谁在窃听

李抒音 曹宏 编著

金城出版社

谁在窃听

形形色色的国际窃听战

李抒音 曹宏/编著

金城出版社

图书在版编目（CIP）数据

谁在窃听：形形色色的国际窃听战/李抒音，曹宏编著．
－北京：金城出版社，2002.5
ISBN 7－80084－419－6

Ⅰ.谁…　Ⅱ.①李…②曹…　Ⅲ.侦听－世界
Ⅳ.E87

中国版本图书馆 CIP 数据核字（2002）第 019623 号

金城出版社出版发行
（北京市朝阳区和平街 11 区 37 号楼　100013）
中国农业出版社印刷厂印刷
850×1168 毫米　1/32　7.5 印张　160 千字
2002 年 5 月第 1 版　2002 年 5 月第 1 次印刷
印数：1－3000 册
ISBN 7－80084－419－6/E·11
定价：16.00 元

前　言

窃听原指偷听他人的谈话，自古以来就是获取他人秘密的重要手段。但现代窃听的涵义却早已超出了“隔墙偷听”的范围。由于科学技术的不断发展，窃听内容已不再局限于窃听电话、谈话等语言信息，而是扩展到了对包括无线电信号、计算机数据、互联网电子邮件等在内的所有情报信息的监听；同时，窃听器材更是不断更新，各种微型窃听器、激光窃听器、微波窃听器、红外窃听器让人耳目一新，而无线电侦听、手机窃听、卫星窃听、海底光缆窃听、动物窃听等各种窃听手段，更是令人防不胜防。目前，高技术窃听业已成为各国情报机构乃至各大利益集团窃取情报的最常用、最有效的手段。

然而，如同有“矛”就有“盾”一样，有窃听就必然有反窃听。先进的科学技术不仅能被窃听者利用，同样也可为反窃听者提供技术支持。于是，各情报大国在不择手段地窃取他国情报的同时，又在不断地研制着各种反窃听、防窃听器材，试图以最先进的反窃听技术和最有效的反窃听手段，为自己编织一张安全大网。

无论是冷战期间还是冷战结束后，各国情报机构之间的窃听与反窃听大战从未停止过，相反，随着人类进入信息社会和国际竞争日益加剧，更呈愈演愈烈之势。其中，件件窃听案例如同故事般引人入胜，种种离奇的窃听手段更是令人

叹为观止。

本书以纪实的手法和翔实的材料，向读者描绘出当代国际窃听活动的恢弘场面，并通过生动的实例介绍了种种窃听手法，以期广大读者在阅读的同时，增进保密意识，增强保密知识。

目　录

第一章

窃听，永不过时的武器

窃听是获取情报的一种最传统、最常用的手段。从古代人用耳朵偷听近在咫尺的谈话，到今天情报间谍利用高科技手段截获远在千万里之遥的信息，都属于窃听。通过窃听获取情报，是由情报的属性所决定的。绝大多数情报信息都是以视、听形式出现的，如果能够听到目标的谈话内容，便可从中得到许多重要的情报。与其他情报手段相比，窃听具有更直接、更简便、更安全、更可靠的特点，因此，许多国家的谍报机关都把窃听作为情报活动的重要手段。其中美国、俄罗斯、日本、以色列、英国等国的情报机关，更是不惜工本，研制和使用了大量的窃听器材，并以此为手段窃取了大量的情报。

由于情报斗争的需要和高新技术的发展，窃听技术也日新月异，不断向高、精、尖方向发展，窃听设备层出不穷。窃听对象已从单一目标发展成窃听某一方向的大系统；窃听范围也已从陆地窃听发展到太空和深海；窃听内容更是从语言扩展到窃取数字信息。正如美国前中央情报局局长艾伦·杜斯所说："除非一个人死了，钉进了棺材，任何人也无法绝对保证他的谈话不会被外人窃听"。老布什总统离任前也曾坦言："作为一个美国总统，我可以肯定地对你们说，在我们的国家决策程序中，技术窃听是一个主要的因素。"经

济间谍专家吉本斯更是一针见血地指出：联合国总部大楼像冷战时代的维也纳一样，已成为世界各国间谍的温床，无数用以量度震动频率的特制红外线镜头均瞄准联合国大楼，以截听大楼内的每一句对话。

可见，在这个情报日显重要的信息时代，窃听无处不在。窃听，已成为一件永不过时的重要武器。

❖ 古今中外窃听史话

窃听，俗称“偷听”，意为在别人不知晓的情况下，听取其谈话内容，从中获取消息的一种行为。古今中外，因话语被窃听而造成损失的事例不胜枚举。

在我国，窃听的历史可以追溯到公元前 202 年。当时，西楚霸王项羽被汉王刘邦率领的几十万大军，团团围困在垓下。在楚军的营帐里，被久困的士兵都在窃窃私语。有的抱怨三军没有粮，有的议论战马没有草，更多的人是发泄对连年战乱的不满，并不时地发出思念故乡楚国的叹息。这一切都被帐外的汉军细作听在耳里，并及时报告给了刘邦。刘邦与其谋士们立刻根据这一重要情报，制订出了瓦解楚军的方案。就在两军决战的前夜，一阵阵深沉的楚国歌曲，从四面八方传进项羽的军营。歌声一下子激起了久已厌战的楚国士兵们思念家乡、父母、妻子的情绪。开始是三三两两地开小差，后来便整批整队地走掉。就这样，项羽的千军万马迅速瓦解。刘邦借助于“墙”外细作之耳，取得了军事上的胜利，逼得项羽走投无路，最终在乌江边被迫自刎。

无独有偶，在第二次世界大战期间，美国政府征集了大批商船运输军火。一位名叫杰克的船员在出海之前，匆匆来

到码头旁的咖啡馆里与女友玛丽进行电话告别。看来，这位多情缠绵的女友对杰克此行的安危实在是放心不下。为安慰女友，杰克告诉她这次船队行动的日期、航行的路线和停靠的港口，让她在家耐心地等待。不幸的是，这温情脉脉的对话，却被坐咖啡馆中扮成商人模样的德国间谍偷听到了，并将这一重要情报迅速报告给纳粹德国的情报机构。结果，这支船队在茫茫的大洋上遭到德国潜艇毁灭性的打击。玛丽等待的杰克永远也不会回来了。这一血的教训换来的是美国人的一句警句——“多嘴能沉船”。

无论是中国古代汉军的细作，还是打扮成商人的德国间谍，他们窃听的方法，还只是用自己的耳朵偷听他人交谈这一原始的方法，属于人工情报的范畴。而事实上，在别人耳朵边谈论重要情报的实例并不多见，因为人们总是关在屋子里讨论秘密的事情。原始的声音窃听，一般都是靠人隐匿在房间的周围，或以其他身份为掩护，偷听他人的谈话。这种窃听方法听到的是最为真实的声音，但常常受时间、地点、环境和条件的限制，又极易被人察觉，因此可操作性大受限制。现代情报战线上的窃听，已不再是“隔墙有耳”这一原始意义上的窃听，而是采用一定的技术手段来获取远距离的谈话，乃至密室内本不可听到的交谈。在科学技术高度发达的今天，无论是密室中的谈论，还是保密电话中的交谈；无论是空中的电波，还是深水海底的电缆；无论是加密的手机信息，还是通过计算机网络发送的电子邮件，都有被窃听的可能，而且所窃听的情报在瞬息之间就会被传送到千里之外。这一切，都离不开日新月异的窃听技术。从这个意义上讲，技术情报要比人工情报更具有可信度。

窃听技术是窃听行动所使用的窃听设备和窃听方法的总称。它包括窃听器材，窃听信号的传输、保密、处理，窃听

器安装、使用以及与窃听相配合的信号截收等。窃听技术的内涵非常广泛，特别是高档次的窃听设备或较大的窃听系统，应该包括诸如信号的隐蔽、加密技术，工作方式的遥控、自动控制技术，信号调制、解调技术以及网络技术、信号处理、语言识别、微电子、光电子技术等现代科学技术的很多领域。考虑到本书的可读性、趣味性，这里我们讲的“窃听技术”，主要是指获取信息的技术方法，也包括获取信息的传递方法。

✣ 形形色色的窃听手段

近年来，随着现代电子技术的高速发展以及数字通信时代的到来，窃听技术也日益完善，窃听设备不断更新换代。目前已形成了包括有线、无线、激光、红外、卫星、计算机等种类齐全、功能先进的庞大窃听家族。

☞ 延伸的耳朵：专线窃听器

1985 年 8 月，美国驻前苏联新建使馆在莫斯科即将竣工。按照常规，美国派安全人员用 X 光对建筑物的混凝土预制板进行检查，结果在第 8 层楼的较敏感地点的混凝土构件中，查出了一大堆麦克风。美国谴责苏联搞窃听，苏联方面不但矢口否认，反而倒咬一口，怒斥美国缺乏诚意，破坏两国首脑即将举行的和平对话，为东西方的缓和进程设置障碍。小小的麦克风和窃听有什么联系呢？

这种麦克风其实是专线窃听器的组成部分，就像是延伸出去的人耳。这种窃听器的结构比较简单。其基本原理是把

小型麦克风隐匿在所要窃听目标的房间内，用导线接到监听点的放大器或录音机上。为了消除由于连接线长而带来的杂音，可在麦克风后加一个前置放大器，把拾取的声音先放大，然后再送到窃听点，使窃听的声音更加清晰。这种前置放大器通常采用集成电路，体积很小，便于放置。通常将麦克风和前置放大器用环氧树脂或有机硅封灌在一起。如果传输的质量好，窃听点可设置在与窃听目标 1.6 公里远的地方，这样更加便于隐蔽。

为使房间内任何位置、任何方向的谈话都能听得清楚，可在房间的不同角度埋设两个以上的麦克风。比如，可以隐藏在门框里、墙壁内、天花板上，甚至可以伪装成墙上的钉子等。随着技术的不断进步，专供窃听用的麦克风已可以做得只有针孔般大小，一般肉眼很难发现。

传输声音的导线大多沿着建筑物的钢筋或金属敷设，从地下或地面引出送至窃听点。窃听点则由专人监听，发现情报，及时上报。

这种窃听技术看来很原始，但窃听效果好，好比人的伸长的耳朵，能真实地听到对方的谈话内容。同时，因其藏匿于钢筋混凝土之中，很难用仪器检测出来，具有很强的生命力。在接待外宾的饭店，特别是在外国领使馆中，常有这种窃听器。埋设专线麦克风窃听器，一般都是在新建或改建房屋时进行。如我们开头所讲的美苏使馆窃听事件，就是苏联在美国建馆时安放的。在已经使用的房间内，则可以安置载波窃听装置。这是一种以电源线作传输线的窃听器，其工作原理是：当窃听麦克风拾取到室内的谈话声音以后，经过放大、调频变换成载波信号闭塞到电源线上传输；而窃听者在电源线的任何位置接上一个载波机，便能听到室内谈话的内容。这种装置的窃听麦克风，一般都安装在室内电源插座附

近。除了电源线外，其他线路如火警报警线等，也都可被用作窃听器的传输线。

除了驻外使馆、宾馆饭店，专线麦克风窃听器也常放置在与毗邻国接壤的边境地区，进行窃听活动。人们把一些麦克风伪装成枯枝、土块之类，安放在对方军队的哨所附近，而窃听的信号则通过埋在地下的导线，越过边境引入己方境内。

☞ 无所不至的“臭虫”：无线窃听器

1963 年 3 月的一个早晨，美国驻罗马尼亚首都布加勒斯特大使馆的保安人员，正在使用无线电检测仪器作例行检查。突然，他们收到了美国大使同别人的谈话声音。根据电波的方向，保安人员来到大使的办公室，递给他一张纸条，上面写道：“请你走出办公室并继续交谈，但要小心讲话的内容，因为你的讲话正在被秘密广播。”但当大使走出办公室后，保安人员仍能从检测仪器里听到他的讲话。由此判断，窃听器一定是藏在大使身上。原来，前几天大使曾经让使馆的女仆将皮鞋拿出去修理，显然，窃听器就是这个时候被间谍人员放进了鞋跟里。

放在大使鞋跟里的这种窃听器，称作无线窃听器。无线窃听器主要由微型拾音器（即话筒）、微型无线电发射机和电池组成。工作时，话筒将拾取到的声音以无线电波的形式辐射到空中，窃听者则在有效的距离内用无线电接收机接收。其工作原理相当于常见的无线电台发射电波，我们能够通过无线电收音机收听节目。为了避免无线窃听器发射的信号被普通收音机接收，就要求窃听器的发射频率要跳出一般无线电台的广播频率，达到窃听的目的。

曾经有这么一个笑话。一个孩子正在收音机旁边选择广播节目时，突然从收音机里传出他爸爸和客人的谈话声。孩子惊讶地叫嚷起来："妈妈，快来听，爸爸正在发表广播讲话呢！"正在隔壁房间里与客人谈话的爸爸闻声赶来，听到孩子的话，吓得面如土色。他马上到自己的房间里细心查找，发现在他的写字台下面贴着一个黄豆大小的窃听器。像这样安放窃听器要么是一种恶作剧，要么就是窃听器的技术太落后，其频率落在了普通广播的频段里。使用调频广播波段的无线电窃听器，频率范围一般在 76～96MHz 范围内，发射距离为几十米到几百米之间。因此种窃听器易被当地的调频广播接收，目前使用者已很少。使用较多的是 VHF 和 UHF 两个波段的窃听器，VHF 波段的频率在 135～155MHz 范围内，UHF 波段的频率范围是 335～445MHz。这两个波段的无线电窃听器均使用晶体振荡器，其发射频率也是固定的，需有专门的人以特定的频率来接收窃听。同时，这两种窃听器的发射距离可达到几百米甚至于几千米之外。

无线窃听器的作用距离，主要是由发射机的功率、发射天线的效率以及接收机的灵敏度等决定的。接收点通常都是事先准备好的，接收机的体积不受更多的限制，所以接收机的灵敏度是容易做到的。为保密起见，窃听器的发射天线的尺寸一般很小，其效率也不高。所以无线窃听器的传播距离主要取决于发射机的功率，二者之间成正比，即发射机的功率越大，无线电窃听器的传播距离就越远。但大功率的发射机要求有充足的电源来保障，这样就增大了窃听器的体积，不符合隐蔽性、保密性的要求。另外，功率越大辐射波也就越强，其安全性也就越差，被检测出来的可能性也就越大。目前生产出来的窃听器，其发射功率只有几毫瓦到几十毫瓦。

早在50年代，前苏联克格勃的特工器材制造厂就开始研制、使用无线窃听器。当时其生产的一种名叫“喊”的窃听器，如火柴盒般大小，能像蝎子一样吸附在墙上，不易被人发觉，但窃听效果却很好。1954年，克格勃在伊朗驻莫斯科大使馆首次安放了这种窃听装置。70年代以后，随着大规模集成电路和微电子技术的迅速发展，无线电窃听技术水平也得到了空前提高。其主要发展趋势是：

①体积微型化

目前，无线电窃听器的体积越来越小，重量也越来越轻，性能也越来越好。如美国CCS公司的STG4003微型无线窃听器，体积仅有$10\times10\times4mm^3$，重量也仅有3克，使用一节1.5伏的纽扣式电池供电，发射距离达200米，可连续工作48小时，窃听器话筒拾音范围为20米。这种超微型窃听器很容易隐藏在台灯、烟灰缸、钢笔、手表、打火机里。德国人甚至还研制出一种可安放在酒杯里的超微型窃听器，专门用来窃听人们餐桌上、酒吧里的谈话。喝酒的人用肉眼根本无法发觉，他们之间的哪怕是低声的交谈，也可被清晰地传递到百米之外的窃听点。

②供电自动化

无线电窃听器一般靠电池供电，使用寿命取决于它的电池能用多长时间，因而使用时限受到限制。为避免经常更换电池造成的不便，装在室内的无线电窃听器使用交流电，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。此外，还有一种利用高谐共振技术的窃听器，本身不用电源，只是个振荡器。室内的谈话声使振荡器先共振，窃听者只要向室内发射高功率微波，用以测出其振动情况，即可还原出声音。美国研制的乳房发射机，可以安装在妇女间谍

的假乳头里，以人体体温为能源工作。使用时，两个假乳头同时装上，即便女间谍在受到最彻底的裸体搜查时也很难查出。

③控制智能化

目前，最先进的无线窃听器大多有遥控功能，当室内无谈话声音时，窃听器便自动停止工作；发现或预感到对方有检查窃听的行动时，遥控窃听器便停止工作，或使电波搜索设备探测不到窃听器及隐蔽的具体位置。此类产品有 IBCOL 公司的 MO2019A 声控窃听器和 MO2015A 无线遥控窃听器。

④传输密钥化

为提高窃听器的防检测性能，无线电窃听器发射的电波要经过加密处理，这样，即使用无线电检测机来检测，听到的也只是一片噪声或杂乱无章的干扰声，解不出任何信息。加密的方法有多种，最常见的是使用跳频技术。

跳频技术是信息传输过程中促使空间信道不断跳变的一种信息技术。普通空间信道是一个“开放”的信息传输通道，使用固定的频率传输，很容易被对方窃听或被无线电干扰，于是，跳频技术就成了反窃听和反干扰的“克星”。它采用先进技术，使通信过程中的频率不断跳变，以此达到隐蔽自己的目的。由于跳频图案可以设置几百乃至上万个，收发两端只要跳频图案一致，跳频时间同步，就可在信息传输过程中不断跳变空间信道，实现跳频通信。就其实质而言，跳频技术既是窃听者的一道密钥，又是防止窃听的一种手段。

无线电窃听是一种方便快捷、行之有效的窃听方法，已经成为各国间谍情报活动中应用非常广泛的一种窃听手段。前苏联克格勃在上个世纪 50 年代中期研制成功、并得到广泛应用的一种微型无线电窃听器“嘁”，可以用气枪弹射到

窃听目标房间的墙外，清楚地听到目标的谈话声。这样，间谍不必蹑手蹑脚地接近目标，就可以窃取秘密信息。

“嗡”还有较强的发射能力，它可以用超短波将所收到的声音发射到直径为5英里的范围之内，用一个灵敏度很高的接收机就能收到。克格勃用这种窃听器窃听了许多国家驻莫斯科大使馆里的谈话。

最早正式宣布发现这种窃听器的是伊朗驻莫斯科大使馆。之后，1956年～1965年间，这种“嗡”又在原联邦德国的西柏林、波恩、科隆等地中心建筑物的蜡壁外面被发现过，还曾在巴黎、伦敦、华盛顿、罗马等地被发现过。为此，人们曾形象地称这种微型无线窃听器为“夏天的臭虫”，比喻其无所不至。

目前世界上最先进的无线窃听器首推美国中央情报局的杰作“BUG”（意为臭虫）。它的体积小到可以握在手掌中，而拾音能力却极佳。这种窃听器中装有一个微型处理机，可以对无用信号进行压缩和抵消，只取出需要窃听的有用信号。与一般的窃听器相比，它最大的优点就是只把需要的声音收进来，把其他杂音分离出去，即使在用音响设备播放音乐的舞厅或闹市，也可以收到目标清晰的谈话声。

☞ 防不胜防的“耳朵”：电话窃听器

自从1876年美国科学家贝尔发明世界上第一部电话至今，经过百余年的发展，电话已成为当今世界最普通的主要通信工具，政治、经济、军事、外交以及科学技术和文化生活都离不开电话。有人把电话比喻成现代社会的“神经”系统，形象地反映了电话通信的重要作用。特别是在信息化高度发达的今天，电话的使用已相当普遍。据统计，日本平均