the camp was situated. The basic elements of clandestine operations were still taught using the OSS manual.

Trainees were also given a thorough grounding in the special vocabulary of the world of espionage. They were taught the differences between types of agents, and learned the skills required to recruit them. Their role as case officers was expressed as providing the "link between the intelligence bureaucracy that wants the secret information and the agents that have access to the information." Technical experts lectured the students on espionage tradecraft, such as clandestine photography, secret writing, surveillance, and dead drops.



Welrod pistol
Designed during World War II at the SOE laboratories in Welwyn Garden City, near London, this silenced weapon remained in service in the postwar years.

In the later stages of their training, the trainees would be taken to the nearby city of Norfolk, to practice their newly acquired skills.

Soviet training

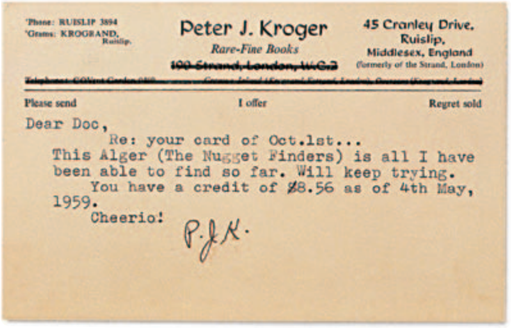
Soviet recruits to the KGB and GRU (see p. 38) were taught much the same basic skills. The KGB's main training center was School 101 (later renamed the Red Banner Institute) near Moscow. The GRU trained its personnel at the Military Diplomatic Academy.

KGB training was based on a textbook entitled *The Foundation of Soviet Intelligence Work*, which covered the tradecraft and case-officer skills required of an intelligence officer. KGB and GRU recruits were not taught to gather intelligence but to persuade others to do this for them by betraying their countries. The work of recruiting and running agents was studied from actual cases, with the aid of experienced instructors with firsthand knowledge. The final stage of training was to learn a foreign language, and this was selected to best meet the current operational requirements of the service.

Operational training
SOE recruits learned the importance of terrain in planning an operation. Here, an instructor shows a group how to use a topographical model.

Covers and legends

IN ESPIONAGE, A COVER is a form of deception designed to conceal a spy's true identity. For simple operations, a cover need not be elaborate—perhaps just a false name. A legend is a sophisticated cover that amounts to an entire artificial background and life history. Legends are created for spies living secretly in a foreign country for as long as a few years without the benefit of diplomatic immunity—in KGB terms, an "illegal" (see p. 217). The equivalent CIA term is NOC (nonofficial cover). A legend has to stand up to scrutiny by counterintelligence. The time and care spent creating a cover or legend are determined by three factors: the importance of the mission, the length of time the identity has to be maintained, and the degree of scrutiny it must endure.



'Phone: RUISLIP 3894
'Grams: KROGRAND, Ruislip.

Peter J. Kroger
Rare-Fine Books
~~190 Strand, London, W.C.2~~

45 Cranley Drive,
Ruislip,
Middlesex, England
(formerly of the Strand, London)

~~[illegible]~~

Please send I offer Regret sold

```
Dear Doc,
        Re: your card of Oct.1st...
   This Alger (The Nugget Finders) is all I have
   been able to find so far. Will keep trying.
       You have a credit of $8.56 as of 4th May,
   1959.
       Cheerio!
```

P.J.K.

LEGEND-BUILDING POSTCARD WITH "HOUSE OF SPIES" ADDRESS (SEE P. 50)

Cover or legend?

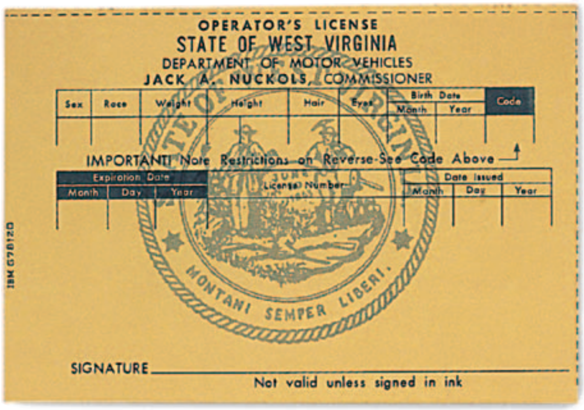
A short-term false identity, for which little preparation is needed, is called a cover. For example, a member of MI6 visiting an electronics trade show in a British town need only sign in under a false name, carry cards relating to a nonexistent business, and set up a telephone line answered in that company's name.

But an illegal needs greater preparation. Elie Cohen (see p. 136) took a year establishing his legend in Argentina before he began his mission, spying for Israel in Syria.

False identities

Spy agencies maintain stockpiles of paper samples from around the world to be able to duplicate most identification documents exactly. Such work must be flawless: the identity of a German spy posing as a Soviet citizen during World War II was discovered because stainless steel staples—not available in the Soviet Union—were used on his documents. The absence of rust marks on his papers was enough to expose him.

The credibility of a false identity can be helped by the careful use of "pocket litter," such as ticket stubs or receipts, to lend support to the cover story. It is vital that a spy carries nothing that would reveal his or her true identity. Sometimes spies are able to obtain the documents that allow them to assume the identity of a person who has died. The research involved in basing a legend on the identity of a dead person must be done thoroughly. For example, care must be taken in checking that the spy conforms to the physical details of the deceased person. A small error can be disastrous, as in the case of the KGB illegal Konon Molody (see p. 51).



OPERATOR'S LICENSE
STATE OF WEST VIRGINIA
DEPARTMENT OF MOTOR VEHICLES
JACK A. NUCKOLS, COMMISSIONER

Sex	Race	Weight	Height	Hair	Eyes	Birth Date		Code
						Month	Year	

IMPORTANT! Note Restrictions on Reverse-See Code Above

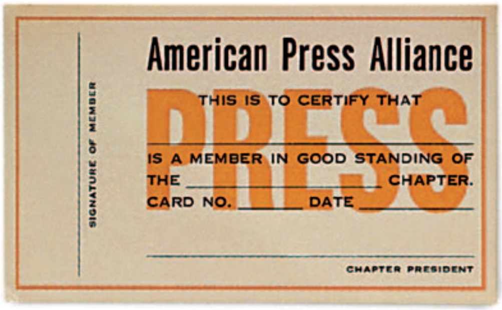
Expiration Date			License Number	Date Issued		
Month	Day	Year		Month	Day	Year

IBM G78120

SIGNATURE ____________
Not valid unless signed in ink

MONTANI SEMPER LIBERI.

SOVIET FORGERY OF A BLANK (UNCOMPLETED) DRIVER'S LICENSE FORM



American Press Alliance

THIS IS TO CERTIFY THAT
PRESS
IS A MEMBER IN GOOD STANDING OF THE ______ CHAPTER.
CARD NO. ______ DATE ______

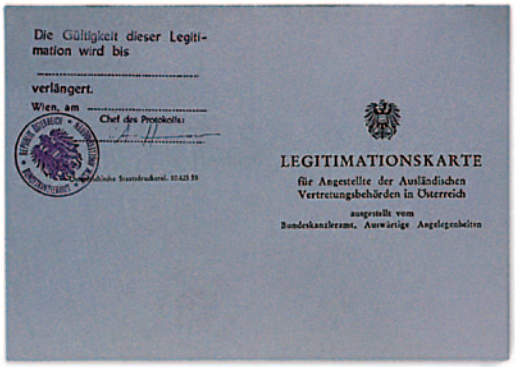
CHAPTER PRESIDENT

SIGNATURE OF MEMBER

SOVIET FORGERY OF A UNITED STATES PRESS CARD

Avoiding discovery

Even if a legend has been constructed perfectly, a spy must behave in the right manner. For an operative working at home or in a friendly country this will not be too demanding, since the legend will not be closely scrutinized. However, a spy using a legend in a hostile country must make every effort to "live" that legend constantly and be very careful not to say anything, even in a casual conversation, that might cast doubt on it. Actions must be in keeping with the character. In World War I, a German officer trying to infiltrate Canada was discovered because he was dressed in shabby clothes but was traveling in the first-class compartment of the train.



Die Gültigkeit dieser Legitimation wird bis
____
verlängert.
Wien, am ____________
Chef des Protokolls:
____

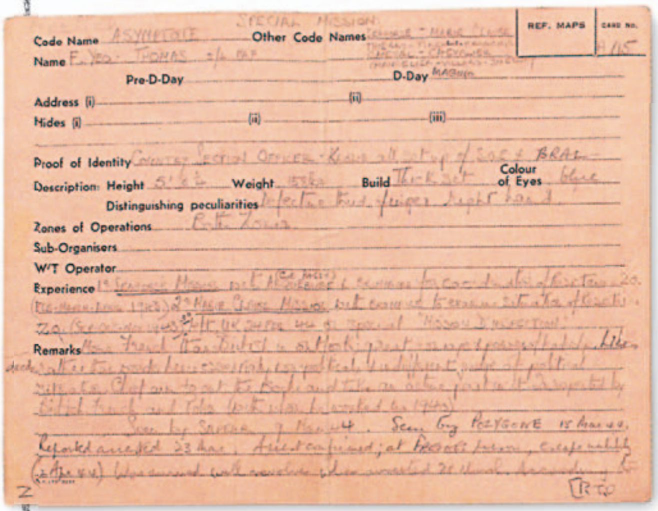
[illegible] Staatsdruckerei. [illegible]

LEGITIMATIONSKARTE
für Angestellte der Ausländischen Vertretungsbehörden in Österreich
ausgestellt vom
Bundeskanzleramt, Auswärtige Angelegenheiten

FORGED STAFF CARD FOR EMPLOYEES OF FOREIGN MISSIONS IN AUSTRIA

FOREST FREDERICK EDWARD YEO-THOMAS

British World War II secret agent Edward Yeo-Thomas (1901–64) was a former Royal Air Force (RAF) officer who volunteered for service with the SOE (see p. 30). He undertook three missions to France, where he worked with the resistance. In 1944, he was captured and tortured by the Gestapo, but he managed to survive captivity until the end of the war. For his bravery Yeo-Thomas was later awarded the George Cross, one of the highest British honors. The items shown below include his SOE file card and RAF identity disks, and an SOE disk knife. The other items relate to legends that were created for his first two missions in France. The identity card in the name of Thierry (born in Arras, northern France) was used on his first mission. The papers in the name of Tirelli (born in Algiers) relate to his second mission in France and include an identity card, ration card, driver's license, and a French Air Force demobilization certificate.



SPECIAL MISSION

		REF. MAPS	CARD No.
Code Name ASYMPTOTE	Other Code Names SEAHORSE - MARIE CLAIRE - THIERRY - TIRELLI - [illegible] - SHELLEY		A 115
Name F. Yeo-Thomas S/L RAF			

Pre-D-Day D-Day MAGNUS

Address (i) (ii)

Hides (i) (ii) (iii)

Proof of Identity Country Section Officer - Knows all set up of SOE & BRA

Description: Height 5'6¾" Weight 155lbs Build Thickset Colour of Eyes blue

Distinguishing peculiarities Defective third finger right hand.

Zones of Operations Both Zones

Sub-Organisers

W/T Operator

Experience 1st Seahorse Mission [illegible] (Feb-March-April 1943) 2nd Marie Claire Mission [illegible] (Sept-Nov 1943) 3rd [illegible] "Mission d'inspection"

Remarks [illegible]

Seen by [illegible] 9 Mar 44. Seen by POLYGONE 15 Mar 44. Reported arrested 23 Mar. Arrest confirmed; at Fresnes prison, [illegible]

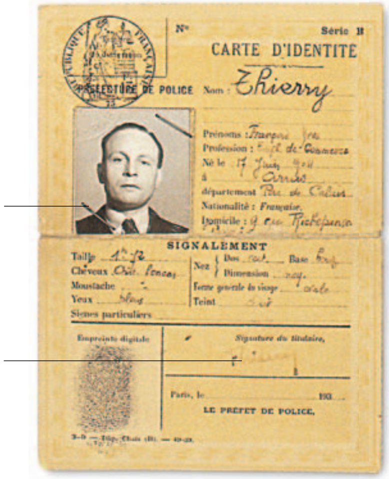
Z

RTO

SOE FILE CARD

RAF IDENTITY DISKS

SOE DISK KNIFE



Photograph of Yeo-Thomas

Signature adopted for assumed identity

Série B

CARTE D'IDENTITE

PRÉFECTURE DE POLICE Nom : Thierry

Prénoms : François Yves

Profession : Empl. de Commerce

Né le 17 Juin 1901

à Arras

département Pas de Calais

Nationalité : Française

Domicile : 9 rue Richepanse

SIGNALEMENT

Taille 1m72 Nez Dos rect. Base hor.

Cheveux Chât. foncés Dimension moy.

Moustache – Forme générale du visage ovale

Yeux bleus Teint clair

Signes particuliers

Empreinte digitale

Signature du titulaire,

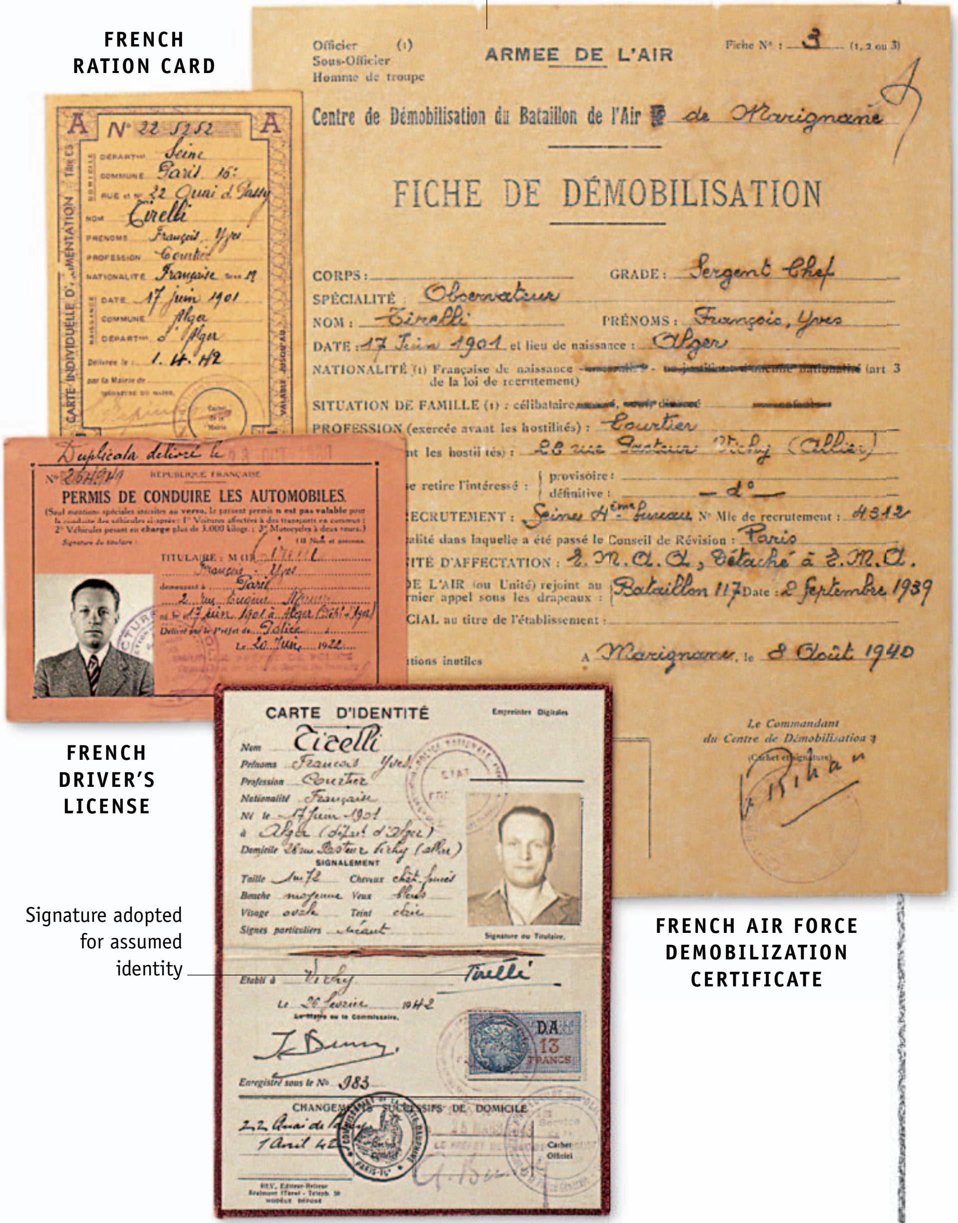
Paris, le 193

LE PREFET DE POLICE,

3-9 — Imp. Chaix (B). — 40-23.

FRENCH IDENTITY CARD

Paper is aged to simulate a certificate that is two years old



FRENCH RATION CARD

A N° 22 5252 A

CARTE INDIVIDUELLE D'ALIMENTATION

DOMICILE DÉPARTt Seine

COMMUNE Paris 16e

RUE et No 22 Quai d'Passy

NOM Tirelli

PRÉNOMS François Yves

PROFESSION Courtier

NATIONALITÉ Française

NAISSANCE DATE 17 juin 1901

COMMUNE Alger

DÉPARTt d'Alger

Délivrée le : 1.4.42

par la Mairie de

SIGNATURE DU MAIRE

Cachet de la Mairie

VALABLE JUSQU'AU

FRENCH DRIVER'S LICENSE

Duplicata délivré le 23 OCT 1930

N° 264.949

RÉPUBLIQUE FRANÇAISE

PERMIS DE CONDUIRE LES AUTOMOBILES.

(Sauf mentions spéciales inscrites au verso, le présent permis n'est pas valable pour la conduite des véhicules ci-après : 1° Voitures affectées à des transports en commun ; 2° Véhicules pesant en charge plus de 3.000 kilog. ; 3° Motocycles à deux roues.)

Signature du titulaire :

TITULAIRE : M (1) Tirelli (1) Nom et prénoms.

François - Yves

demeurant à Paris

2 rue Eugène Manuel

né le 17 juin 1901 à Alger (Dépt d'Alger)

Délivré par le Préfet de Police

Le 20 Juin 1922

PRÉFET DE POLICE

FRENCH AIR FORCE DEMOBILIZATION CERTIFICATE

Officier (1)
Sous-Officier
Homme de troupe

ARMEE DE L'AIR

Fiche N° : 3 (1, 2 ou 3)

Centre de Démobilisation du Bataillon de l'Air de Marignane

FICHE DE DÉMOBILISATION

CORPS : GRADE : Sergent Chef

SPÉCIALITÉ Observateur

NOM : Tirelli PRÉNOMS : François, Yves

DATE : 17 Juin 1901 et lieu de naissance : Alger

NATIONALITÉ (1) Française de naissance ~~[illegible]~~ - ~~[illegible]~~ (art 3 de la loi de recrutement)

SITUATION DE FAMILLE (1) : célibataire ~~marié~~, ~~veuf divorcé~~ ~~[illegible]~~

PROFESSION (exercée avant les hostilités) : Courtier

…nt les hostilités) : 26 rue Pasteur Vichy (Allier)

…e retire l'intéressé : provisoire : définitive : – d° –

…ECRUTEMENT : Seine 4ème bureau N° Mle de recrutement : 4312

…alité dans laquelle a été passé le Conseil de Révision : Paris

…ITÉ D'AFFECTATION : E.M.A.A., Détaché à E.M.A.

…DE L'AIR (ou Unité) rejoint au …rnier appel sous les drapeaux : Bataillon 117 Date : 2 Septembre 1939

…CIAL au titre de l'établissement :

…tions inutiles

A Marignane, le 8 Août 1940

Le Commandant du Centre de Démobilisation
(Cachet et signature)

Signature adopted for assumed identity

CARTE D'IDENTITÉ Empreintes Digitales

Nom Tirelli

Prénoms François Yves

Profession Courtier

Nationalité Française

Né le 17 Juin 1901

à Alger (Départ d'Alger)

Domicile 26 rue Pasteur Vichy (Allier)

SIGNALEMENT

Taille 1m72 Cheveux chât. foncés

Bouche moyenne Yeux bleus

Visage ovale Teint clair

Signes particuliers néant

Signature du Titulaire. Tirelli

Etabli à Vichy

Le 26 Février 1942

Le Maire ou le Commissaire,

Enregistré sous le No 983

DA 13 FRANCS

CHANGEMENTS SUCCESSIFS DE DOMICILE

22 Quai de Passy
1 Avril 42

LE PREFET DE POLICE

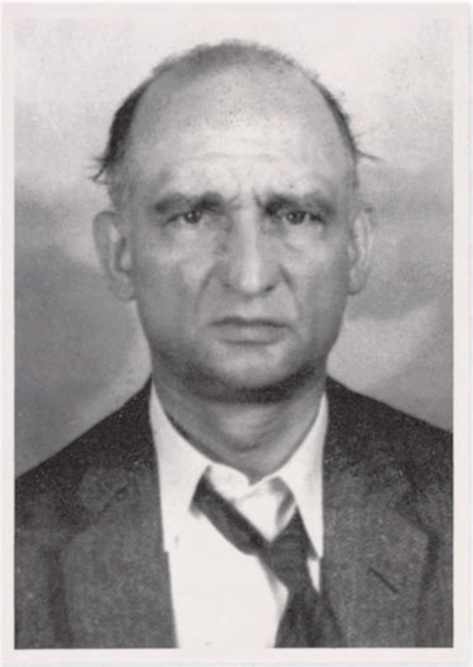
Cachet Officiel

REY, Editeur-Relieur
Réalmont (Tarn) - Teleph. 36
MODÈLE DÉPOSÉ

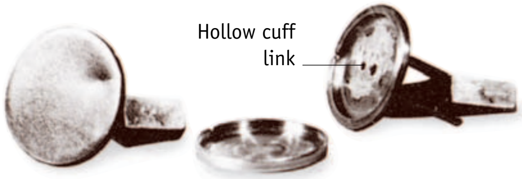
UPDATED FRENCH IDENTITY CARD

Spy networks

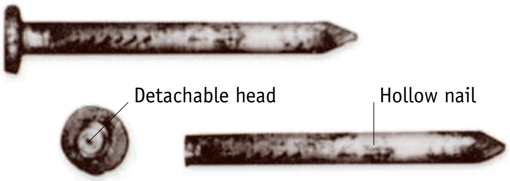
A spy network is a group of agents working under the supervision of a controller. Each person in the network reports to a single superior but may control more than one person. Consequently, networks have a pyramidal structure, with many agents at the bottom and only a few controllers at the top. An example of a controller might be a CIA case officer, working under diplomatic cover, or a Soviet "chief illegal" (a senior "illegal" officer, see p. 217) under an assumed identity.



RUDOLF IVANOVICH ABEL (1903–71)



Abel's cuff links
Microdots could be concealed in a cavity within these cuff links, which were found in the possession of Rudolf Abel.



Hollow nail
The Abel spy network used this specially constructed nail as a dead drop in which microfilm could be hidden.

Controllers need to know as much as possible about their agents to be able to handle them effectively. For the sake of security, agents are told as little as possible about their controllers and nothing about fellow agents. This principle, called compartmentalization, ensures that an arrested agent cannot betray those above him or those in other branches of the network. Without compartmentalization, the entire network may be put at risk.

Sometimes, for reasons of operational expediency, controllers of spy networks have chosen not to apply the principle of compartmentalization. This was the case in the Cambridge network in Britain (see opposite) and in some of the American networks of World War II.

The Abel spy ring

The spy ring operated by the Soviet illegal Colonel Rudolf Ivanovich Abel was put at great risk by its lack of compartmentalization. Working from his apartment in New York, Abel kept in contact with Soviet agents who were involved in trying to steal American atomic secrets. In 1954 another illegal, Reino Hayhanen, became Abel's assistant. He proved unreliable, and Abel had him recalled to Moscow. While in transit, Hayhanen defected. He gave details of Abel's cipher to the FBI and, having been to Abel's apartment, was able to help the FBI to locate Abel himself. Abel was arrested but was later traded in a spy swap for Francis Gary Powers (see p. 52).

Abel's network had contacts with Julius Rosenberg and his wife Ethel, Soviet agents both executed for treason in 1953. Damage to the rest of the network after their arrest, however, was limited by their refusal to give up names.

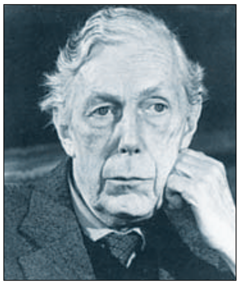
MI5 – THE BRITISH SECURITY SERVICE

Despite the letters MI in the names of MI5 and MI6 (see p. 217), neither body is now a component of military intelligence. MI5 is responsible for counterintelligence and counterespionage and monitors activities of subversive and terrorist groups and foreign nationals in Britain. In World War II, MI5 had great success detecting German spies. From 1992–96, Stella Rimington (b.1935) was head of M15, the first woman to head an intelligence agency in a major country.

JULIUS ROSENBERG

ETHEL ROSENBERG

GUY BURGESS



ANTHONY BLUNT

DONALD MACLEAN

HAROLD (KIM) PHILBY

The Cambridge spies

The KGB recruited a number of agents in Britain in the 1930s, including five who had all been pro-communist students at Cambridge University. They were later controlled by NKVD (later KGB) officer Yuri Modin (b.1922).

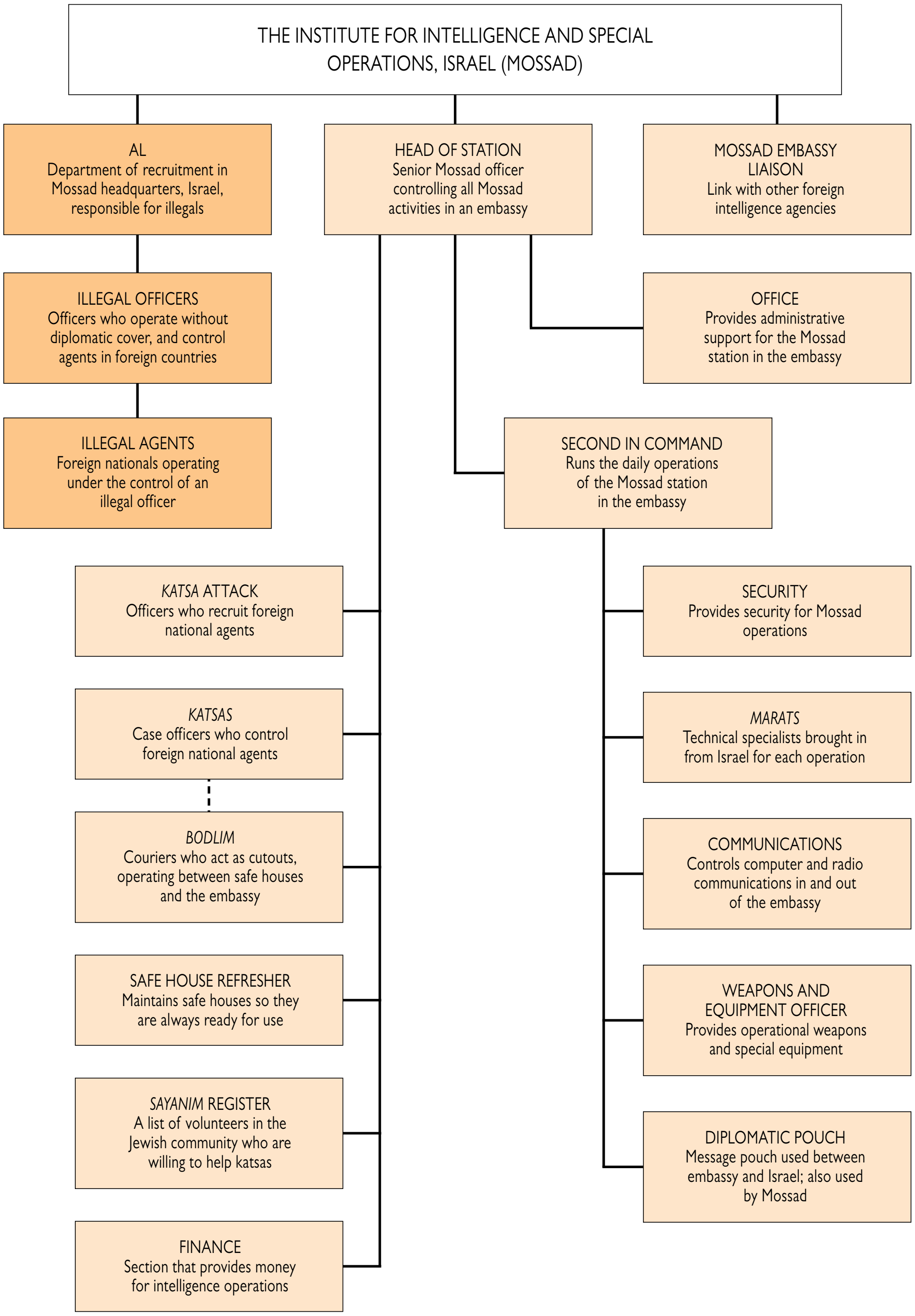
Two of these agents—Foreign Office officials Donald Maclean and Guy Burgess—defected to the Soviet Union in 1951, as they were under suspicion. Their friend Harold (Kim) Philby was forced to resign from a high-ranking post with MI6 as a result. Philby worked in journalism until, in 1963, he also defected. Once regarded as a possible future chief of MI6, he had betrayed many operations to the KGB.

The fourth man in the network was Sir Anthony Blunt, who was an officer in MI5 from 1940 to 1945. He later functioned as a spy while serving as Surveyor of the Queen's Pictures. His guilt had been known to MI5 before it was publicly revealed in 1979.

The last of the five to be publicly named was John Cairncross. He had a career that included positions in MI6, a wartime signals intelligence agency known as GC & CS (later GCHQ), and other government ministries.

MOSSAD SPY NETWORK

Mossad networks operate under the cover of Israel's embassies in other countries. Illegals are controlled directly from Israel, working without diplomatic cover or support from embassy staff. In each country there is a Head of Station who works under diplomatic protection inside the embassy, and when necessary can direct even the ambassador to support Mossad activities. The *sayanim* register is a list of volunteers in the Jewish community available to help when required—this helps keep Mossad manning levels low. Each station imports technical specialists when they are needed, rather than keep them as full-time members of the station.


THE INSTITUTE FOR INTELLIGENCE AND SPECIAL OPERATIONS, ISRAEL (MOSSAD)
AL
Department of recruitment in Mossad headquarters, Israel, responsible for illegals
HEAD OF STATION
Senior Mossad officer controlling all Mossad activities in an embassy
MOSSAD EMBASSY LIAISON
Link with other foreign intelligence agencies
ILLEGAL OFFICERS
Officers who operate without diplomatic cover, and control agents in foreign countries
OFFICE
Provides administrative support for the Mossad station in the embassy
ILLEGAL AGENTS
Foreign nationals operating under the control of an illegal officer
SECOND IN COMMAND
Runs the daily operations of the Mossad station in the embassy
KATSA ATTACK
Officers who recruit foreign national agents
SECURITY
Provides security for Mossad operations
KATSAS
Case officers who control foreign national agents
MARATS
Technical specialists brought in from Israel for each operation
BODLIM
Couriers who act as cutouts, operating between safe houses and the embassy
COMMUNICATIONS
Controls computer and radio communications in and out of the embassy
SAFE HOUSE REFRESHER
Maintains safe houses so they are always ready for use
WEAPONS AND EQUIPMENT OFFICER
Provides operational weapons and special equipment
SAYANIM REGISTER
A list of volunteers in the Jewish community who are willing to help katsas
DIPLOMATIC POUCH
Message pouch used between embassy and Israel; also used by Mossad
FINANCE
Section that provides money for intelligence operations

Fate of a spy

Poisoned pin
American spy pilot Francis Gary Powers carried this poison-tipped suicide pin, concealed in a silver dollar.

SPIES OPERATE UNDER constant threat of detection and capture, which may result in them facing anything from a period in custody to the death penalty. "Legal" officers—those under cover of diplomatic immunity—are sometimes well known to enemy counterintelligence and are often treated leniently: a few hours of detention may be followed by release into the custody of representatives from the embassy of their own country.

Those personnel who operate without diplomatic protection, and are known as illegals (see p. 217), face far greater risks. Illegals are at the mercy of the judicial system of the country in which they are arrested. The agency controlling them may try to offer protection, but may have difficulty because knowledge of the illegals' identity is compartmentalized: the illegal agents are known only to those directly needed to support and control their activities.

Betrayal

Despite taking precautions, spies are always vulnerable to betrayal by moles (see p. 12). Moles work from within intelligence agencies and are often able to identify spies to the enemy service that is controlling them. The KGB mole Aldrich Ames (see p. 202) operated within the CIA and was able to betray at least 10 agents operating in the Soviet Union for the CIA. Most of these were killed. Ames also betrayed Oleg Gordievsky (b.1938), a KGB officer who worked as a mole for the British intelligence service MI6. The latter helped Gordievsky defect to Britain and avoid capture and possible death. Other important moles have included those of the Cambridge spy ring (see p. 209) who operated for years, betraying many agents.

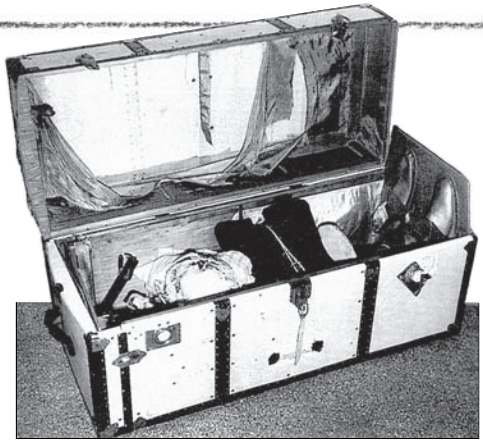
Interrogation cosh
This weapon was used in KGB interrogations. The flat end contains a lead weight which is covered in leather to avoid inflicting fatal blows while still causing great pain to the victim.

Cyanide vial and rectal concealment
This tube, which could be concealed in the rectum, was made for Germany's World War II security service, the SD. It held a glass vial of cyanide.

Punishments

The sentence for espionage varies from country to country and is affected by many circumstances. The former Soviet bloc countries generally executed those convicted of spying. Oleg Penkovsky (see p. 106), a GRU (Soviet military intelligence) officer who worked as a mole both for the CIA and for MI6, was executed after a well-publicized show trial, to make an example of him as a warning to others.

Illegals, too, may face execution if they are operating in particularly hostile circumstances. For example, the Arab



HUMAN TRANSPORTATION TRUNK

THE MAN IN THE TRUNK

Mordecai Louk, an Israeli, was a double agent working for both Mossad and Egyptian intelligence. In 1964, when Louk was living in Rome, the Egyptians suspected him and decided to bring him in for questioning. Louk was seized, drugged, and put in a specially designed trunk to be flown secretly back to Cairo. Inside the trunk, Louk was strapped in a leather seat, his feet were clamped to the floor of the trunk, and his hands and head were held in special fixtures. At Rome's Fiumicino airport, however, a delay allowed the effect of the drugs to wear off. Customs officers heard Louk's voice and released him. Later, Louk returned to Israel. Ironically, he was convicted and jailed on account of his contacts with the Egyptians.

MORDECAI LOUK

states almost always execute captured Israeli illegals. Such a grim prospect has led members of the Israeli intelligence organization, Mossad, to refer to the Arab states as "The Land of the Dead."

In post-World War II America and Western Europe, convicted traitors have generally received prison sentences. An important exception occurred in the case of Ethel and Julius Rosenberg (see p. 208), who were executed in 1953 for passing American atomic bomb secrets to the Soviets during World War II. The couple were the first American citizens to be executed for treason since the end of the Civil War.

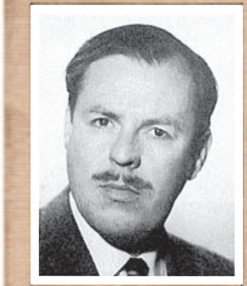
Illegal agents operating in the relative safety of the industrialized countries, such as Western Europe or North America, where there is less political violence may receive prison terms but may not have to complete them. They may be exchanged for prisoners held by other countries, in spy swaps.

Interrogation and torture

Counterintelligence services interrogate and occasionally torture captured spies to extract vital information from them. Some spies choose to commit suicide rather than risk being forced to give information that may compromise their mission and those involved in it. World War II SOE operatives (see p. 30) were often issued with "L" pills, capable of causing almost instant death; the U-2 spy pilot Francis Gary Powers (see p. 52) carried a poison-tipped suicide pin.

Glienicke Bridge, Berlin
The Glienicke Bridge across the River Spree between East and West Berlin. The bridge became well known as the site of several important exchanges of convicted spies.

GREVILLE WYNNE



SPY PROFILE

While in Moscow in 1961, British businessman Greville Wynne (1919–90) became a courier working between Soviet military intelligence officer Colonel Oleg Penkovsky and British intelligence. Wynne would visit Eastern Europe on business and collect material from Penkovsky to take back to England. In 1962 the KGB arrested Penkovsky and Wynne. Penkovsky was executed; Wynne was released in a swap for Konon Molody (see p. 50).

Turning a spy

In some cases, captured spies are offered their lives or freedom in return for becoming double agents (see p. 216). Many German spies detected by British intelligence during World War II took this option. The Germans, too, tried to turn spies. One of their main successes was in the case of an SOE agent whom they captured in Holland. He agreed to help the Germans by asking the SOE to send more men to Holland. Hoping to warn the SOE of his fate, the captured agent did not use the SOE security code when radioing his controllers. SOE headquarters failed to recognize this omission as a warning, however, and sent more than 50 operatives to Holland. All were immediately captured by the Gestapo.

One World War II spy, codenamed Cicero, met an ironic fate (see p. 34). He worked as a butler to the British ambassador to Turkey, and also as a spy for Germany. However, it was only after the war that he discovered that the Germans had paid him in forged English banknotes. Cicero's fate was to end his days in poverty.

The last cigarette
This unknown Russian spy was captured by Austrian forces in the Balkans in World War I. This picture was taken moments before his execution.

Spying in the future

21ST-CENTURY INTELLIGENCE AGENCIES face an array of challenges. As well as their traditional espionage and counterintelligence activities, they must increasingly help law enforcement agencies combat worsening economic espionage, international drug-trafficking, "cybercrime," and terrorism (see also p. 70), and counter the ever-growing threat of "rogue" nuclear states (see also p. 71). But the technological changes in how intelligence is collected, communicated, and analyzed are dramatic and ongoing. Most information is no longer stored on paper in one place, but is stored on networks that can be accessed from anywhere via the internet. All the secrets stolen by KGB and CIA spies in the Cold War could now be hidden on a memory card the size of a fingernail. Where once gadgetry supported agents in the field, now and in the future it is agents who increasingly must support technical operations as "cyberspies" (see also p. 74).

New for old
Handheld computer software can duplicate the clandestine function of most of the ingenious gadgets issued to agents in the Cold War.

Economic espionage

Intelligence agencies will increasingly conduct economic espionage in the future. Those in France, Israel, and China have long been suspected of helping companies in their own countries compete with foreign rivals. At the same time, intelligence agencies will increasingly have to investigate economic espionage, especially given the growth of "new economies" such as India. Already, international borders have become less of a barrier to industrial spies, who can anonymously use the internet to access corporate secrets stored in digital databases and archives from anywhere in the world.

SHELDON MENG

SPY PROFILE

A Canadian born in China in 1964, Sheldon Meng worked for Quantum 3D, a top California developer of visual simulator technologies. When he left the company in 2004 he took its prize "Mantis" software and tried to sell it to China's Naval Research Center, which could have used it to train fighter pilots. On his return to the United States in 2006 he was arrested by the FBI, who found thousands of stolen military and industrial files on his laptop. He received two years in prison.

Industrial spying is especially prevalent in the field of technology. The high cost of research and development means that any company that can steal a rival's fully designed concept can make vast savings. Especially valuable are secrets with both a military and an industrial application, as the case of Sheldon Meng (left) shows, but there is also plenty to be gained when the application is only an industrial one.

In 2007 in the United States, the Lubrizol Corp, which makes polyurethane products, noticed a huge improvement in similar products made by a South Korean rival called SK Chemicals. When someone from SK Chemicals let slip to an executive from Lubrizol that the Korean firm had someone "inside Lubrizol," Lubrizol called in the FBI, who discovered that a disgruntled Lubrizol employee of South Korean descent, Kyung Kim (b.1946), had been spying for SK Chemicals since 2001. Kim was sentenced to 19 months in prison for his betrayal.

Drug trafficking

Drug cartels have become so rich and powerful that they threaten to bring down the governments of some countries. In Mexico, for example, drug traffickers are now better armed and better paid than the police. They routinely use murder and kidnapping to terrorize anyone in their way. With the violence threatening to spread across the border into the United States, plans are in place to deploy US military forces as a deterrent. Meanwhile, US intelligence agencies are working with cooperative Central and South American governments to share information about drug shipments and locate processing facilities. But the drug trade is so big that it has become important to some countries' economies, such as Colombia's, so cooperation is not always forthcoming.

DOWNING
PARLIAMENT ST / GT GEORGE ST
LAMBETH BR / LAMBETH PALACE
HORSEGUARDS AV / VICTORIA EMB
NORTHUMBERLD AV / TRAF SQUARE
TOWER BRI -PT2- N- UP STREAM
HORSEFERRY RD / MARSHAM ST
TWEEDY RD / SHERMAN RD
ST THOMS - WATERFR - S
WHITECHAPEL RD / FIELDGATE ST
ARMOURY WAY
ROMFORD RD / VICARAGE LANE
EASTERN AVE
A124 Barking
NATIONAL GALLERY / TRAFALGAR SQUARE

Surveillance in the 21st century
With a huge bank of CCTV monitors—many more than are shown here—the Metropolitan Police Special Operations Room in London, opened in 2007, may be the largest of its kind in the world.

Cybercrime

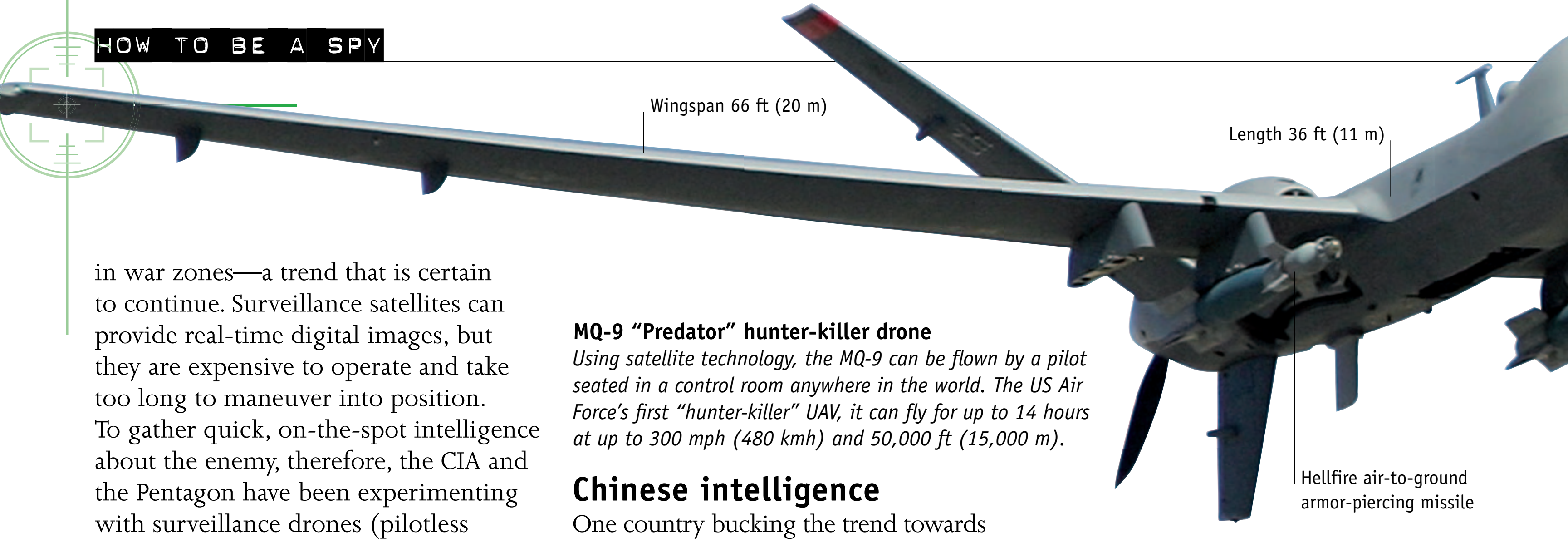
One relatively new problem faced by security agencies is cybercrime: crimes committed over the internet, including the theft of credit or debit card numbers, the spread of child pornography, identity theft, and network security violation. Police forces often lack the technology or training to trace cybercriminals, who can operate anonymously from anywhere in the world. A purchase made using card details stolen in country A may use an email address in country B, yet be the work of an individual in country C. Many companies no longer accept online card purchases for shipment to Africa, Russia, or parts of eastern Europe, because they are so often fraudulent. In 2008 in the USA, the details of more than 100 million computerized credit card transactions were stolen from Heartland Payment Systems, with no clues as to the identity or location of the culprit or culprits. Corporate information is also increasingly stored on databases that are connected to the internet, putting it at risk of network security violation. No wonder police forces are increasingly turning to government agencies for help.

Sawn-off AK-47
Drug traffickers in Mexico saw off the thin metal stocks of their favorite AK-47 assault rifles to make the weapons easier to hide under their coats. Drug-trafficking cartels murdered more than 5,000 people in Mexico in 2008.

Surveillance

Governments are increasingly installing closed circuit television (CCTV) cameras in public places. The recorded images from surveillance cameras help law enforcement and security agencies alike identify and apprehend terrorists and other criminals. CCTV cameras deter some criminals, help in the apprehension of others before they can carry out their intended offenses, and provide recorded evidence that helps in criminal convictions. However, like compulsory identity cards, they raise important questions about loss of personal privacy. Yet the likelihood is that they will continue to be used as vital tools in fighting crime, and that many more of them will be installed in the future.

Governments do not use modern surveillance technology only to fight crime. They are also increasingly using it



MQ-9 "Predator" hunter-killer drone
Using satellite technology, the MQ-9 can be flown by a pilot seated in a control room anywhere in the world. The US Air Force's first "hunter-killer" UAV, it can fly for up to 14 hours at up to 300 mph (480 kmh) and 50,000 ft (15,000 m).

in war zones—a trend that is certain to continue. Surveillance satellites can provide real-time digital images, but they are expensive to operate and take too long to maneuver into position. To gather quick, on-the-spot intelligence about the enemy, therefore, the CIA and the Pentagon have been experimenting with surveillance drones (pilotless planes) since the early 1980s, with significant success. Such highly maneuverable unmanned aerial vehicles (UAVs) can be launched from short runways close to battlefields and remain airborne for more than 24 hours to provide field intelligence. They can be operated at a much lower cost than conventional military aircraft, can stay in the air for longer, and do not expose highly trained pilots to enemy fire.

"7/7" LONDON BOMBINGS

The city of London has been called "the surveillance capital of the world," because it has more CCTV cameras per square mile/km than any other city. On July 7, 2005 four Islamic suicide bombers – three (below) on underground trains and one on a bus – killed 52 commuters and injured 700 more during the morning rush hour. Clear color CCTV footage from a number of locations helped the authorities establish their identities and track their precise movements that day.

Chinese intelligence

One country bucking the trend towards ever more technical intelligence-gathering seems to be China. As China's economy burgeons, so its government increasingly seeks to learn about foreign industrial and military technology, but in a low-tech way. China's primary intelligence agency is the Ministry of State Security (MSS), which conducts counterintelligence operations within China and HUMINT (human intelligence) operations abroad. The MSS conducts traditional agent operations, recruiting "volunteers" from among the many Chinese citizens working abroad in universities, in businesses, and in the military. Instead of employing clandestine gadgetry, dead drops, or the internet, volunteers report verbally—often during return visits to China. Volunteers from overseas frequently work for the MSS for only a few weeks of their entire careers. This very simple but highly effective set-up makes MSS operations very difficult indeed for foreign counterintelligence agencies to intercept or monitor with much degree of success.

"Rogue" nuclear states

In the future, Western intelligence agencies must continue to try to counter the spread of nuclear weapons and technology, and the accompanying rise of "rogue" states, that followed the collapse of the Soviet Union (see p. 71). Pakistan, India, and Israel are all believed to have acquired nuclear weapons in contravention of the 1968 Nuclear Non-Proliferation Treaty. Indeed, India, Pakistan, Israel, and North Korea are the only recognized sovereign states not to have signed up to the treaty. Since the late 1980s, nuclear know-how from one scientist—Abdul Qadeer Khan (b.1936), the "father" of Pakistan's nuclear program—has been secretly provided to North Korea, Libya, Iran, and Syria. In 2007, Israel destroyed a mysterious building in Syria with missiles in the belief that it was part of a nuclear reactor. Satellite images showed it to be almost identical to a building at a nuclear plant in North Korea, a country that recently reported that it now has "the bomb." Iran is rapidly enriching uranium, insisting it is for nuclear power generation only. Western intelligence agencies have programs in place to stop shipments of nuclear fuel and technology to Iran, but they also continue to monitor the global black market in fissionable material.

KATRINA LEUNG

SPY PROFILE

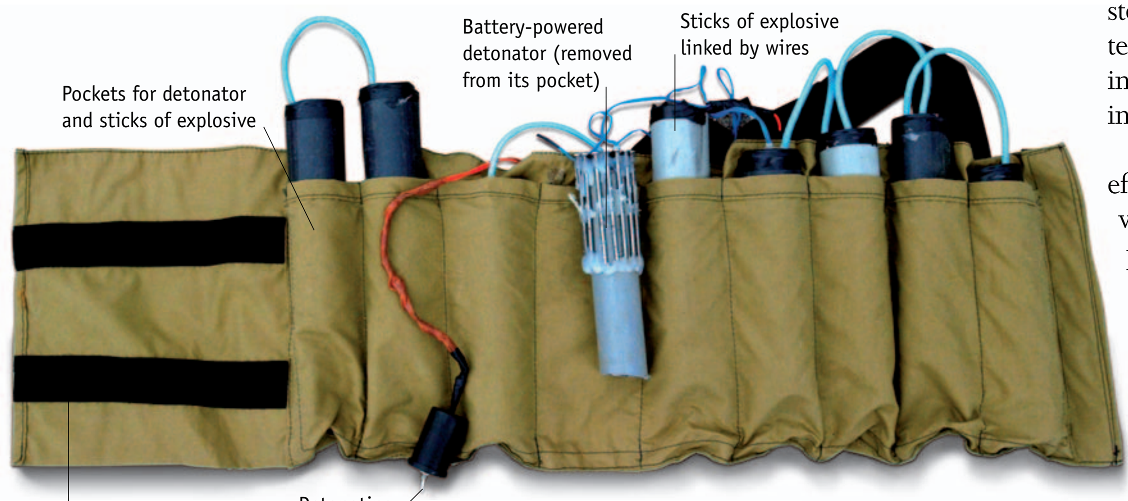
In the 1980s the FBI recruited Chinese-American businesswoman Katrina Leung (b.1954) to gather intelligence on the high-level contacts she made on her frequent trips to China, assigning her the code name Parlor Maid. But she soon switched sides and began passing information on FBI counterintelligence to the MSS. Leung was arrested in 2003, but in 2005 the case against her was dismissed when it emerged she had had an improper relationship with her FBI handler.

Global terrorism

Intelligence agencies in the future are certain to find themselves increasingly occupied with countering terrorism (see p. 70)—and particularly Islamic fundamentalist terrorism, which has been growing since the end of the Cold War.

So far, most terrorist operations conducted by Islamic fundamentalists have been suicide bombings, which require less sophisticated technology and, experience has shown, have proven difficult to prevent. The 9/11 attack on New York and the Pentagon in 2001 caused immense loss of life, but the terrorists responsible used little in the way of technology. They used box-cutters to muder plane crews, then used the planes themselves as guided missiles. In the many instances of individual suicide bombers on the ground, ingenuity and planning have usually been more important than technology. For instance, to get close enough to kill anti-Taliban leader Ahmad Shah Massoud in Afghanistan in 2001, two Arab suicide bombers posed as television journalists, with a bomb in their camera equipment.

In the future, terrorists look likely to use increasingly sophisticated technology in highly coordinated attacks, as in the simultaneous attacks by just a handful of terrorists on more than 10 sites in the city of Mumbai in India on the same day in November 2008—attacks that left at least 170 people dead and many more people injured. Among other highly up-to-date technologies, the terrorists used advanced Global Positioning Satellite equipment to navigate a hijacked fishing vessel from Karachi in Pakistan to the waterfront of Mumbai. All the while they talked to their controllers back in Pakistan over satellite phones, using Voice Over Internet Protocol to make their calls harder to be intercepted and monitored. They carried CDs with high-resolution satellite images of their targets. And once they were in Mumbai itself and had split up to attack their various targets they kept in touch by texting and emailing each other on smart phones.


Pockets for detonator and sticks of explosive
Battery-powered detonator (removed from its pocket)
Sticks of explosive linked by wires
Detonating switch
Velcro fastenings

Palestinian suicide bomb belt
Israeli soldiers removed this bomb belt from a would-be Palestinian suicide bomber. Designed by Yahya Ayyash (see p. 199), such belts are quite inconspicuous under loose clothing. Some female bombers conceal their belts under padding that makes them look pregnant.

A policeman at the Taj Mahal Palace Hotel
Mumbai police were unable to stop the attack at two hotels and other sites in November 2008 because they were unprepared for the superior planning and technology of the terrorists.

Cyberspying

Intelligence agencies will always employ the best technology available to support their activities. Penetrating an enemy's computer networks is now the best way to steal its secrets, but emerging information technologies also allow more traditional intelligence agency tradecraft to be applied in new ways (see p. 74).

But for "cyberspying" to continue to be effective, intelligence agencies in the future will have to seize the opportunities presented by new technologies as they emerge. It is vital that they stay ahead of their rivals. At the same time, as the example of the MSS in China makes abundantly clear, intelligence agencies must not lose sight of the essential, old-fashioned value of people. Human intelligence is often flawed, and the risk of betrayal is ever present, but a person on the ground can go where no search engine can yet follow—not least into the heart of a terrorist cell.

Glossary

Words in SMALL CAPITALS refer to other entries in this glossary.

Abwehr
German military intelligence, established before World War II. It was the primary organization for foreign intelligence-gathering until its merger with the SD in 1944.

Agent
A person, often a foreign national, who works for, but is not officially employed by, an intelligence service.

Assassination device
A special weapon selected for use in carrying out assassinations. These devices are usually concealable and some are designed to leave no traces at the site of the assassination.

Audio surveillance
A technique for surreptitious eavesdropping, often using electronic devices.

BfV
(Bundesamt für Verfassungsschutz) German counterintelligence agency, founded in West Germany in 1950.

BND
(Bundesnachrichtendienst) German foreign intelligence-gathering organization, established in 1956 in West Germany.

Case officer
An intelligence officer who controls or is responsible for an agent. See HANDLER.

Cheka
(Russian abbreviation for Extraordinary Commission for the Struggle against Counter-revolution, Espionage, Speculation, and Sabotage) Russian secret police organization founded in 1917 to serve the Bolshevik Party; replaced in 1922 by the GPU, later the OGPU.

CIA
(Central Intelligence Agency) Founded in 1947; the American agency responsible, like Britain's MI6, for the combined tasks of worldwide intelligence-gathering and COUNTERINTELLIGENCE abroad.

Cipher
A form of CODE in which numbers or letters are substituted systematically for those in a plain text message, so as to prevent unintended recipients from understanding the message.

Code
(1) A system designed to obscure the meaning of a message of any kind by substituting words, numbers, or symbols (from a code book or by any other previous arrangement) for plain text. Not every code is a CIPHER; in some codes, a symbol can represent an idea or even convey a whole message. (2) A non-clandestine letter substitution system such as MORSE CODE.

Concealment device
An object that has been altered for the secret storage and transportation of messages, ciphers, electronic bugs, or other TRADECRAFT items.

Counterespionage
COUNTERINTELLIGENCE operations that involve the clandestine penetration of a hostile intelligence service.

Counterintelligence
Broader category than COUNTERESPIONAGE, including action against foreign intelligence, and protecting information, personnel, equipment, and installations from espionage, sabotage, and terrorism.

Countersurveillance
Techniques used to detect hostile surveillance, and also to frustrate it.

Counterterrorism
COUNTERINTELLIGENCE operations aimed at foiling the plans and actions of terrorists.

Courier
A person who carries secret material for an intelligence service, either wittingly or unwittingly. A courier may also be a CUT-OUT.

Cryptanalysis
Also known as code-breaking, this is the study of CIPHERS and other kinds of CODES in order to reveal the original message, without having access to official keys or encryption systems.

Cryptography
The use of codes and ciphers to render communications that have been originally written in plain text unintelligible and secure except to the intended recipients.

Cut-out
A person acting as an intermediary between members of intelligence services or spy networks, improving network security by preventing contact between members.

Dead drop
A secure location, usually with a concealed container, used for secret communication and exchange of material between a spy and his controller. Dead drops remove the need for potentially dangerous personal meetings.

Defector
A person who, by choice, physically leaves the control of a country or intelligence service to serve the interests of another country. Such people often provide information of high value to the host intelligence service.

DGSE
(Direction Générale de la Securité Extérieure) French external intelligence service. Founded in 1981, the DGSE is similar in function to America's CIA and Britain's MI6.

Digital espionage
The use of digital technology, especially involving computers and satellites, for espionage activities.

Double agent
An agent of one intelligence service who is recruited and controlled by another intelligence service, to secretly work against their original service. A double agent should not be confused with a MOLE.

ECM
(Electronic countermeasures) The use of devices that render the electronic equipment of an enemy ineffective. ECM is applied extensively in warfare, and also in COUNTERINTELLIGENCE.

Enigma
An electromechanical, rotor-based CIPHER machine invented by German engineer Walter Scherbius in 1923. Versions of the Enigma were used for enciphering and deciphering messages by the German military and civil organizations during World War II.

FBI
(Federal Bureau of Investigation) Founded in 1924; responsible for COUNTERINTELLIGENCE and some other law enforcement duties within the United States. In its internal security and counterintelligence role, it is similar to MI5.

Flaps and seals
TRADECRAFT term for opening, examining, and resealing envelopes and packages without raising the suspicions of the recipient. The procedure originally involved clandestine manipulation of envelope flaps and wax seals, from which its name is derived.

FSB
(Russian abbreviation for Federal Security Service) Internal security service in Russia, successor to KGB Second Chief Directorate.

GCHQ
(Government Communications Headquarters) The British signals intelligence centre, similar to the NSA in the United States.

Gestapo
(Abbreviation for *Geheime Staatspolizei*) World War II German secret state police. Founded in April 1933, it was controlled by the Nazi Party and had responsibility for internal security throughout Germany.

GPU
See CHEKA.

GRU
(Russian abbreviation for Chief Intelligence Directorate) Founded in 1918 as the Soviet military intelligence service. The GRU survived the fall of the Soviet Union in 1991 and has continued serving the state of Russia.

Handler
A person, usually an intelligence officer (also usually a CASE OFFICER) who is responsible for, or controls, an agent.

HUMINT
(Abbreviation for *hum*an *int*elligence) Refers to information directly collected by human sources, such as AGENTS, as opposed to that collected via technology such as satellites.

HVA
(Hauptverwaltung Aufklärung) East German Foreign Intelligence Service, founded in 1952.

"Illegal"
A intelligence officer belonging to an agency of the former Soviet Union (KGB or GRU), an allied country, or to present-day Russia (SVR or GRU), operating in a hostile country without diplomatic protection but with the benefit of a legend (see p. 206). An illegal usually has no direct contact with his or her embassy, being controlled directly from Moscow.

Industrial espionage
The clandestine acquisition of information about business; may be carried out by a competitor, or by an intelligence agency.

Intelligence
This term can be applied to the profession of espionage, the information collected by espionage, or the final analysed product.

KGB
(Russian abbreviation for Committee for State Security) Founded in 1954 as the intelligence and security organization of the Soviet Union, and the successor during the Cold War of the CHEKA. In 1991, the KGB First Chief Directorate (for foreign intelligence-gathering) was dissolved but later re-formed as the SVR. The Second Chief Directorate (for internal security) was renamed the FSB.

"Legal"
An intelligence officer protected by diplomatic immunity and belonging to an agency of the former Soviet Union or one of its allies; since 1991, the equivalent in the case of Russia.

Listening post
A site at which signals received by means of electronic audio surveillance are monitored.

MI5
(Originally an abbreviation for Military Intelligence, section 5) MI5 has no military connection and is now officially called the Security Service. Founded in 1909, it is the British internal security organization. Like the FBI in the United States, MI5 is responsible for domestic COUNTERINTELLIGENCE.

MI6
(Originally an abbreviation for Military Intelligence, section 6) MI6 no longer has any military connection and is now officially known as the Secret Intelligence Service (SIS). Founded in 1909, it is Britain's foreign intelligence service. The role of MI6 is similar to that of the CIA in the United States and MOSSAD in Israel.

MICE
(Money, Ideology, Compromise, and Ego) These are considered to be the four prime motivating factors that may be of use in recruiting a potential agent.

Microdot
An optical reduction of a photographic negative to a size that is illegible without magnification. In practice, a microdot is considered to be 1 mm or smaller in size.

Minox
A subminiature camera, using 9.5 mm film, that has a wide range of uses in clandestine photography. The Minox was first produced in Riga, Latvia, in 1938. After World War II, a new Minox company was founded in West Germany. This company was, in 2002, still making cameras based on the original design.

Mole
An employee or officer of an intelligence service who agrees to work for another intelligence service. Some would-be DEFECTORS who approach an intelligence service they wish to work for are persuaded to remain in their posts and function as moles.

Morse code
Developed by Samuel Morse, an American, in 1838 for the electromagnetic telegraph, this code substitutes a series of dots and dashes for letters and numbers. The code is still in use and is internationally recognized.

Mossad
(Hebrew abbreviation for the Institute for Intelligence and Special Operations) Mossad was founded in 1951 and is Israel's external intelligence- gathering organization. It is similar in function to America's CIA and Britain's MI6.

NKVD
(Russian abbreviation for the People's Commissariat for Internal Affairs) The internal security and (despite the name) worldwide intelligence organization of the Soviet Union that succeeded the OGPU from 1934 to 1946.

NOC
(Non-official cover) An intelligence officer who belongs to an American agency and operates without diplomatic immunity.

NSA
(National Security Agency) The American agency, formed in 1952, responsible for information security, foreign signals intelligence, and CRYPTOGRAPHY.

OGPU
(Russian abbreviation for the Unified State Political Directorate) Founded in 1923 as the organization responsible for internal security and intelligence for the newly formed Soviet Union. It succeeded CHEKA and the GPU, and was replaced by the NKVD.

Okhrana
The secret police that operated in Russia under the Tsars between 1881 and 1917.

One-time pad
A set of paper or silk sheets, each bearing a series of random numbers or letters that is used only once for encipherment and decipherment of a message. The CIPHER is usually printed in groups of five letters. If each CIPHER is used only once, it is considered unbreakable. Pads for individual sheets are sometimes converted into MICRODOTS.

Operative
An officer or AGENT operating under the control of an intelligence service.

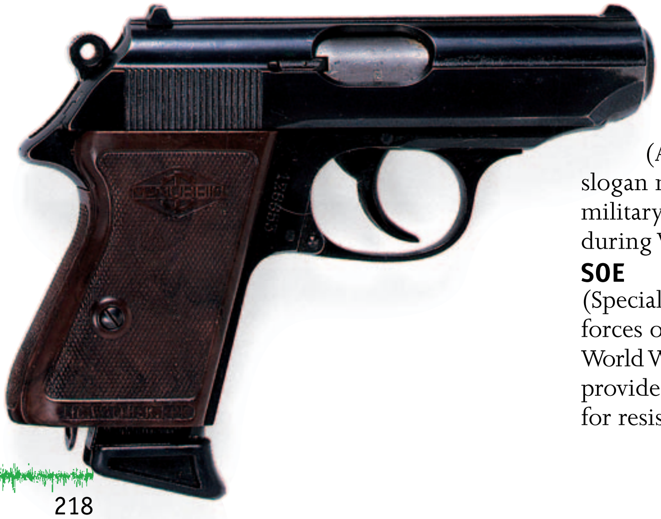
OSS
(Office of Strategic Services) Operational between 1942 and 1945, this American organization was the forerunner of the CIA.

OTS
(Office of Technical Service) The makers of gadgets and special devices for the CIA. Also the designation of the former makers of special equipment for the MfS (STASI) of East Germany.

OTU
Operational–Technical Department of the KGB and SVR, responsible for producing espionage equipment for Soviet and Russian spies.

Polyalphabetic substitution
The use of two or more CIPHER alphabets in a prearranged pattern to provide multiple substitutes for a particular letter in a message.

Receiver
Electronic equipment used to receive signals from electronic surveillance devices.



Reconnaissance
A mission undertaken to secure information, usually in advance of a secret operation.

Red Orchestra (Rote Kapelle)
The German name given to the successful Soviet military spy network that operated in Europe before and during World War II.

Resistance group
An indigenous underground organization that makes use of guerrilla warfare techniques and conducts sabotage and intelligence operations against an occupying power. Clandestine services of a country at war may work with resistance groups in enemy-occupied territory.

Safe house
A house or apartment that is thought to be unknown to foreign intelligence or COUNTERINTELLIGENCE and is considered temporarily safe for clandestine meetings.

SD
(Sicherheitsdienst, or Security Service) The SD was founded in 1934 as the political intelligence and COUNTERINTELLIGENCE service of the Nazi Party. In 1944 the SD was merged with the ABWEHR and became the dominant force in wartime Germany for intelligence-gathering and counterintelligence.

Secret writing
TRADECRAFT terminology for the use of secret inks (wet system) or special carbon papers impregnated with chemicals (dry system) for clandestine communication. Both systems use reagents to reveal the message.

SIGINT
(Abbreviation for *signals intelligence*) Refers both to intelligence gathered by eavesdropping on enemy electronic transmissions and to the process of gathering such intelligence.

Silenced weapon
A weapon modified by a noise suppressor fixed to the end of the barrel. Such weapons are not completely silent, but it may be difficult to identify the source of the noise.

Sleeper
An AGENT or officer who lives in a foreign country for years as an ordinary citizen. When a hostile situation develops, the sleeper is activated on preassigned missions of sabotage, assassination, or intelligence collection.

SMERSH
(Abbreviation for *Smert shpionam*, a Russian slogan meaning "death to spies") Soviet military COUNTERINTELLIGENCE organization during World War II.

SOE
(Special Operations Executive) A British special forces organization founded in 1940 during World War II to conduct sabotage operations and provide equipment, training, and leadership for resistance groups in Nazi-occupied Europe.

Spy
A frequently misused term that only applies to a person who secretly collects and reports information on the activities, movements, and plans of an enemy or competitor.

Spy satellite
An orbiting satellite that uses sensors to record photographic or electronic intelligence.

Stasi
(Abbreviation for *Staatssicherheitsdienst*) Founded in 1950, dissolved in 1989; East German state security, with a component (HVA) conducting foreign intelligence operations.

StB
(Statni tajna Bezpecnost or State Secret Security) Founded in 1948; the Czech intelligence and security service.

Steganography
The science of hiding messages, for example in MICRODOTS or as SECRET WRITING. Digital steganography involves hiding messages or images in digital media, such as computer files.

Support agent
An AGENT who services another agent or a network. This might involve replenishing SAFE HOUSE supplies or acting as a CUT-OUT.

SVR
(Russian abbreviation for Russian Foreign Intelligence Service) Succeeded the KGB's First Chief Directorate in the 1990s.

Tokko
The Special High Police Bureau of the Tokyo Metropolitan Police Department. During World War II, Tokko carried out domestic COUNTERINTELLIGENCE.

Tradecraft
The procedures, techniques, and devices used in clandestine intelligence operations.

Visual surveillance
The observation of a person, place, or thing, using visual means.

Index

Page numbers in **bold** type denote the main entry for a subject.

Acknowledgments

The author would like to thank the following for their assistance in preparing this book:
Al, Christopher Andrew, Annette, Inge Atwood and the late Col. Jim Atwood, Nick Benigsen, Ralf Beyer, Willi Bickel, Sid Boorstein, Janusz Borowski, Carl Boyd, Chase Brandon, David Brown and the John Brown family, Beth Bruins, Robin C., Rusty Capps, Dave Carey, CIA Museum, CIA Public Affairs Office, Tom Clinton, Jerry Coates, Peter Deriaban, Jr., Rich Di Sabatino, John Edwards, Dr. Charles Ewing, Dennis Flinn, Steve Gold, Oleg Gordievsky, Mick Gould, Sam Halpern, Chet Hanson, Michael Hasco, The Hon. Richard Helms, Herb Hetu, Toni Hiley, Col. William Howard, Lyle Hunger, Jack E. Ingram, James G. Joyce, Brian K., Maj. Gen. Oleg Kalugin, David Kharab, Steve Klindworth – Supercircuits, John Koehler, Jim Lecroy, Richard Lovell, Peter McCollum, David G. Major, Peter Mason, Prue Mason, Scott Meinket, Dawn Melton, Tony and Jonna Mendez, Ambassador and Mrs. Hugh Montgomery, Dr. Paul D. Moore, Seth Moore, Morris Moses, Dan Mulvenna, Dave Murphy, Jack Naylor, NSA – Office of Public Affairs, "Mr Orkin," Victor Ostrovsky, Dr. Oto, Jon Paul, Hayden B. Peake, Martha Peterson, Walter Pforzheimer, Rufina Philby, Jim Phillips, Carolyn Reams, Liane Reinecke, Gerald "Jerry" Richards, Gordon Rocca, Douglas St. Denny, Susan Rowen, Lloyd Salvetti, Jerrold L. Schecter, Rick Schroeder, R. Harris Smith, Glenmore Trenear-Harvey, Bob Troisi, Dr Helmut Trotnow, Oleg Tsarev, Detlev Vreisleben, Bob Wallace, Ron Weingarten, Nigel West, Glenn Whidden, Reade Williams, Gen. Markus Wolf, Capt. Greg Woody.

Dorling Kindersley would like to thank the following for their assistance:
Mark Cavanagh, Nicola Powling, and Duncan Turner for jacket design, and Jane Oliver-Jedrzejak for jacket copy writing; David Cooke, Jill Hamilton, Mary Lindsay, Lesley Malkin, Mukul Patel, Cathy Rubinstein, and Charles Wills for editorial assistance; Raúl López Cabello and Almudena Diáz for dtp design assistance; Neville Graham, Nicola Hampel, Nathalie Hennequin, Philip Ormerod, Helen Taylor, Hans Verkroest, Chris Walker, Todd Webb, and Mark Wilde for design assistance; Ray Allen, John Bullen, Diana Condell, Paul Cornish, and Mike Hibberd at the Imperial War Museum; Susan M. Rodgers at the Special Forces Club; Theresa Bargallo, Nick Goodall, Neville Graham, Louise Tucker, Nicholas Turpin, and Mark Wilde for modelling; Zygote Media Group.

Indexer Helen Peters.

Illustrators Mick Gillah, the Maltings Partnership; kja-artists.

Special photography Andy Crawford, Steve Gorton, and Gary Ombler.

Additional photography Bruce Chisholm, Geoff Dann, Philip Gatward, Dave King, Tim Ridley, Clive Streeter, and Kim Taylor.

PICTURE CREDITS
Dorling Kindersley would like to thank the following for their kind permission to reproduce the photographs:
a = above; b = bottom; c = center; f = far; l = left; r = right; t = top; crb = centre right below
Alamy 212tr
Archive Photos 38tr; 40tc; 127bl; 167tl; 209tl
Archiv für Kunst und Geschichte 16cr/**Palazzo Venezia, Rome** 18cl; 19br
Associated Press 9br; 12br, 58tr; 70bl; 128bl; 177cr; 199tl; 204bc; 210bl; 211bl/**Dennis Cook** 71b
Courtesy of Elizabeth Bancroft 58bl
Bildarchiv Preussischer Kulturbesitz 34cl
Bilderdienst Süddeutscher Verlag 156bl
Professor Carl Boyd 36tr
David Brown 147tc
Bundesarchiv, Koblenz, Germany 38cl
Cambridge University Library 37tr
Camera Press 8br; 11tc; 41br; 51bc; 52bl; 203tc
Corbis 26tr, 71tc, 72tr, 199c, 215bl
Courtesy of the Central Intelligence Agency, Washington, DC 47tl; 59tl
William Colby 33bl; 193cl-c-cr
Corpus Christi College, Cambridge 18bcr
Couvrette/Ottawa 1994 80bl
Crypto-AG 155cr
Geoff Dann/DK/Courtesy of the Imperial War Museum 133tl
Ian Dear 186ca
Peter Deriaban, Jr. 195bc
Deutsche Presse-Agentur GmbH 34bl; 211tr
The Devan Adair Company 13bc; 178cr
Richard Dunlop 33tr
Mary Evans 21bl
Courtesy of the Federal Bureau of Investigation, Washington, DC 1c; 54cl; 54bc; 55t; 55cl; 55c; 55b; 80br; 94tr; 170c; 170bl; 170bc; 208cl
Brian Fraser-Smith 124bcl
Willis George 142c
Getty Images 27br, 72bl, 198tr, 198br, 212cl, 213t, 214–15t, 214bl, 215tr
Hatfield House 19tl & ca
Jason Hawkes Aerial Library 74bl
Hulton 20tr & bc; 24bl; 25br; 37br; 45t; 179tr; 204ca; 209tc
Imperial War Museum/G.M Hallowes, Esq. 12tl; 30bl; 31bl; 35cl; 40b; 125tc; 125cl; 146bl; 146bc; 202tr; 203b; 204cl; 205cla; 205bc
Courtesy of Jack Ingram, Curator, National Cryptologic Museum/NSA, FT. Meade, Maryland 29bl; 36bl; 36br; 41bl; 42cr; 112tr & cr
Katz Pictures/Levy/Gamma Liaison 70br/**Najlah Feanny/SABA** 70bc
David King Collection 175tl
Library of Congress (BH82-4864A) 20bl; (LC-US262-11182) 23tr
Lockheed Martin Skunk Works/Denny Lombard 42tl; 52–53t
Los Angeles County Sheriff's Department 59bl
Peter Mason 190bl
Courtesy of Jim Minnery 188br; 206c; 206bl; 206br
Morris G. Moses 95br
Museum of the Confederacy, Richmond, Virginia 16bl/**Katherine Wetzel** 21tl; 21cr
National Archives 41tr
National Security Agency, Public Affairs 47tr
Courtesy of Victor Ostrovsky 190cr
Pearson Asset Library 69bc, 133cr
Jim Phillips 150bl
Popperfoto 8bl; 29tl; 44cl; 50cl; 50bl; 51tl; 51c; 51tr; 51bl; 190bc; 202bc; 209cl
Anthony Potter 136tc
Press Association 176br
Range 9cl; 11crb; 41tc; 46bl; 47br; 59tc; 122br; 137cl; 210br
Reuters 199br, 214c
Rex Features 73cl, 73cr, 73crr
Rex Features/Sipa Press 56b
Royal Marines Museum 130cr
Scala/Palazzo Vecchio, Firenze 18cr
Jerrold L. Schecter & Peter S. Deriaban 106cr
Science Photo Library/David Parker 74tr
Courtesy of the Security Service and the College of Arms 208cr
Carl Strahle 32bl
Topham 11br; 37bl; 39cr; 53cr/**Paul Elliott** 89cl; 106tc; 111br; 117br; 120bc; 122bl; 174bc & br
Oleg Tsarev 209c
US Airforce Office of Special Investigations, Public Affairs 158tc
WorldMap International/Ian Wilkinson 59br
Philip Zimmermann 75b

All other images are from the collection of **H. Keith Melton (www.spyimages.net).**

Every effort has been made to trace the copyright holders. Dorling Kindersley apologizes for any unintentional omissions and would be pleased, if any such case should arise, to add an appropriate acknowledgment in future editions.