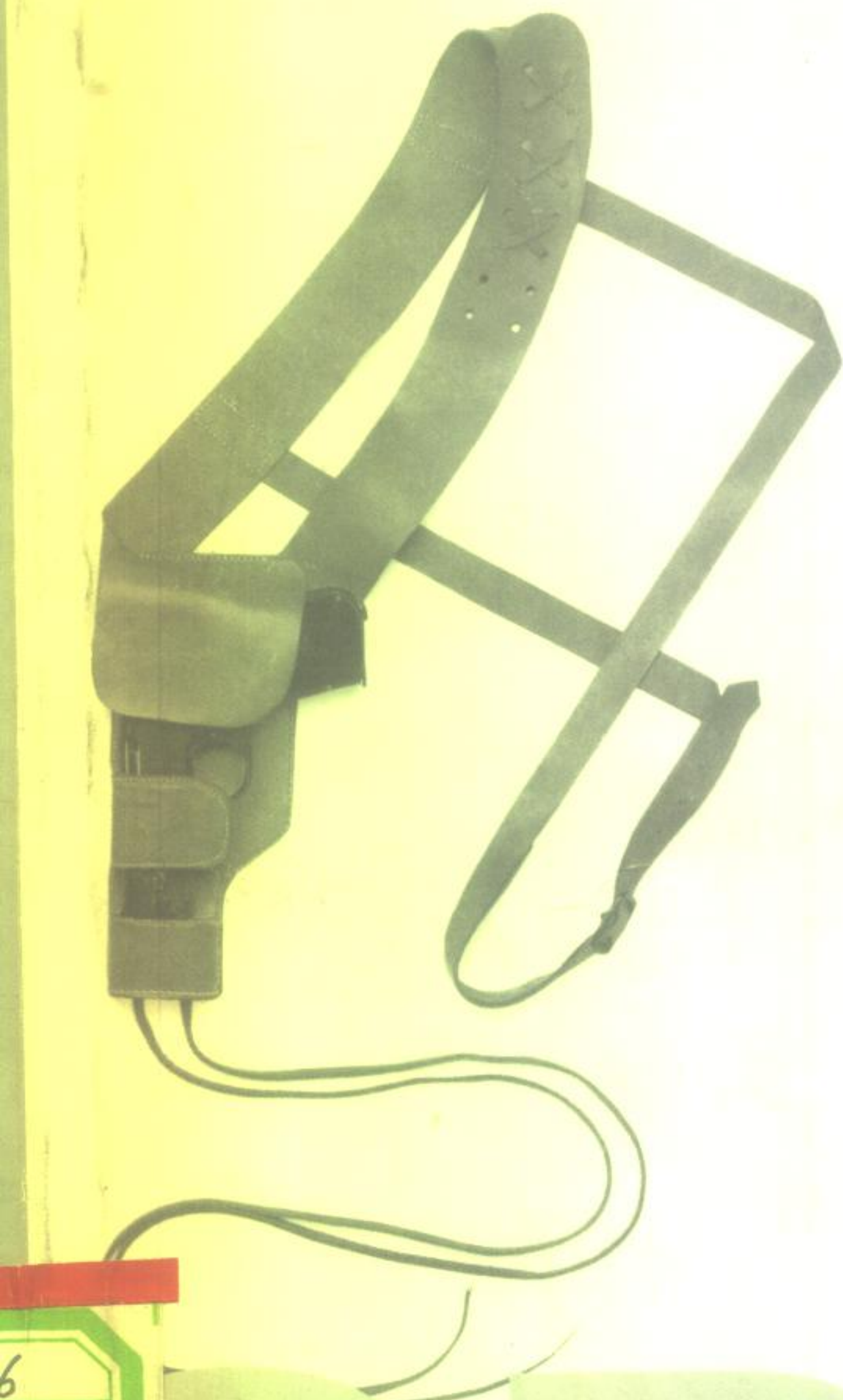


# 境外谍报器材与技术

裴迅 吴名等 / 编著

时事出版社



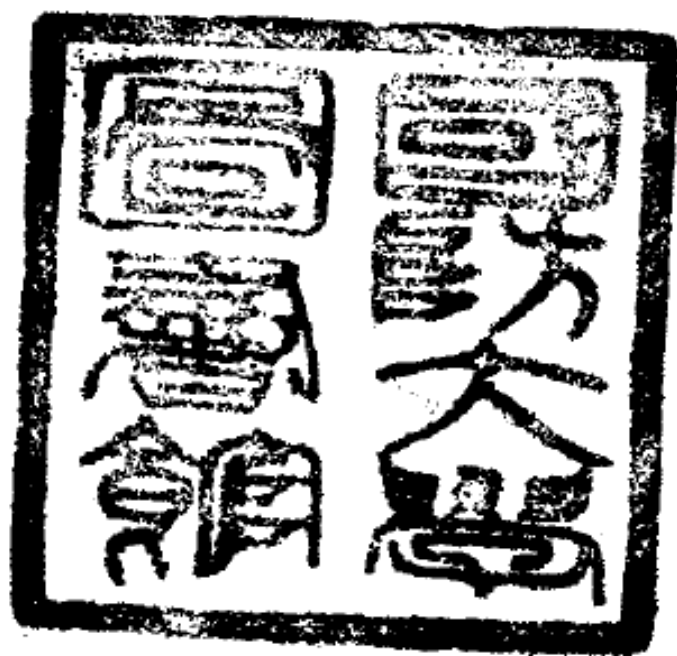


国防大学 2 065 6850 6

607-99/01

# 境外谍报器材与技术

编著人 裴 迅 吴 名  
开 厚 敏 利  
琛 玲 楠 桢等



时事出版社

内部资料 请勿外传

时事出版社出版发行

(北京市海淀区万寿寺甲 2 号 邮编: 100081)

新华书店经销

北京时事印刷厂印刷

---

开本: 850×1168 1/32 印张: 10.75 字数: 250 千字

1998 年 11 月第 1 版 1998 年 11 月第 1 次印刷

印数: 1—3000 册 工本费: 28.00 元

# 目 录

|                     |    |
|---------------------|----|
| 开篇导言 .....          | 1  |
| 一、声音情报的获取与保护 .....  | 6  |
| (一) 窃听 .....        | 6  |
| 1. 窃听器的种类 .....     | 6  |
| 2. 形形色色的窃听器 .....   | 10 |
| 3. 窃听案例 .....       | 22 |
| (二) 反窃听 .....       | 27 |
| 1. 环境检查 .....       | 27 |
| 2. 反窃听器材 .....      | 29 |
| (三) 侦听 .....        | 34 |
| 1. 侦听技术 .....       | 36 |
| 2. 侦听活动 .....       | 38 |
| (四) 反侦听——保密电话 ..... | 43 |
| 二、图像情报的获取 .....     | 47 |
| (一) 窃视与监视 .....     | 47 |
| 1. 窃视 .....         | 47 |
| 2. 监视 .....         | 49 |
| (二) 窃照 .....        | 51 |
| (三) 案例 .....        | 57 |
| (四) 恶劣环境下的观察 .....  | 62 |

|                    |     |
|--------------------|-----|
| 1. 微光成像 .....      | 62  |
| 2. 热成像 .....       | 65  |
| (五) 摄像、照相器材 .....  | 69  |
| 1. 特种照相、摄像器材 ..... | 69  |
| 2. 数字照相 .....      | 73  |
| 3. 新型成像技术 .....    | 76  |
| (六) 高空拍摄 .....     | 79  |
| 三、数据情报与信息战 .....   | 81  |
| (一) 概述 .....       | 81  |
| (二) 信号的侦收与防范 ..... | 83  |
| (三) 电磁辐射 .....     | 94  |
| (四) 病毒与防治 .....    | 96  |
| 1. 病毒 .....        | 96  |
| 2. 病毒的防治 .....     | 101 |
| (五) 网络安全 .....     | 103 |
| 1. 网络黑客 .....      | 105 |
| 2. 电子攻击 .....      | 109 |
| 3. 网络攻击案例 .....    | 112 |
| 4. 防火墙 .....       | 116 |
| 5. 数据加密 .....      | 119 |
| 四、密取与反密取 .....     | 126 |
| (一) 千奇百怪的锁 .....   | 126 |
| (二) 开锁能手 .....     | 134 |
| (三) 报警器与保安系统 ..... | 137 |
| (四) 复印与防复印 .....   | 142 |
| (五) 密取案例 .....     | 144 |
| 1. 绝招 .....        | 144 |
| 2. 漏洞 .....        | 147 |
| 五、通讯与联络 .....      | 155 |

|                   |     |
|-------------------|-----|
| (一) 秘密联络 .....    | 155 |
| (二) 密台与测向 .....   | 159 |
| 1. 密台技术 .....     | 160 |
| 2. 密码通信 .....     | 164 |
| 3. 测向侦察 .....     | 165 |
| 4. 案例 .....       | 167 |
| (三) 邮件与邮检 .....   | 171 |
| 1. 特殊邮件 .....     | 173 |
| 2. 邮检 .....       | 175 |
| 3. 案例 .....       | 176 |
| 六、空中侦察与通信 .....   | 181 |
| (一) 卫星简介 .....    | 182 |
| 1. 卫星结构 .....     | 182 |
| 2. 卫星轨道 .....     | 183 |
| 3. 卫星发展趋势 .....   | 184 |
| (二) 卫星侦察 .....    | 186 |
| 1. 侦察卫星的种类 .....  | 187 |
| 2. 侦察卫星举例 .....   | 190 |
| (三) 通信卫星 .....    | 197 |
| 1. 概述 .....       | 197 |
| 2. 举例 .....       | 198 |
| (四) 反卫星武器 .....   | 199 |
| (五) 卫星谍报案例 .....  | 203 |
| (六) 侦察飞机 .....    | 207 |
| 1. 侦察飞机简介 .....   | 207 |
| 2. 案例 .....       | 212 |
| (七) 高空气球 .....    | 214 |
| 七、人身安全有关技术 .....  | 215 |
| (一) 跟踪器材与案例 ..... | 215 |



|                    |     |
|--------------------|-----|
| (二) 测谎仪 .....      | 218 |
| (三) 证件与防伪 .....    | 219 |
| (四) 取证技术 .....     | 227 |
| 1. 照相方法 .....      | 227 |
| 2. 指纹识别 .....      | 232 |
| 3. 其他取证技术 .....    | 236 |
| (五) 药物 .....       | 239 |
| 1. 化学毒剂 .....      | 239 |
| 2. 基因武器 .....      | 245 |
| 3. 中毒案例 .....      | 246 |
| 4. 侦毒与解毒 .....     | 254 |
| (六) 特殊武器 .....     | 255 |
| 1. 非致命武器 .....     | 255 |
| 2. 杀伤武器 .....      | 263 |
| 3. 其他 .....        | 268 |
| 4. 案例 .....        | 270 |
| 八、谍报技术的应用 .....    | 273 |
| (一) 综合使用技术 .....   | 273 |
| (二) 谋略与技术手段 .....  | 279 |
| 1. 宣传战与心理战广播 ..... | 280 |
| 2. 培训特工 .....      | 282 |
| 3. 胁迫招募 .....      | 282 |
| 4. 情报策略 .....      | 284 |
| 5. 侦察案情 .....      | 285 |
| 6. 保卫防御 .....      | 288 |
| 7. 暗杀活动 .....      | 290 |
| 8. 爆炸破坏 .....      | 293 |
| 9. 目标指示 .....      | 294 |
| 10. 金融破坏 .....     | 294 |

|                 |     |
|-----------------|-----|
| 11. 特殊技能 .....  | 294 |
| 九、有关新技术 .....   | 296 |
| (一) 通信 .....    | 296 |
| (二) 计算机 .....   | 303 |
| (三) 信息处理 .....  | 307 |
| (四) 微加工技术 ..... | 312 |
| (五) 模糊技术 .....  | 315 |
| (六) 定位 .....    | 316 |
| (七) 其他新技术 ..... | 320 |
| 1. 电池 .....     | 320 |
| 2. 探测 .....     | 320 |
| 3. 传感 .....     | 323 |
| 4. 影像 .....     | 323 |
| 5. 武器 .....     | 325 |
| 6. 其他 .....     | 329 |
| 编后赘语 .....      | 335 |



## 开篇导言

自古以来就有间谍活动，从蒋干盗书到特洛伊木马，凡有敌对势力存在的地方，就有间谍活动。特别是在二次大战和冷战时期，形形色色的间谍活跃在各国政治斗争和战争舞台上，写下了许多不朽的历史。美国在中途岛战役大获全胜，就是因为它破获了日本人的密码；英美联军靠制造假情报迷惑了德国人，使他们以为诺曼底登陆仅是一场佯攻而失去了调动部队的时间。

随着社会的发展与进步，间谍活动已经不只局限于军事和政治斗争之中，在社会经济、科学技术等各个领域，都存在窃密与反窃密、破坏与反破坏的斗争。而且，间谍活动也不只是国家之间的行为，在企业集团、以及在一些特殊人物之间也有属于间谍性质的活动。据报载，法国巴黎每年要发生十几万件窃听案，多数市民时常有被窃听的感觉。据说其中仅“行政窃听”专用窃听线路就多达 1800 条。

翻开间谍活动的历史就会发现，这些间谍活动离不开使用各种各样的谍报器材。值得注意的是，谍报器材是随着世界科技的发展而发展的，在不同的历史时期，谍报器材大不相同，但几乎各国都把最先进的技术用在军事和谍报活动之中。

因此可以说，间谍人员无孔不入，谍报技术五花八门。

谁掌握了信息，谁就掌握了世界。准确和及时的信息是政权和管理机关的工作基础，如果一个国家作出政治决定的系统失去这些信息，那么很容易想象这个国家政治生活遭到破坏的程度。如今，美国政府制定对外政策，大到向海外派遣军队，小到征收进口汽车的关税，样样离不开国家安全局通过高科技手段窃取的各种情报。例如，法国总理巴拉迪尔 1994 年 1 月赴利亚德时深信自己能带回一份历史性合同，即 300 多亿美元的销售合同（主要是空中客车飞机），想不到却空手而归。这份合同被空中客车飞机公司的竞争对手——美国麦道公司夺走了。法国指责美国人利用电子窃听技术窃取了空中客车公司在这笔交易中的底牌和行贿情况。美国是通过位于从华盛顿到巴尔的摩的高速公路旁的一栋大楼黑色玻璃窗后面的超级电脑设备窃取到这些情报的。反过来，美国国家安全局通过窃听获取了情报，又指责法国汤姆森无线电报总公司为赢得巴西的雷达系统合同而行贿。最后，这份合同又给了汤姆森公司的竞争对手——美国雷声公司。高科技情报让美国占尽了便宜。

任何情报机关的中心任务都是获取秘密情报。但这仅仅是一系列必不可少的秘密活动之一，其他还包括通信、反侦察、破坏和逃脱（避免被敌方抓获）等。

为了进行上述活动，大型情报机关要训练掌握高级技能的人员并研制、开发特殊的技术和设备。在克格勃，这些工作是由一个称为 OT (Technical Operations) 的部门进行的。在中央情报局，相应的部门是技术服务办公室。为了达到同样的目的，以色列摩萨德雇用了一些称作 *marats* 的技术专家。

现在，让我们首先粗略地看一看上述秘密活动都需要哪些

技术和设备，详细介绍将分章节进行。

首先，声音侦察能得到大量有价值的情报。训练有素的专门人员可能会在进行秘密会谈或召开秘密会议的地方安置窃听装置。在某些情况下，他们用导线将窃听话筒与附近的侦听装置相连，也可能将窃听器连上一个发射机，将声音变成无线电信号发出，然后由特殊的接收机来拾取这些信号。有时他们还会使用录音设备。有些间谍会随身携带小型侦听设备到需要的地点，例如把麦克风和录音机藏在衣服或提包里。另一类声音侦听的方法是获取电话网络或空中传输的信号，这种情况下，不需要把侦听器材放在谈话现场。

除了声音情报以外，图像情报在谍报工作中也具有十分重要的作用。照相机可以用来偷拍秘密文件，照相机、摄像机可以用来监视外国间谍的活动。许多著名的间谍都是由于视频侦察手段的作用而被抓获的。侦察别国的地物地貌，根据其变化分析动向，是空中拍照的内容。在战时可以发现对手部队的调遣，在平时可以了解对手建设（特别是有关战略性武器发展）的情况。

各种通信设备都可能成为间谍通信的工具。第二次世界大战期间，秘密电台发挥了巨大的作用。在电信事业不太发达时，密写技术发挥着重要作用，而在通信技术高度发达的今天，各种电信器材都可能成为间谍通信联络的工具。

尽管使用特殊器材，可以从门下面或钥匙孔中观察室内的活动。但是有时需要直接进入室内，如果能“借”到一把可以复制的钥匙然后再还回去，无疑是最好的方法，不然就需要用万能钥匙尝试，如果这些都作不到就只好撬锁了，当然撬锁也是一门特殊的技能。

间谍机关还要训练间谍人员逃跑或避开敌人追捕的能力。

为达到某种目的，还要开发从事破坏和暗杀活动的工具和技术。例如伪装成煤块儿或动物粪便、和专门攻击停港轮船的小船等各种各样的爆炸装置；而各种暗杀武器有唇膏短枪、绞颈索、“在近距离发挥最大刺戮威力”的三指推压匕首、暗藏在拐杖内的毒气暗杀器、藏有毒气发射器和解药的钱包等等。

在人类从工业社会向知识产业社会过度的过程中，信息显示出越来越大的作用，热武器为主的战争形式也在朝着电子战、信息战发展，因此，围绕着信息安全的间谍活动也日趋频繁。当然，新形式下的间谍活动有其新的特征，往往不需要地理上的介入就可以获取对方的情报，甚至给对方以致命的打击。安全环境保护的问题是反间谍斗争的重要手段。为了防止敌对势力窃取我方情报，必须针对可能的泄密渠道，采取防范措施，其中包括必要的技术手段。

关于本书内容，需作如下几点说明：

1. 本书内容均选自公开发表的资料，重点是国外各种谍报技术，但是它又不是一本纯技术性的书籍，没有任何理论推导，适合于从事有关工作的读者参考。书中也收集了一些案例，以增加趣味性和可读性。至于有关间谍谋略的内容，不包含在本书中。

2. 由于广义上的谍报活动不仅牵涉到间谍机构，同时和公安、部队也有密不可分的关系，因此书中的内容就不局限在狭义间谍活动的一个方面。

3. 已经出版的一些有关间谍、反间谍的书籍中，有的主要论述间谍历史、作用、性质、谋略、培训等，是情报机关的很好的参考书；有的专门讲述一些著名案例，有很好的趣味性和

可读性，但是专门介绍谍报器材的书籍却不多见。“科学技术是第一生产力”在任何时代，谍报工作都离不开科学技术，因此，我们感觉有必要出版一本专门介绍国外谍报技术的书籍，这对从事有关工作的读者或许有一点帮助。

4. 从广义上讲，谍报技术不应该仅局限于具体的器材、工具，特别是现代技术的发展，使得利用现成的器材进行谍报工作成为可能，也就是说，有的谍报技术仅仅是一种技术，而不是什么特别的器材和工具。因此书中个别章节看似缺少具体器材的介绍，而着重情况的说明。

5. 有些技术可以用在不同的场合。例如，窃听可以是获取敌方情报的手段，也可以是发现间谍保卫自己的手段。所以在章节的编排上，难以十分清晰。这一点希望读者见谅。

6. 我们知道，各个国家都设法把最先进的技术用于军事国防、谍报工作中，有些尚未开发、但可能开发成谍报器材的新技术，我们也把它们收录在本书之中。

最后，尽管笔者收集参考了许多资料，但是毕竟数量有限，可能有些重要的资料没有收集在内；加之笔者水平有限，可能存在一些不足和错误，敬请读者指正。

## 一、声音情报的获取与保护

### (一) 窃听

绝大多数情报都是以视、听形式出现的。如果能够听到目标的谈话内容，就可能得到许多重要的信息。为了获得声音情报，许多国家的谍报机关都把窃听做为情报活动的重要手段，尤其是美国、俄罗斯、日本、以色列、英国的情报机关，他们不惜工本，开发、使用了大量的窃听器材，并且利用窃听技术窃取了大量的情报。

例如，俄罗斯情报局很是偏爱“顺风耳”技术，他们以窃听、监听为主。只要对你有“兴趣”，当你踏上他们的国土后，就可能被窃听器“包围”，而你却毫无知觉。

与其他的情报手段相比，窃听具有简便、可靠、安全的特点，因此尽管窃听器被叫作臭虫 (BUG) 而臭名昭著，发达国家仍把最先进的电子技术应用于窃听器的研究，并大量地使用它。现在，无论是窃听器本身，还是窃听技术，都已达到了很高的水平。

#### 1. 窃听器的种类

窃听器有很多种类型，最常见的是无线窃听器、有线窃听器、红外窃听器、激光窃听器等。



(1) 无线窃听器是指通过某种频率的无线电波把窃听到的信号发送出去，然后用接收机收听。现代科学技术使无线窃听器的性能达到了空前的水平，并使之成为当代间谍反间谍斗争中应用十分广泛的最典型的窃听工具。

无线窃听器一般由超小型高灵敏度拾音器、超小型高性能发射机和电池组成。它常常被秘密地安放在目标处的各种日用、办公用品中，例如钮扣、领带夹、计算器、手表、打火机、酒瓶盖上等等，甚至放在昆虫的身上。性能良好的无线窃听器可以窃听到几十米以外的窃窃私语，并将它传送到几十米、几百米甚至几千米外，在那里，人们坐在旅馆的房间里或坐在不太远的汽车里就能收到窃听的声音。无线窃听器必须和专门的窃听接收终端配用。

为了不被发现，有的无线窃听器在听到声音之后，马上把它变成密码传递出去。

一般，无线窃听器靠电池供电，使用寿命取决于它的电池能用多长时间，因而受到限制。也有的装在室内的无线窃听器使用交流电，靠电源线、电话线供电，如装在台灯插座内、电话机内等地方。这种无线窃听器不受电池使用寿命的限制，可以长期使用。使用调频广播波段的无线窃听器，频率范围一般 76—96MHz 范围内，用一般调频接收机即可接收。其发射距离可达几十米至几百米。使用这种窃听器必须避开当地调频广播电台，是一种低档货。VHF 波段的无线窃听器，频率一般在 135—155MHz 范围内，UHF 波段窃听器的频率范围是 335—445MHz。这两个波段的无线窃听器使用了晶体振荡器，频率是固定的，必须用专门的窃听接收机收听。由于受到接收机的限制，不易被他人收听到。发射距离可达几百米甚至几千米之外。无线窃听器的发射距离受到所用天线和周围环境的影响，在开



阔地区的发射距离比建筑物密集的地区要远得多。

无线窃听器的研究正在向微型化、长寿命、可遥控、可加密的方向发展；前端趋向于无金属、无 PN 结 调制方式由原先的简单调频或简单调幅发展为现在的双调制，或采取跳频方式，有的还在时域上进行压缩，以提高发射速度。

(2) 有线窃听器由微型麦克风、馈线及听录音设备组成。它依靠室内的电话线、电源线或其他金属导体提供电源和传送声音信号。它可以安装在电话机内、墙壁、窗框或建筑物的构件中，由专线或电话线、电源线与监听站的收听、录音设备相连接。例如载波窃听器就是利用电源线作传输线。麦克风拾取室内话音后，经放大调制在载波信号上送到电源线上传输，窃听者在电源线上接一个接收机，即可听到室内的谈话。

使用有线窃听器，无需向空中发射电磁波，用普通的反窃听接收机很难发现它。因此，有线窃听是一种可靠性较高、早已为人们所熟知的窃听方式。其弱点是需要事先潜入目标场所，把窃听装置安装在电话机内或电话线上。

另外，电话机本身也能成为窃听话筒，70 年代末期，美国情报机关发现，被挂断了的电话机的话筒里面的麦克风仍然可以通过电话线发射微量的脉冲，这种脉冲可以被分离出来，并转换成声音。只要能接上电话线并配备一套相应的仪器，每一个房间和办公室里的电话机就都变成潜在的窃听器。

现在，有线窃听器已发展到使用光纤技术，细小的光纤极易隐藏在墙壁的粉浆或油漆下面，把声音信号变成光信号传送可以对抗反窃听探测。光纤窃听器用特别的振动腔代替通常的微型话筒，没有金属导线。一般反窃听装置都是通过接收窃听器发射的微弱电磁波，或者探测金属材料来发现窃听器的，因而，采用光纤技术的窃听器不易被探测出来。

(3) 激光窃听器是近年来发明的一种新的窃听技术。激光窃听系统由以下几部分组成：a. 激光发射机；b. 激光接收机；c. 具有几万倍放大倍数的均衡器；d. 电池；e. 耳机。

它的工作原理是：房间内或汽车里的谈话声波使门窗玻璃产生轻微振动，放在附近的激光发射机对准窃听目标的门窗玻璃发射不可见激光束，射到玻璃上的激光束受到玻璃轻微振动的调制（激光束随着这些振动发生变化）并且被反射回来，反射回来的激光束已经携带了门窗玻璃的振动信息。激光接收机把收到的反射激光束过滤，并转变成电信号，再由均衡器滤掉干扰噪声并对声音信号整形放大，带上耳机进行准确调谐，就可以清楚地收听到紧闭门窗的屋内或汽车里的谈话声。

激光窃听器窃听距离可以达到 500 米，窃听过程中不易受到其他声源的干扰。但是它的操作比较复杂。

(4) 红外窃听系统和激光窃听系统相似，也是一种近年发展起来的利用光学原理实现窃听的装置。红外窃听器由微型红外听筒发射机、红外光学接收机、瞄准望远镜和运算放大器组成。红外听筒发射机带有红外传感器，它可以无声地拾取周围 30 米以内的话音，并把话音传送到几百米甚至上千米远。红外窃听系统不单适合窃听室外谈话，也可以透过混凝土和关闭的玻璃窗拾取室内的话音并发射出去。使用时，把红外听筒发射机放在目标场所，如公园里、汽车上、墙壁、窗框、阳台上等地方，用带有 5000 毫米透镜的精密的红外光学接收系统，瞄准发射机的方位进行接收，即可窃听到目标处的讲话，并同时讲话声录音。这种窃听器用常规的探测器也是无法发现的。

(5) 声音的直接窃听在某种场合也是有效的。例如利用管道或者使用定向话筒做为传声器。早期的定向话筒是喇叭式的，根据声音的传播特性，它可以听得很远，现代的定向话筒采用