
学校的理想装备
电子图书·学校专集
校园网上的最佳资源
神奇的电子战
BOOK
内部资料 非卖品

引　言

远在第二次世界大战后期，被喻为“战场幽灵”的电子战（又称电子对抗）就已和到全面的运用。1945 年，第二次世界大战结束了，而对电子战的理论研究和电子对抗 试验等，不少国家的军队，都在紧锣密鼓般地进行着。

伴随着现代科技日新月异的发展，军事领域中的高技术层出不穷。从近些年世界上发生的局部战争和武装冲突来看，电子进攻与电子防御这一矛盾体的对抗，已成为高技术条件下局部战争的主要作战样式之一。其成功与否，往往直接关系不战争的进程与成败。

电子对抗是什么？交战双主是怎样进行对抗的？电子对抗的现况如何？明天又将怎样？这本小册子就上述这些问题作了解答。

本书在编写过程中，参考了同类书籍和报刊上发表的文章，在此，对其作者表示衷心的感谢。

从第二次世界大战到今天。世界上发生了 100 多次局部战役战斗的各个方面，并贯穿于作战人全过程，从而提高了作战效能，直接影响着战役战斗的主动权。电子对抗被称为是继陆、海、空战之后的“第四维战争”，使战场上有的正面、纵深和高度三维空音又增 加了一维——电磁频谱。

内容提要

随着科学技术的发展，高新技术不断被用于军事装备中。本书介绍了许多高新技术应用于战争中的战例，向我们展现了高新技术参与下的电子攻防对抗战，以帮助读者认识高新技术的作用，现代战争中电子对抗的发展动态。

神奇的电子战

一、“ 魔法战争 ”今和昔

当年英国首相邱吉尔，在回忆第二次世界大战的情景时，曾把战争中使用的电子对抗誉为神奇的“ 魔法战争 ”。

那么，什么是电子对抗？它“ 魔 ”在何处？伴随着科学技术的进步，电子对抗是怎样发展起来的？下面就来说说这些问题。

(一)先机制敌的悄声战争

电子对抗是什么？目前世界各国尚无统一定义。这是个智者见智、仁看见仁的问题。多数学者认为：电子对抗是指敌对双方利用电子设备或器材所进行的电磁斗争。它利用电磁能探测、识别敌方使用的电磁频谱和电子设备，并根据探测和识别结果，采取各种措施，削弱或破坏敌方使用的电子设备的效能，同时又能保障己方正常运用电磁频谱，使电子设备得以充分发挥作用。在国外，人们把电子对抗称作“电子战”或“电子斗争”。

通过以上对“电子对抗”的描述，可以看出它有这样五层含意：

一是电子对抗作为现代战争中一种重要的作战手段，其目的是为了“消灭敌人，保存自己”。

二是电子对抗要“消灭”的不是敌方的有生力量，而是各种电子设备，使其通信中断、雷达迷盲、兵器失控、指挥瘫痪、战斗力丧失，整个军队就将变成一个“又聋、又瞎、又哑的乌合之众”。

三是电子对抗所使用的武器，不是枪炮、飞讥、坦克、军舰等有形的“硬性”杀伤手段，而是一种无形的“软杀伤”工具——电磁能。

四是电子对抗之所以称“对抗”，是由于它遵循了一般作战行动的基本规律，有攻有防。电子对抗主要有三种对抗方法——电子侦察与反侦察，干扰与反干扰，摧毁与反摧毁。

五是电子对抗打击的目标，是敌方的通信、雷达等电子设备，往往是在明火执仗的战争之前发起。也就是说，战争尚未打响，电子战早已进行。海湾战争的例子最能说明这一点。

1991 年 1 月 17 日凌晨 2 点 35 分，也就是在联合国限定伊拉克从科威特撤军的期限刚过 17 个小时，一枚枚“战斧”式巡航导弹从停泊在波斯湾中的美军“密苏里”号和“威斯康星”号战列舰上呼啸升空，飞向巴格达，准确地击中了那里的战略军事目标。至此，持续了 5 个多月的以“沙漠盾牌”为代号的战争准备阶段，终于演变成为以“沙漠风暴”为代号的海湾战争。

其实，这场海湾战争并不是以第一枚导弹的轰炸声而宣告开始的。早在 1990 年 8 月，从伊拉克入侵科威特那天起，一场静悄悄的电子战争就已开始部署，并在美国白宫发言人正式发表向伊拉克进攻的声明之前 5 小时就已大规模展开了。由此看来，电子对抗是一场先机制敌，不见刀光剑影的特殊战争。

(二)年逾古稀的战争宠儿

纵观科技发展史，各种先进技术往往应战争需要而诞生，并首先服务于战争领域。电子对抗技术也不例外。

电子对抗问世于第一次世界大战，在第二次世界大战期间得到广泛运用。

第一次世界大战爆发前，英国物理学家麦克斯韦总结了前人对电磁学的研究成果，预示了无线电波的存在，而且指出它的传播速度和光一样快。随后，德国物理学家赫兹用人工的方法产生了无线电波，并在另一个地方接收到了它，证实了麦克斯韦的预言，从而奠定了无线电通信的基础。从此，人类的通信开始跨入了无线电波的时代。

无线电通信的问世引起了世界各国军队的普遍关注。第一次世界大战期间，所有参战国的部队，几乎都建立起了通信兵团(当时叫信号部队)，发明无线电报的先躯——马可尼先后亲自服役于意大利陆军和海军。

无线电波在空间传播，能飞越国界，无论己方还是敌方，只要拥有相应的无线电设备都能接收到。根据这一道理，敌对双方可用相应频率的无线电信号，干扰对方无线电台工作，于是，就出现了互相利用电磁波进行的电子斗争。

1914 年，第一次世界大战拉开了序幕。当大不列颠帝国刚刚对德宣战不久，地中海上发生了引人注目的事件，为电子对抗成功地用于战争开创了“ 元年 ”。

那年，航行在地中海上的德国巡洋舰——“ 格贝恩 ”号和“ 布雷斯劳 ”号被英国巡洋舰“ 格林斯特 ”号尾随盯梢。这艘英舰紧紧盯梢的目的，原是想把德舰的踪影和活动情况利用无线电通信及时报告设在伦敦的皇家海军部，以便海军部下令地中海舰队利用适当战机去拦截和击毁这两艘德国军舰。然而事与愿违，德国巡洋舰利用装在舰上的先进的无线电侦察设备，迅速侦听到“ 格林斯特 ”号与英国海军部之间的通信情况，并探明了英舰上无线电通信设备的技术参数，先发制人下了手。他们果断地发出一串串与“ 格林斯特 ”号上无线电台相同频率的噪音信号，严重地扰乱了英军正常的无线电台通信，有时甚至使英军无线电信号完全被噪音淹没而无法分辨。英军舰无线电台人员曾几次更改通信频率以躲开干扰，但都无济于事。此时，德舰趁机调头，突然改变航线，全速行驶至与其友好的土耳其达达尼尔水域，成功地甩开了英军的跟踪和阻截。英军舰困于严重的无线电干扰，眼巴巴地望着德军两艘军舰从自己的眼皮底下溜掉。这可算是无线电电子侦察和干扰技术的早期的一次实战应用。

地中海海战失利，刺激了英军电子对抗技术的发展。特别是引起了军事首脑人物对电子斗争的重视。时隔两年，1916 年 5 月，英德两国军舰再次对阵，英国皇家海军上将亨利·杰克逊运用海岸无线电测向器及时侦察德军舰队的活动。根据当时捕捉到的一些微弱的无线电信号，掌握了德军舰队的航行路线，将主力埋伏在既定海域，并选择有利战机，调遣舰只进行攻击，打得德军措手不及，惨遭重创，几乎全舰队覆没。

如果说作为战争“ 宠儿 ”的电子对抗技术在第一次世界大战中崭露头角，随着科学技术的发展，第二次世界大战则为它提供了大显身手的活动舞台。

与第一次世界大战相比，第二次世界大战期间的电子对抗有了长足的发

展，促成了一系列作战指挥的胜利。主要表现在：对抗的种类愈来愈多。第一次世界大战以后，磁控管、脉冲振荡器和定向天线等新型技术相继涌现，随之问世了雷达、导航和兵器控制系统，使电子对抗由单一的通信对抗发展成导航对抗、雷达对抗等诸多类型。

导航系统被喻为飞机的“向导”，有了它，可改变靠目视的飞行状态，这对提高飞行精度、保证飞行安全起着举足轻重的作用。正因为这样，交战双方为了削弱乃至摧毁对方的空战力量，总是千方百计地在破坏对方的导航系统上打主意。因此，“导航对抗”应运而生。1940 年，德国空军为了空袭英国，在法国北疆建起了无线电定向发信系统，为德军飞机引航。使德机按照无线电波束的引导，顺利飞达伦敦上空。英国人得知这一情报后，迅即制定出了反空袭无线电对抗方案。他们建起了一套模拟导航系统与之对抗，使德军飞机同时接收到两种寻航信号。由于鱼目混珠，造成德军飞行员难辨真伪，以致多次迷航，误将飞机着陆在英国空军基地上，或使轰炸机的炸弹纷纷落入英吉利海峡中。英首相将这一奇妙而又诡秘的电子战夸耀为“魔术战”。

雷达被喻为“国防千里眼”，成了第二次世界大战中预报敌机空袭的强手。有了雷达就引来了雷达对抗。1943 年 7 月 25 日凌晨到 8 月 3 日，英国轰炸机群大举进攻德国汉堡布，总共出动了 3100 架次飞机，借助于雷达对抗系统，仅被德军击落 86 架，损失率不到 3%。

对抗的规模愈来愈大。1944 年的诺曼底半岛战役，是世界战史上规模宏大的登陆战。交战双方是英美联军和德军。德军为了反登陆进行了为期两年多的周密准备。据记载，构筑工事用去钢铁近 150 万吨，水泥达 150 万立方米。联军为了突破这道坚固的物质防线，采取了“软硬兼施，双管齐下”的作战方针。一方面运用火力直接摧毁；与此同时，几乎动用了所有的电子对抗设备，其规模之大，实属有史以来所罕见。其中包括设立假司令部、拍发假电报、进行通信欺骗、实施各种强有力的电子干扰，使德军电子设备和指挥系统陷入“聋、哑、瞎”瘫痪状态。在强有力的电子干扰下，盟军登陆部队迅速地下破了诺曼底防线登上半岛。整个登陆过程中，盟军共出动了 2127 艘舰只，只有 6 艘被德军击沉，损失率不到 3‰。

对抗的范围愈来愈广。第一次世界大战期间电子战主要应用于海军；第二次世界大战期间，电子战便开始应用于空军；第二次世寻大战后愈来愈广泛地应用于陆军诸兵种。第二次世界大战期间，电子战还与“气象战”结伴，直接参与了旨在破坏敌方气象情报体系的斗争。1940 年夏秋时节，英军通信侦察部门通过电子侦察发现了德军设在冰岛和格陵兰地区的一些地面气象站，随即通过火力系统将其摧毁。英军通信侦察部门通过电子侦察还截收和破译了德军的大量气象报告，根据德军对那些地区的气象最感兴趣，推断出他们的作战企图，以便及时采取措施，予以防范，或先机制敌进行打击。

对抗的速度愈来愈快。“兵贵神速”这一兵家格言，不仅对明火执仗的火力战来说。是制胜之道，对无声无影的“电子战”也不例外。有时军事情报早来或迟到一刹那，就会对战争结局造成截然不同的影响。随着电子技术的发展，第二次世界大战期间，电子对抗速度日益加快，对保障作战胜利起到了重要作用。

1940 年 8 月 8 日，德国空军司令下达了大规模空袭英国的命令，这一命令迅速被英国电子侦察部门侦察、截获，在不到一个小时时间内，就将这一

情报送到了英国首相邱吉尔的案头。英国战斗机部队根据邱吉尔的命令，迅速作好战斗准备，采取了各种有力措施，及时挫败了德军消灭英国空军的企图。第二次世界大战后期，盟军的无线电侦察技术更加发达。1943 年，英军研制成功了一种代号为“ 赫夫—杜夫 ”的自动测向器，它能在 1 秒钟内准确地测出敌军的电磁辐射，并计算出辐射源的地点和辐射方向。这种自动测向设备可以海陆两用，装在舰船上和海岸站内，只要德军潜艇开机发信，英军就能迅即捕捉到信号，测算出潜艇位置，并派遣反潜舰艇与飞机予以攻击、摧毁。

对抗的频谱愈来愈宽。电子战频谱在第一次世界大战期间还仅限于短波、超短波，到第二次世界大战期间就开始扩展到微波，现在已扩展到毫米波，乃至微米波的光电对抗。

对抗的密级愈来愈高。随着保密通信的破译技术日益先进，第二次世界大战期间，电子侦察的对象已由侦听、探测一般性的无线电信号逐步发展到侦察敌方要害部门和首脑人物间的通信。大战中，盟军情报机构就曾通过“ 超级破密机 ”，截收和破译德国陆、海、空军的各种作战情报，甚至截收和破译了包括希特勒等头面人物在内的有关德方高级指挥部之间来往的高密级电报和情报，为赢得大战胜利奠定了基础。

第二次世界大战结束时，“ 电子对抗 ”时值“ 而立之年 ”。经过两次世界大战的洗礼，它风华正茂，呈现出一派生机勃勃的景象。不仅电子对抗设备的数量激增，功能和威力更是今非昔比，已成为世界各国部队先机制敌的法宝，成为战斗力中一个不可缺少的基本要素。

(三)高效费比的作战手段

从第二次世界大战末期开始，直到近期发生的越南、中东、马岛、美利冲突和海湾等战争中，电子战都发挥了很大的作用。实战表明，成功地运用电子战可以及时收集敌方的军事电子情报，干扰、迷惑、破坏敌方的电子设备及武器控制系统，对保障己方的电子设备和武器控制系统的正常工作起着巨大作用。无数事实都雄辩地表明，电子战是一种效费比很高的作战手段。

电子对抗的效费比是衡量电子对抗战场效益的一项重要指标。具体定义为：

$$\text{电子对抗效费比} = \frac{\text{电子对抗装备参战后减少损失所节约的资金}}{\text{参战电子对抗装备消耗的资金}}$$

第二次世界大战中，英美联军为了打赢电子战争，成立了电子干扰航空队，专门执行干扰任务。在一次对德军的夜袭中，共出动了 211 架轰炸机，并伴用 11 架飞机专门对其施放积极干扰和消极干扰。在英美联军的严重干扰之下，德军的高炮效率大大降低。据估计，在飞机没有装备电子对抗设备时，德军高射炮每击落一架飞机只需 800 发炮弹，而作战飞机装备了电子对抗设备后，每击落一架飞机所需的炮弹猛增至 3000 发。因此，电子对抗设备的使用，给英美联军创造了很大的战场效费比。定量计算可得到，上述战例的电子对抗效费比为 27.5。这个数字粗略地告诉我们，假设给电子对抗装备投资 1 元钱的话，在作战过程中就可使飞机本身少损失 27.5 元。

朝鲜战争中也有类似的战例。据统计，战争中联合国军共损失飞机 1300 多架(飞机上已不同程度地装有电子对抗设备)。据军事专家们推测，联合国军若不采取电子对抗行为，损失的飞讥将可能是这个数字的 3 倍，即要损失 4000 架飞机。因而，可求得电子对抗效费比为 20。即每给电子对抗装备投资 1 元，在战争中可使飞机少损失 20 元。

随着电子对抗设备的日益高技术化，电子对抗效费比也日益提高。剖析越南战争、中东战争和海湾战争的战例，电子对抗效费比已上升到 60 以上，甚至超过 100，而且战争越现代化，武器对军事电子技术的依赖性越大，电子对抗装备的战场效费比也就越高。

强有力的电子对抗手段，不仅使敌方的电子设备和武器控制系统不能正常工作甚至瘫痪，而且给对方人员造成很大伤亡，使战斗力骤降。据国外军方对历次战争的分析，用不用电子对抗对人员的伤亡有很大区别。剖析第二次世界大战、朝鲜战争、越南战争和中东战争情况，可大致得到以下结论：

在达到相同战果的条件下，应用电子对抗以后，可以使伤亡人数减少 10～90 倍；或在敌我伤亡人数相同的条件下，应用电子对抗以后，可以使投入的初始兵力减少 10～90 倍。这无分说明，电子对抗是现代战争中的“ 高效费比兵力倍增器 ”，是增强作战能力的最有效的手段。

(四)现代国防的电子屏障

第二次世界大战以后，世界上虽然没有发生全球性的大战，但各种类型的局部战争和武装冲突此起彼伏，而且都运用着现代科学技术，显示着高新技术的威力，促使战争形式发生重大变化，使电子对抗在战争中的作用日益突出，成为现代国防中不可须臾离开的“电子屏障”。

过去，一提起保卫国防，人们往往想到的只是保卫领土完整，“寸土不让，寸土必争”。这无疑是对的，但从现在看，这种想法不全面。随着高新科技兵器的投入战争和现代作战手段的日益多样化，“陆海空天电”一体战将成为现代战争的重要特征。

所谓“陆海空天电”一体战，是指按照统一的作战目的和计划，在统一指挥下，将地面作战、海域作战、空中作战、外层空间(“天”)作战和电子作战融为一体，旨在全方位、多层次地与敌较量并予以打击。显然，传统的守上意识和狭义的陆疆观念已远远不合时宜。除了“制海权”、“制空权”、“制天权”外，还有“制电(磁)权”。一句话，在现代战争中，要确立“陆、海、空、天、电”一体化的大国防观。可以预测，争夺“制海权”、“制空权”、“制天权”和“制电权”必将成为未来军事、政治、经济斗争的热点。近几年来，世界上发生有较大影响的越南战争、中东战争、马岛战争、黎巴嫩战争以及举世瞩目的、被喻为“2.5 次世界大战”的海湾战争，都从不同侧面、不同程度地说明了这一点。

在世界各国争夺制“陆海空天电”权五大热点中，争夺“制电权”可谓是争夺控制现代战争的“制高点”。这是因为随着电子技术的飞速发展，各种先进武器系统威力的正常发挥，愈来愈依赖于有关电子设备的性能。因此，利用电子对抗这一“软杀伤”手段来削弱乃至摧毁敌方的电子系统，显得十分重要。普通动能和化学能武器在一定时间内往往只能摧毁几个有限的目标，而有效的电子打击却能使敌方的“指挥、控制和通信系统失灵，等于全面地摧毁了敌人营垒中整个武器库”。从某种意义上说，现代战争中能否成功地实施电子对抗和电子反对抗，是取得作战胜利的关键所在。谁夺得了电子战的主动权，谁就能赢得战争的胜利在高科技战争年代，有些外国军事专家提出了“两个作战空间”和“两个战场”的理论。认为在未来的军事对抗空间中，除了陆、海，空、天四维一体化的“地理作战空间”外，还要增加控制电磁频谱的“第五维空间”，而且这个第五维空间将成为其他四维空间的关键纽带。从战场设置观点看，随着第五维空间的出现，将形成两种性质不同、而又交融为一体的战场：一个是包括海、陆、空、天的有形的“地理”战场，另一个是虽看不见，但具有战略意义的“电子战场”。没有“电子战场”的胜利，就没有制电磁权。没有制电磁权，就没有制空权，也就没有海上、陆上乃至太空作战的主动权。海湾战争中，号称“世界第四军事强国”的伊拉克，拥有为数不少的现代化武器，有百万之众的部队，有八年两伊战争作战经验，但由于缺乏精良的电子作战兵器和部队，终于没有逃脱失败的命运。无数事实表明，具有先进、完善的电子作战能力的国家，能在其国土周围筑起一道像火力屏障一样的电子屏障，这是一道坚不可摧的“万里长城”。

为了筑起这座坚不可摧的“长城”，世界各国不借血本投入巨资。有的国家专门成立了电子战协调委员会，对海、陆、空三军电子战实施统一的管

理；为了评估电子战的实战能力，有的国家建立了电子作战效能评估体系；为提高电子战实力，不少国家纷纷增编电子战部队，大力研究开发新型的电子对抗技术和在高技术条件下的电子战战法。随着，电子战“软杀伤”武器性能空前提高，电子战“硬杀伤”武器也取得了突破性进展，这对巩固国防起到了重要作用。

二、电子对抗媒质多

“知己知彼，百战不殆”。这一兵家格言历来力古今中外战争指导者们所重视。在科学技术不发达的时代，为了“知彼”，敌对双方首领通常亲临前线直接观察，或用抓“舌头”、派“细作”等手段收集敌方情报。随着科学技术的日益发展，这种传统的方法逐渐被先进的电子技术设备所代替。现代电子技术侦察、干扰的手段尽管形形色色，但所涉及的是电磁能。因此，都离不开以“三波”为传输媒质——电波、光波和声波。

我们生活在丰富多采的“波”的世界中。白天有阳光照射，黑夜用灯光照明，打开收音机、电视机，对国内外大事可了如指掌。你可知道，这些都有电磁波的功劳。

电磁波是一种在空间传播的交变电磁场。在真空中，电磁波的传播速度为每秒钟 30 万公里，相当于一刹那环绕地球赤道行走了 7 圈半。

电磁波是一个庞大的家族，由光波和无线电波两大族系组成。从物理学观点看，无论是光波还是电波都是一种能量的振动。电磁波在一个周期的振荡时间内(即完成一个波峰和一个波谷所需的时间)所走过的距离，科学术语上叫“波长”；电磁波在一秒钟内完成的振动次数，称作“频率”。波长的单位是米，频率的单位为赫兹(简称赫)，也称为“每秒周”。

电磁波的波长、频率与波的传播速度有着密切关系，可以用以下公式来表示：

$$\text{波长（米）} = \frac{\text{波速（米/秒）}}{\text{频率（赫兹）}}$$

任伺频率的电磁波的波速均为每秒 30 万公里，因此，波长和频率是成反比例的。波长越短的电磁波，它的频率越高；波长越长的电磁波，它的频率越低。

如果按波的波长来排行，在电磁波家族中，无线电波是老大，光波为次子。无线电波的波长较长，光波的波长相形见短。无线电波波长的短边界(毫米波)是和光波波长的长边界(红外光)相连接的。电磁波的分类如图 2-1 所示。

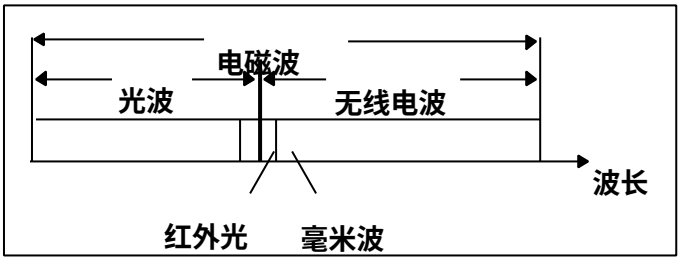


图 2-1 电磁波的分类

声波是一种由物体振动产生的弹性波。但它的振动频率和在介质中传播的速度，要远比电磁波低得多。

人耳被喻为“天生的收音机”，它能感觉到的频率范围在 20 赫兹～20000

赫兹之间，称之为“可听波”。高于这个范围或低于这个范围的为“不可听波”。前者，称超声波；后者，称次声波。

声波在不同的介质中的传播速度是不相同的。例如，在摄氏零度时，声波在空气中的传播速度为每秒 332 米；在水中则为每秒 1450 米左右，约是在空气中传播的 4.5 倍；在铁中的传播速度则更快了，每秒钟大约可达 5850 米。

尽管电波、光波和声波，它们的频率、波长不同，传播速度也不相同，但都可用来作为电子对抗的媒质。因此，电子对抗的种类繁多、形式不一，下面分别分析这“三波”在电子对抗中的具体运用特点。

(一)电　波

无线电波一般指波长由 100000 米到 0.75 毫米的电磁波。根据电磁波传播的特性，又可分为超长波、长波、中波、短波及超短波、微波等 6 个波段，号称“ 电族六姊妹 ”。

无线电波在空间传播，传播方式主要有三种：天波、空间波和地波(表面波)。

天波指受到高空电离层反射或折射后返回地面的无线电波。电离层也叫游离层，是地球上空 40～800 公里高度电离了的气体层。它像一面高悬太空的“ 镜子 ”将来自地面的电波，反射到另一处，传播距离很远。在短波无线电通信中，均用这种传播方式进行远程通信。由于电离层的高度与浓度经常变化，天波传播不 够稳定。图 2-2 是电离层反射电波的示意。

图 2-2 电离层反射电波示意

地波指沿着地球表面传播的无线电波。它不受气候影响，可靠性高，但在传播过程中，由于部分能量要被大地吸收，衰减得比较快，因而传播距离不远。通常长波及中波的无线电通信利用地波传播。图 2-3 是地波传播示意。

空间波，又称直射波。是从发射点经由空间直线传播到接收点的无线电波。空间波传播距离一般限于视距范围。在传播过程中，它的强度减弱很慢。超短波无线电通信和微波无线电通信是利用空间波进行的。图 2-4 是空间波传播示意。

图 2-3　地面波示意

图 2-4　直射波示意

各类无线电波的波长脸主要用途如表 2-1 所示。

表 2-1

波段		波长	频率	主要用途
超长波		100000 — 10000 米	3 — 30 千赫	海上导航，海岸舰艇通信
长　波		10000 — 1000 米	30 — 300 千赫	海上导航，中等距离通信，地下岩层通信
中　波		1000 — 100 米	300 千赫— 3 兆赫	广播，海上导航
短　波		100 — 10 米	3 — 30 兆赫	远距离通信和广播
超短波		10 — 1 米	30 — 300 兆赫	散射通信，流星途迹通信，卫星通信，雷达
微波	分米波	1 — 0.1 米	300 — 3000 兆赫	中小容量微波通信，雷达
	厘米波	10 — 1 厘米	3000 — 30000 兆赫	大容量微波通信，卫星通信，雷达
	毫米波	10 — 1 毫米	3000 — 3000000 兆赫	波导通信，雷达

无线电波虽然看不到、摸不着，但却是客观存在。只要无线电通信设备

一工作，它发射出的无线电波就会立即被电子仪器检测到而暴露无遗。电波这种暴露性就为敌方实施无线电侦察和干扰以可乘之机。通过以上对各类电波传播特性的分析，从电子对抗角度看，“ 电族六姊妹 ”的抗侦察、抗干扰和抗摧毁能力各有千秋。超长波具有穿透海水的能力(一般能穿透 15～30 米深的海水)，特别适合于对水下潜艇的通信，能保证潜艇的隐蔽性。从电波传输观点看具有较强的电子对抗能力。但超长波通信的发射设备，尤其是发射无线的体积非常庞大，在战争中容易遭敌侦察而被摧毁。长波通常用作水下通信和地下岩层通信，具有一定的隐蔽性。但同样存在着通信设施庞大，容易遭敌侦察和摧毁。短波可利用电离层的多次反射，进行远距离通信。由于电离层对电波进行的是泛反射，四而八方都可接收到，保密性较差，电波易被敌方截获。但短波无线电台设备比较简单，易于隐蔽、机动。不像长波、超长波通信那样，容易暴露目标。

超短波和微波具有一些相似的传播特性。号称电波“ 小字辈 ”的微波，因与光波是近邻，能像光线那样沿直线传播，具有很强的方向性，保密性强，稳定性好。但微波绕射能力很弱，一般只能进行视距内的通信。实施长距离通信时，可采用接力传递的方法。就是在地面上每隔一定距离设立一个中继接力站，像运动场上的接力赛跑那样，由中继接力站将上一站发过来的信号接收下来，经过放大、处理后再转发给下一个站，如此辗转相传，将信号遥送远方。也可以将中继接力站由地面搬上天，利用人造卫星进行转发，即卫星通信。由于中继接力站和卫星地球站上的天线高耸地面，暴露目标，容易遭受敌方侦察和破坏。

基于以上分析，不难看出，为了提高通信系统的电子对抗能力，组织与实施无线电通信联络时，应棉据敌我双方态势和作战意图，因地、因时地选用通信方式和电波波长，以保证通信迅速、准确、保密和不间断。

(二)光波

光波是电磁波领域中的重要分支，本身也是一个大家庭，拥有红外光线、可见光线、紫外光线、伦琴射线和丙种射线五个弟兄。

就波长长短而言，红外光线的波长最长，丙种射线的波长最短。具体数值如表 2-2 所示。

表 2-2

分　类	波　长
红外光线	075 毫米～ o76 微米
可见光线	0.76 微米～ 0.4 微米
紫外光线	0.4 微米～ 5000 埃
伦琴射线(X 射线)	5000 埃～ 4 埃
丙种射线(γ射线)	4 埃以下

人们对光波形象的比喻，说是“笔直直，白亮亮，有缝往外钻，想弯弯不了，要割割不断”。这则谜语概括了普通可见光线的一般特性：直线传播、呈现白色。其实，普通光(例如，太阳光)是一种包含有众多频率的复色光(光波的频率不同，颜色也就不一样)。当它经过棱镜分解以后，就大致变成了七种颜色红、橙、黄、绿、蓝、青、紫。其中，红色光波的频率最低、橙色光波次之……紫色光波的频率最高。

红外线是一种人肉眼看不见的光线，由于它在光谱中位于红光之外而得名。细分起来，红外光线有三个波段：

近红外线(靠红光光谱较近的那一部分)0.76～1.5 微米；

远红外线(离红光光谱较远的那一部分)15～750 微米；

中红外线(离红光光谱介于近红外线与远红外线之间)1.5～15 微米。目前红外技术的研究与应用主要集中在近红外与中红外两个波段。

红外线也是一种电磁波，可以用作通信、夜视、制导等，成为电子对抗的重要媒质。在自然界中，凡是温度高于—273℃的物体都有内部分子的运动存在，都会不断地辐射红外线，成为红外线辐射源。红外线的波长与物体的温度有关。物体的温度越高，辐射出的红外线波长就越短；反之，物体的温度越低，辐射出的红外线波长就越长。例如，人体的表面温度约为 32℃，所辐射的红外光峰值波长约为 9.5 微米，汽车发动机机罩的表面温度约为 60～70℃,辐射的红外光峰值波长约为 8.5 微米 ;坦克排气管的表面温度约为 200℃,辐射的红外光峰值波长约为 6 微米(图 2-5 所示是一些常见的军事目标所辐射出的红外光波长)。不过，上述这些红外线辐射源，由于强度微弱，而且能量不集中，不能满足电子对抗的要求。要想利用红外线来传输电子对抗信息必须人为地制造一种强大而集中的辐射源。采用的方法通常有三种：利用物体加热到一定程度产生出红外线，这叫热辐射源：利用在气体和金属蒸气中放电产生出红外线，这叫激发辐射光源(也叫气体放电源)；同时利用热辐射和气体放电产生出红外线，这叫混合型辐射源。

图 2-5—些军事目标的红外光辐射波长

为了探侧和接收红外线，可以采用“ 红外线探侧器 ”。它是由对红外线特别敏感的材料制成，能解调出所载送的信息。在接收过程中，为使所需波段的红外线通过而将不需要的可见光和红外线全部吸收，可以采用“ 红外线滤光器 ”。它是由特种玻璃(或胶体)制成的光学器件，具有很高的滤光比，即可见光完全不能通过，而所需红外线却可通行无阻。

红外线通信机与一般无线电通信机一样，也是由发射机和接收机两大部分组成。前者，让信息去调制红外线辐射源，变成一束束相应的红外线发射出去；后者，将对方送来的红外线还原成信息，从而完成双方通信。为了延长通信距离，提高通信质量，收发双方均应装设红外线滤光器。图 2-6 所示的是左边发信右边收信时的示意。

图 2-6 红外线通信示意

从电子对抗角度看，由于红外线是一种不可见光、但又能像可见光那样集中成很窄的一束发射出去，因此红外线通信具有两个很突出的优点：不容易被人发现和截获，通信保密性强；不容易受到人为等干扰，抗干扰能力强。当用无线电通信怕暴露的场合，使用红外线通信将显示出其无与伦比的优越性。

紫外线也是一种电磁波，可用作通信，成为电子对抗的媒质。和红外线通信一样，紫外线通信也是由发信装置和收信装置两部分组成。由于紫外线频率很高，辐射的波束宽度很小，在抗窃听、抗干扰方面，比红外线通信更具优越性。

伽玛(γ)射线可谓是整个电磁波家族中的“ 频率制高点 ”。它比 X 射线的频率更高，波长更短。据科学预测，利目 γ 射线通信，可以实现 12000～120000 公里的远距离传输，相当于从地球卫星与月球之间的距离，有望成为未来的外层空间的一种通信方式。

本世纪 60 年代，光族中绽放出了一朵奇葩——激光，为信息传递和电子对抗注入了新的生机与活力。说它“ 奇 ”，首先奇在发光原理上。普通人工光和太阳光等都是一种自发辐射出来的光，而激光是一种受激辐射的光，通俗他说，它是被“ 激 ”出来的光。在英语中“ 受激辐射的光放大 ”发音为“ 莱塞 ”，所以激光电叫“ 莱塞 ”。说它“ 奇 ”，还奇在它具有十分特殊的性质：具有极高的光源亮度，其数值甚至比太阳表面的发光亮度还要高 100 亿倍；具有极高的方向性，其光束发散角可以比探照灯光束的发散角小几千倍。举个例子，普通探照灯照到几公里远时，其灯光直径就扩大为几十米，而用激光照射几乎是成一条直线；具有极高的单色性，它只有一种发光频率，是当今世界上颜色最纯的单色光源。说它“ 奇 ”，还在于激光具有奇妙的用途。可以用作通信，其通信容 量之大是当今所有其他通信方式都不能比拟。在理论上，用激光通信可以同时传送 1000 万路电视节目或 100 亿路电话。激光通信的保密件是其他通信手段望尘莫及，因它方向性极强，而且又可采用不可见光，因而很不容易被敌人截获，保密性能好。由于激光束发散角小，方向性好,通信所需的发射天线和接收天线都可以做得很小(一般天线直径为几十厘米)，重量不过几公斤，不容易遭敌侦察和摧毁。

激光武器具有很大的威力，享有“死光”之称。利用高能激光束可以直接熔化、摧毁敌方的电子设备或其他各种设施，是当今电子对抗领域中最强大的打击力量。

(三)声波

声波也是电子对抗的一种媒质，进行“水声对抗”，非它莫属。

我们知道，浩瀚无际的海洋，是一个巨大的导电体，无线电波一旦到了海里，就会立即被海水“吞没”，变得寸步难行。海水对一般的可见光和红外线、紫外线等不可见光，也同样具有很强的吸收作用。“海水不是电磁波的天地”，此话言之有理。

声波在海水中的传播特性和电磁波大不相同。它在海水中的传播速度要比在空气中几乎提高五倍，而且传输时遇到的衰减小，可以传得很远，在深海中，它甚至能横贯海洋，迅速传至海洋之彼岸。

声波在海洋中传播，如同光波在空间中传播一样，也会产生直射、反射、折射、透射、绕射、散射等现象。声波在同一种均匀物质中是直线传播的；遇到两种不同介质(如海面、海底或其他障碍物)时，在其分界面处，就会改变传播方向形成反射和折射(如图 2-7 所示)。声波具有透射特性，即使房舍的门窗关闭，户外的各种声波同样可以传入房内就是这个道理。声波在海洋中传播也存在着透射现象。它在传播道路上如果遇到一种不透声的障碍物，就会像无线电波那样，“爬”过障碍物产生绕射(图 2-8)。因此，在障碍物的另一侧，仍然可以察觉到声的振动。绕射现象是否显著，与障碍物的几何尺寸及声波的波长等有关。实验表明，若障碍物的尺寸远比声波波长小得多，那么声波的绕射现象就

图 2-7　声波的反射和折射

图 2-8 声波的绕射现象

非常显著，反之，绕射现象就不那么明显。有些水声探测设备，就是根据声波这种绕射特性探测水下目标的。声波在浩瀚的大海中传播，免不了要遇到海水气泡、浮游生物、鱼群等东西，部分声能就会向其他方向发散，形成散射。有的散射彼也会返回到发声源产生回波。

本世纪 60 年代初，美国科学家就声波上述特性进行了一次试验：他们在澳大利亚南部海洋，爆炸了当量为 300 梯恩梯炸药，炸药爆发出来的声波，绕过非洲南端的好望角，析向赤道，直奔北美洲。历经近 4 个小时，走了 2 万多公里，最后被设在美国百慕大群岛的水下测听站侦听到。声波的这些奇妙的特性，引起了科学家们极大兴趣，于是出现了水下探测、通信设备——声纳，并随之问世了“声纳对抗”，成为电子对抗的一个分支。

“声纳”就是利用声波在水中传播的特性而制成的，它是由声音、导航和测距三个英文字母的缩写组合而成的，由于它的功能与雷达很相似，故有“水下雷达”之称。声纳探测和搜索目标的原理与蝙蝠相同，也被称为“海中蝙蝠”。·声纳问世于第一次世界大战之中，成熟于第二次世界大战之后。第一次世界大战中，德国首先使用了潜艇，在海上给协约国一方造成了巨大的威胁。曾在不到一个月时间内相继击伤、击沉了协约国近 500 艘舰船。于是，潜艇当时被称之为“海下魔王”。为了对付潜艇对舰船的袭击，大战爆

发后的第二年，出现了“ 水听器 ”，可谓是最早的声纳雏型。

1918 年，世界上第一部军用声纳在法国问世。它借助于刚刚发明的电子管，能将信号进行放大，可探测到近 2 公里远的水下目标，收听到从潜艇反射出的回波。本世纪 60 年代，战场上出现了核潜艇，使得声纳的身价大为上升。因为利用雷达、红外探测器、无线电侦察定位技术和磁探测技术，都无法探测到潜艇的行踪，只有声纳才能担其重任。如今，声纳已成为潜艇战与反潜艇战斗争中的能手，是现代海战中保存自己消灭敌人不可缺少的重要手段之一。

三、电子打击“攻要害”

军队的指挥、控制系统有点类似于人体的结构。通信与雷达好比是人之“耳目”；融指挥、控制、通信与情报于一体的自动化指挥系统(C3I)相当于人之“神经中枢”；精确制导武器，犹如人之“拳头”。如果说，在战争中，整个作战指挥系统是敌方电子打击的重点，那么，通信与雷达、自动化指挥系统、精确制导武器则是敌电子打击的“要害”。穴位是人体的经络枢纽，拳师攻击对手的“要穴”，常会置对手于死地。在战争中，上述三者正是起“要穴”作用。

(一)击敌之“耳目”

“眼有明兮耳有聪，能与千里决雌雄。神机才动情先泄，密计方行事已空。”这是《封神演义》第 90 回开头的一首诗。赞颂的是两个十分神奇的人：一个叫高明，外号“千里眼”，能看千里之远；一个叫高觉，外号“顺风耳”，能听千里之遥。由于他俩有此神通，遂对姜子牙的用兵、布阵一清二楚，结果多次打败号称“所向披靡”的西周军队。迫使姜子牙不得不用“红旗招展”和“锣鼓齐鸣”的办法对他们的视觉和听觉施加干扰，才敢议论军机、运筹帷幄。这当然是一则神话故事。

纵览我国历代兵书，将通信联络喻为军旅中的耳目，早已有之。生活在公元前 6 世纪、号称“中国兵学鼻祖”的孙子，在《孙子兵法》一书中就有“夜战多火鼓，昼战多旌旗，所以变人之耳目也”的记述。《春秋左氏传》中，也有关于“师之耳目，在吾旗鼓进退从之”的论断。然而这些“耳目”都是最简单的声光通信。由于人体生理结构的局限性，人类仅仅借助于自身的耳目传递信息。无疑要受到时空条件的限制。直到上一世纪中叶，人类历史上出现了电话、电报和随后发明了雷达等电气通信工具后，神话中的“千里眼”和“顺风耳”才奇迹般地变成了现实。

无线电通信(简称通信)自诞生的那一天起，就与战争结缘。世界大战的例子暂不说，国内战争的例子几乎俯拾皆是。

1927 年 8 月 1 日，以周恩来为书记的中央前敌委员会和贺龙、叶挺、朱德、刘伯承等人领导的 3 万多北伐军将士，在江西省南昌发动了武装起义，打响了反对同民党反动派的第一枪，开创了中国共产党独立领导武装斗争和创建革命军队的新时期。

参加南昌起义的部队中，大都编有通信分队，使用的主要手段是电话、运动通信和简易信号通信。这些负责通信联络的战士，就是我军最早的通信兵。起义开始前，叶挺领导的第 24 师交通队中的电话分队，在起义总指挥部设立了电话总机，在其他领导人所在地安装了电话机，使总指挥部和各部队之间沟通了电话通信。从 8 月 1 日凌晨两点开始，经过五个多小时的战斗，歼灭了南昌守敌，取得了起义的胜利。我军最早的通信兵为保障起义的作战指挥和各部队之间的协同配合建立了不朽功勋。朱德元帅有诗道，“南昌起义诞新军，喜庆工农始有兵”，其中，也包括有我们通信兵。

随着电子技术的飞速发展和作战样式的不断演变，通信在军队中的使用愈来愈广泛。可以毫不夸张地说，哪里有部队，哪里就有通信兵；哪里有作战行动，哪里就离不开通信兵。上至天空、下至海底，到处都有通信兵的足迹和身影。它已经成为世界各国军队这个复杂机体中不可缺少的神经系统。

军事通信之所以成为敌对双方电子打击的重点目标，是由于它在现代战争中起着其他兵种所起不到的重要作用。

通信联络是保障军队作战指挥的基本手段。纵观中外战史，战争的胜负与通信联络对作战指挥的保障息息相关。苏德战争初期苏军的失败和我志愿军在抗美援朝战争中取得第二次战役的胜利，从反、正两个方面证明了这一点。

1941 年 6 月 22 日拂晓，希特勒指挥德军向苏联发动了大规模的突然袭击，仅仅半个多月时间，前苏联就有近 90 多万人被俘，损失坦克 2500 余辆，大炮 1500 多门，苏联的大片领土迅速沦丧，德军长驱直入，很快兵临莫斯科

城下。苏联为什么败得这么惨？一个关键性的原因，是由于通信联络没有搞好。正像苏联编写的《1941～1945 年苏联伟大卫国战争历史》一书对此总结说，“ 在战争初期，妨碍对我军战争行动进行战役指挥的重要原因之一，是没有总参谋部同各方面军的通信联络，而且也没有各方面军指挥部同所属各集团军的通信联络。 ”

1950 年冬季，我志愿军入朝后的第二次战役打响了。为速战速决，我志愿军参战部队采取了正面进攻与穿插迂回相结合的战术，在前后夹击下，敌军向南溃退。为在运动中消灭敌人，志愿军领导机关当机立断，通过无线电通信信号命令前线部队勇起直追，断敌退路。终于取得了整个战役的全胜。无线电通信在关键时刻起到了关键性的作用。上述两例，从不同角度雄辩地说明了“ 胜由信息通 ”的道理。

通信联络是诸军兵种协同作战的纽带。综观世界风云，协同通信是否顺畅，对现代战争的胜负关系极大。第二次世界大战期间，1944 年 7 月 25 日，举世瞩目的诺曼底登陆战役打响了。为了给登陆部队开辟通路，盟军空军在登陆前沿阵地进行了地毯式轰炸。但由于空中和地面的协同通信不灵，结果，美军轰炸机将重磅炸弹投掷到自己的步兵头上，还当场炸死了一名将军。由于协同通信顺畅而取得胜利的战例当然也是不胜枚举的。

1973 年 10 月 6 月，第四次中东战争开始了。这是埃及和叙利亚两个国家联合反击以色列的一场闪电式作战。参加战斗的有海军、陆军，还有炮兵、坦克、工程兵以及导弹部队，几乎囊括了全部的军兵种。合成程度之高是当时有史以来所罕见，当天下午。埃及先以炮兵打头阵，2500 余门大炮齐轰合击，接着 200 余架飞机升空，对以色列阵地上的主要军事目标进行全面轰炸。在正面战场，埃及以步兵为骨干组成先头部队，在大饱和飞机的掩护下，乘艇横渡苏伊士运河，击毁了河对岸以军的许多坦克。在先头部队的掩护下，4 万多名主力部队随后过河。工程兵迅速架通了浮桥，500 多辆坦克很快过河投入了战斗。与此同时，埃及海军舰艇在多处海域同时向以色列海军开战。在此期间，叙利亚也以空降部队、集群坦克和其他力量联合作战，一举夺取了以军占领的戈兰高地，不到一昼夜，一向被喻为坚不可摧的巴列夫防线很快被突破了。被打得晕头转向的以色列总理梅厄只好连连向美国哀求，“ 救救以色列吧！ ”这次战役获胜的因素固然很多，协同通信搞得好，不失其为一个重要原因。正因为这样，在战役过程中，诸军兵种之间，不但没有误伤，而且配合得十分默契。充分发挥了协同作战的威力，有人把合成作战中的通信联络比喻成“ 粘合剂 ”是很有道理的。

随着高新技术广泛运用于军事领域，未来战争将是诸军兵种参加的，海、陆、空、天、电一齐展开的立体战。协同通信的纽带作用显得尤为必要。在高技术条件下，在诸军兵种合成作战中，不管是哪个军兵种，无论其地位多么重要，所起的作用多么重大，对于作战全局来说，只能是一个局部。协同搞好了，战斗力就会成倍增长，反之就会造成成倍衰减的恶果。

通信联络是军队快速反应的先决条件。“ 兵贵神速 ”，“ 时间就是军队 ”，这些兵家格言道出了一个道理：要夺取作战胜利，必须“ 快 ”。在这“ 快 ”字中，打头阵的是通信联络要快。通信联络不快，信息不灵，指挥员就不能及时决策，上情不能及时下达，下情不能及时上报，部队不能及时展开，武器不能及时运用，一句话，就会贻误战机，被动挨打。在这方面，美国珍珠港被日军偷袭可谓一例。据资料介绍，在日军发动袭击前 12 小时，美军驻东

京的情报部门就已破译了日海军已出发去袭击珍珠港的密码电报。但由于破译等种种原因，这一情报传到美军陆军部时就用了很长时间。陆军部在战前两小时才向太平洋有关基地发出预警电报。但由于军用信道阻断，只好将预警电报送到地方电报局去拍发，开战前 22 分钟，电报才传到夏威夷群岛。

1941 年 12 月 7 日上午 7 时 55 分，日军对停泊在珍珠港的美同太平洋舰队发起了空中袭击，美国巡洋舰、战列舰、驱逐舰和飞机以及大量人员纷纷遭日机击毁、击毙，这时(11 时 45 分)，电报才由夏威夷电信局送到美陆军指挥部。经过一小时的译电和登记，直到下午 3 点，美驻珍珠港指挥官才看到这封电报。但这是日军袭击已基本结束 3 个多小时以后的事了！美军太平洋舰队惨遭灭顶之灾的原因，在很大程度上，是出在通信联络“ 慢 ”这个字上。

在军事科学技术飞速发展的今天，各种新式兵器，特别是战略武器的射程、射速和威力空前增大，军队的机动能力空前提高，战争节奏空前加快，使得未来的战争很可能以闪电般的速度开始，以迅雷不及掩耳之势决出胜负。时间的军事价值比以往任何时候都高。有时信息早来或迟到一刹那，往往会给战争结局带来截然不同的影响。通信联络的快速性将成为作战取胜的关键因素。

通信不仅是己方作战指挥的“ 耳目 ”、协同作战的“ 纽带 ”和快速反应的基础外，通过巧用谋略，还可引敌自相厮杀。这方面的情况，在世界通信史上不乏其例。

早在第二次世界大战期间，一些国家就开始用无线电通信模拟方法实施军事欺骗，造成敌人错觉，乃至牵着敌人的鼻子走，成了敌方的“ 指挥官 ”。据资料记载，1943 年，西西里岛战役期间，德军在获取了美军将向西西里岛空运部队的情报后，便用无线电通信冒充美军基地向美军空运机群发出指令，将美空运机群调集到英美舰队上空 5000 英尺的高度。由于英美舰队刚刚遭到德国航空兵在 5000 英尺高度的轰炸，余惊未消，所以误认为临空的又是德国航空兵。于是，指使炮兵万炮齐发，对临空机群进行猛烈射击。殊不知，搬起炮弹砸了自己的头，庞大的空运机群成了己方舰队的靶子。美国飞行员还不知道是乍回事就一头扎进了大海，惨遭有史以来罕见的厄运。

在中东战争中，利用无线电通信，冒充敌台，以假充真，乱中取胜的事例也有。交战双方都十分重视破译对方的通信密码，不仅是为了获取有价值的军事情报，而且是为了向其通信信道输入假的信息、指令。据有关资料介绍，在第三次中东战争中，以色列破译了埃及的通信密码，然后冒充埃军司令部，用埃及的无线电通信呼号和频率，向所属部队下达作战命令。他们命令埃及军队一支运送弹药和油料的车队，在途中临时改变行驶方向，径直进入以色列的伏击圈。结果，不仅运输车队全部被歼，而且使急需油料补充的坦克部队“ 断水断粮 ”，成了一堆废铁。“ 更令人惊奇的是，他们还直接指挥埃及重炮向自己的部队开炮轰击达 2 小时之久 ”，使其主力损失殆尽。这种利用无线电波进行“ 窝里斗 ”的现象，恐怕是当年赫兹发现电磁波时，所始料不及的。曹操说得好，“ 兵无常势，以诡诈为道。 ”尽管当今世界科学技术空前发达，然而只要有人用诈，就会有人继续上当。

如果说，通信联络因其在战争中的特殊地位和作用，成了敌军的“ 眼中钉 ”，那么，号称“ 国防千里眼 ”的雷达就将成为其“ 肉中刺 ”了。

雷达起家于第二次世界大战初期，当时是为了防空需要而发展起来的。

第一次世界大战后期，飞机对战局影响日趋显著，如何及时、准确地打掉敌机，成了交战双方颇为关注的问题。“雷达”以其拥有一副特殊的“眼睛”登上战争舞台，肩负着国土防空“了望哨”的重任。

有了“远警雷达”能及时察觉企图入侵我领空的敌方飞机和导弹，为领导机关及时制定作战方案提供准确情报。有了“炮瞄雷达”，可及时“抓”到飞临我重要目标上空的敌机，为高射炮兵提供准确的射击目标。有了“制导雷达”可使导弹准确寻的，使其在特定空域击毁来犯的敌机或导弹。

如果将上述种种“地面防空雷达”搬上天，放到飞机上成为“机载雷达”时，则会使它大开眼界、更显神通。据报道，“远程警戒雷达”上天后，可探测 1000 公里远的低空飞行目标，能发现更远的敌机或导弹，为防空系统提供更长的预警时间。

如果让雷达下海，成为“舰载雷达”时，它将成为海军作战的得力助手。“舰载对空警戒雷达”可以使军舰发现几百公里以外来袭之敌机；“舰载对海警戒雷达”，可以发现几千公里以外敌人的军舰；“舰载导航雷达”，可以透过茫茫大雾为军舰充当向导，保证军舰安全航行，神通之大，不胜枚举。雷达在国防，尤其是在防空系统中所起的作用不言而喻。

显而易见，一个主权国家，如果一旦雷达和通信系统遭敌电子打击，就会致盲致瞎。国防安全将受到严重威胁，祖国的领空将任人侵略蹂躏。

(二)击敌之“中枢”

综观古今中外战史，历来的军事行动都离不开有效的组织指挥。从冷兵器时代开始，军队的指挥方式，一直以手工作业为主，在现代战争中，随着高技术武器的发展，这种指挥方式已日益不能满足需要了。

这是因为，现代战争是陆海空天电一体化、多军兵种参战的高度合同化的战争，没有一套灵敏有效的自动化指挥系统，就难以进行战场兵力协调和合同作战，就难以使各种各样的兵器发挥其整体作战效能。现代战争中，随着新式兵器的广泛使用，使得作战反应时间大为缩短。一枚飞行上万公里的洲际导弹从发射到击中目标，只需不到 30 分钟的时间。为了捕捉稍纵即逝的战机，交战双方都需要迅速地作出反应，没有一套高度自动化的指挥系统是难以完成这种任务的。

图 3-1 所示的是作战指挥过程框图。所谓指挥，指的是为实现某一目标，了解和掌握与实现这一目标有关的各方面情况，并对所掌握的各方面情况进行科学地、全面地分析和判断，然后制定出实现这一目标的行动计划(方案)，并组织、管理实现这一目标的各个机构和各类人员，使其在实现计划的过程中充分发挥各自的作用。概率统计表明，用手工作业方式实施指挥，收集情报速度慢而且不全，只能处理获取情报的 30%以下，而真正送到指挥官手中供决策的情报，还不到 10%。有了先进的指挥自动化系统，情况就大不一样。

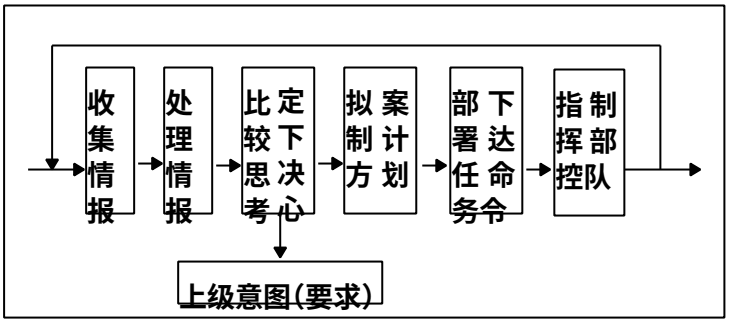


图 3-1 作战指挥过程框图

自动化指挥系统广泛应用了运筹学、控制论、信息论、电子学、系统工程等有关学科的研究成果，以电子计算机为核心，使指挥(commad)、控制(control)、通信(communicatlon)和情报(Intelligence)融为一体。因为指挥、控制和通信三个英文单词的第一个字母都是 C，简称 C^3；情报的英文单词第一个字母是 i，合称 C^3I 系统。它之所以不称之为 3CI，是由于它们经有机组合以后能起倍增作用，被誉为“兵力倍增器”。在国外，也有人把指挥、控制、通信与情报说成是“胶”(gule)，意思是说它把军事力量粘合在一起，因此，也称 C3I 系统是现代战争的“粘合剂”。

C^3I 系统的问世，实现了信息收集、传递、处理的自动化，以及决策方法的科学化。它把指挥、参谋人员从大量的、繁琐的事务性劳动中解脱出来，以便集中精力从事创造性的指挥活动。

军队指挥自动化系统，是在历史进程中逐步发展起来的。它的雏型是 1958 年美国建立的第一个半自动地面防空指挥控制系统——“赛其(SAGE)”

(前苏联差不多在同时也建立了“天空 1 号”半自动防空指挥系统)。“赛其”系统是为北美联合防空指挥部提供的半自动化作战指挥系统。这个系统可以自动搜集、处理、传输和显示关于北美地区的空中情况、指挥部下属部队的武器状况和战备方面的信息。它还可以自动提供选择拦截武器和部队的方案，发出对防空导弹和战斗机的指示。“赛其”系统除了自动收集本系统内各雷达站的情报外，还获取与其相连接的其他系统的情报。计算出用各种防空力量打击被发现目标的多种方案，供指挥员选择。有了这套指挥、控制系统可以使指挥员随时掌握敌我双方的情况，及时地作出正确的判断，并使部队能够迅速作出反应。

“赛其”系统能实施作战指挥与作战控制，可谓之 C^2 系统；60 年代以后，通信作为指挥与控制的纽带，显示出它至关重要的作用，使 C2 系统发展成了 C^3 系统；70 年代以后，情报(信息)的作用日益显著(因为无论指挥、控制和通信都离不开信息)，在 C^3 系统中又增加了情报(I)，演变成了 C3I 系统。如今，C^3I 系统涉及战略、战役和战术各个层次，遍布海军、空军、陆军和战略火箭部队(图 3-2)，成为现代战争中作战指挥的神经中枢，它把军队的快速反应能力、协同作战能力、电子战能力、野战生存能力和后勤保障能力，提高到前所未有的高度。C^3I 系统的建立被军事专家们视为“是继核武器之后，军事上的‘第三次革命’”。

图 3-2 各种类型的 C^3I 系统

然而，任何一个 C^3I 系统，不论是战略的、战役的，还是战术的；也不管它是为哪个军兵种服务的，都是由下列三个基本部分组成的：

——侦察探测系统

——指挥系统

——通信系统

图 3-3 C^3I 系统的简化模型

侦察探测系统负责搜集有关敌方的各种情报，是为 C3I 系统提供源源不断的信息源。侦察探测系统获取情报信息，有多种渠道，有各种分系统。其中，包括飞机和巡航导弹的探测分系统(主要有地面雷达、飞机、气球和舰载雷达、观察哨等)；弹道导弹和间谍卫星探测分系统(主要有雷达、预警卫星等)；地面(海面)侦察分系统(主要有雷达、照相、侦察船、观察哨等)以及水下探测分系统(主要包括声纳、光学探测等)等。

指挥系统负责汇集、处理和显示敌我双方的各种情报、态势、威胁力量的分析，进行判断决策。它主要包括计算机处理分系统、显示和控制分系统、数据库分系统

(图 3-4)以及文字处理分系统等。

通信系统用来传递情报和命令，由信源、信道、信宿以及交换设备等组成。信源和信宿合称为终端设备。借助于终端设备、交换设备和传输设备能组成各种类型的通信网络。有战略通信网、战役战区通信网和战术通信网等。

像人体的神经系统那样遍布 C3I 系统的各个角落。

C^3I 系统依靠上述三大组成部分可以实现下列六种功能：

信息搜集功能。此功能由侦察探测系统提供。

信息传递功能。此功能由通信系统提供。

信息处理功能。此功能由电子计算机完成。旨在对输入电子计算机内的各种信息自动进行综合、分类和运算，并能进行军事运筹，协助指挥人员拟制各种作战计划和对各种方案进行模拟、评估和选优。

信息显示功能。旨在以各种字符、表格和图象等形式，为指挥人员、参谋人员提供形象直观的情况，供指挥、参谋人员使用。

决策监控功能。主要是根据各种信息状况，评估出敌我发展态势并根据预定目标采取相应的对策。在武器控制上，可以按预定方案实施自动决策控制。

执行检查功能。主要任务是将命令信息付诸实施，转换成行动。下属部队执行命令情况以及武器的打击效果，又能通过信息搜集分系统实时地收集上来，以供指挥人员进行检查、纠正。

在上述六项功能中，几乎每一项都离不开信息。高技术战争在一定意义上说，也可以叫“信息化战争”(因为在高技术群体中，核心是信息技术)，而 C3I 系统正是高技术战的中枢神经。一旦主体受损，就会造成群龙无首，肢身解体。正因为这样，在激烈的电于对抗中，交战双方总是将电子打击的矛头指向敌方的 C3I 系统。它们深知“干扰敌方雷达”，只能说是消灭敌人一种武器，干扰了自动化指挥系统，则是毁灭了敌人营垒中的整个武器库。没有自动化指挥系统的军队，只能是一个麻木的白痴；没有自动化指挥系统的武器，就将是一堆废铁。近几年来，有不少战例，从正反两个方面对此提供了论证。

1982 年 5 月，英国和阿根廷之间爆发了一场旨在争夺马尔维纳斯群岛的战争。论兵力，双方相差不多；论武器，双方几乎不分上下；论天时和地利，完全有利于阿根廷。马尔维纳斯群岛距离英国本土约 14000 公里，离阿根廷大陆却只有 560 多公里。可以说，英军是劳师远征，而阿军则以逸待劳。然而，战争却以英胜阿败而告终。究其原因，英军具有先进的 C3I 系统，能实施自动化程度很高的指挥，是致胜的一个关键因素，马尔维纳斯群岛不在英国军事通信卫星的覆盖区以内，但英国取得美国同意，租用了美国的国防卫星通信系统，形成了一套比较完整的 C3I 网络。借助于它，英军统帅部在英国本土能与万里之遥的每艘舰艇沟通联络；足不出户，就能通过大屏幕显示，对战场情况了如指掌。因而极大地扩展了耳目，牢牢地掌握了战场的主动权。

与此相反，阿根廷由于没有先进的 C3I 系统，信息不灵，三军情报不能共享，作战时各军兵种“锣齐鼓不齐”，形似一盘散沙。

英军统帅部以 C3I 系统为依托，直接指挥近 14000 公里远的英国潜艇，一举击沉了拥有现代化武器装备的阿根廷“贝尔格拉诺夫将军号”巡洋舰，开创了世界海战史上的成功先例。难怪人们将 C3I 系统奉为打赢现代战争的“灵丹妙药”，誉其为高技术战争中的“效率之神”。有了先进的指挥自动化系统，真正做到了我国古语所说的，“运筹帷幄之中，决胜千里之外”。

1982 年 6 月 9 日，以色列和叙利亚在贝卡谷地打了一场闪电式空战。交战前，以色列和叙利亚曾多次“对火”，终因实力相当难分胜负。为了改变战局，在贝卡谷地之战中，以色列引进了美国制造的 E-2C“鹰眼”预警飞机

作为战场 C^3I 系统的指挥中心。它具有一些“特异功能”：能自始至终随时随地鸟瞰整个战场情况；能指挥无人驾驶飞机用 15 倍的可变焦距电视摄像机，以每秒拍摄 50 幅图象的速度，摄下叙利亚军队阵地的兵力兵器状况；能让无人驾驶飞机“乔装打扮”，模拟战斗机，诱使叙利亚雷达开机，以便掌握叙军雷达网的配置情况和雷达的技术参数，然后利用电磁辐射将其摧毁；能调动各类电子干扰设备，对叙军的雷达和通信系统实施高强度的压制性干扰，造成叙军指挥失灵。以色列凭借其拥有的 C3I 系统，仅用 5 分多钟，就摧毁了叙利亚 19 个“萨姆—6”地对空导弹阵地，重创了叙大量兵器，击毁叙军飞机 80 余架，而以色列自己仅损失了一架 F-4G 飞机和一架直升飞机。叙利亚几乎没有交上火就一败涂地。

上述两例中，一个是海战，一个是空战，但它们“异曲同工”，谁拥有 C^3I 系统，谁就能赢得战争胜利。

至于说到海湾战争，C^3I 系统更是大显身手出尽风头。我们知道，海湾战争是一场多国家、多军兵种参战的战争。战争中飞机种类之多，武器种类之广，都是近几年来历次局部战争所没有的。在陆、海、空一体化的战争中，如何协同各参战国、诸军兵种的作战行动，形成一种密切配合、运转灵活、指挥有序的整体打击力量，是制胜的一个关键因素。这个庞大的复杂的战区指挥核心，就是海湾地区的 C^3I 系统。

海湾开战的头一天，就有美、英、法等七八个国家的飞机，从数十个机场和航空母舰上起飞，出动 1300 多架次，集中对伊拉克上千个目标实施高密集、高强度的狂轰烂炸。这么多机群，又是在无月的黑夜进行出击的，再加上指挥、协同上的语言障碍，要想有序、准确、高效地实现作战计划，困难是可想而知的。但以美国为首的多国部队依靠了先进的 C^3I 系统，实现了高度自动化的协同引导，达到了战役行动的预期目的。据报称，美国运用完善的全球性战略 C^3I 系统，能在 1 分钟内使所有战略进攻力量处于戒备状态。美总统的作战命令从白宫传递到遥隔万里的海湾地区只需 1～3 分钟,因而保证了对战区的实时、快速的指挥与控制，保证了大规模、多方向、诸军(兵)种协调一致的行动，使近百万多国大军联结成一个统一的整体，形成一股强大的攻击力，终于夺取了战争的胜利。

这些战争实践，使人们越来越对 C^3I 系统刮目相看。在军事界，过去一直认为枪炮、炸弹、坦克、飞机、军舰和导弹等这些大规模的硬杀伤武器是衡量战斗力的唯一标准，现在则不得不承认 C3I 系统是国防实力的关键因素，是战争致胜的法宝。

C^3I 系统的特殊地位与作用，在战争中自体会成为敌方电子打击和火力摧毁的首要目标。一旦 C^3I 系统失效，就可能造成部队失控，以至于陷入自己打自己的灾难性局面。此时，C^3I 系统不仅不是“兵力倍增器”，反倒成为“兵力倍减器”了。所以，在发展 C^3I 系统的同时，必须要研究保护 C^3I 系统和对 C^3I 系统进行反对抗的必要措施，才能使它真正发挥作用。

(三)击敌之“拳头”

随着高新技术的发展和其广泛地被运用于军事领域，进入 70 年代以来，在世界现代武器库中，“一代天骄”——精确制导武器异军突起，成为现代战场上众多高技术兵器中的佼佼者。

精确制导武器最早出现在第二次世界大战的后期,闻名于 1972 年的越南战场上。那时，美越战争已接近尾声，美国运用一种“聪明炸弹”在很短时间内，使越南北方 100 多座桥梁毁于瞬间。从此，精确制导武器登上了战争舞台，并且以超远距、全天候、强突防、高命中率的优势，独领风骚，成为“战争”中打击敌方有生力量的一个强劲的“拳头”。国外军事专家认为，“精确制导武器很有可能使战争发生革命”，将成为“未来兵器之星”，甚至认为它的发展“比第二次世界大战爆发时启用雷达的意义还要大”。

顾名思义，制导武器是指按照特定基准选择飞行路线，控“制”和引“导”它对目标进行攻击的武器。我们知道，世上各种目标的物理表征是各不相同的。精确制导武器正是通过自身装备的探测器、传感器等“耳、目”，自动进行精确寻的、跟踪并制导。这一过程，科学术语上称之为“制导”。

有人说，“导弹，导弹，无导不能战”。这句话很有道理，因为导弹的关键就在这个“导”字上。通俗他说，“导弹”就是一种可制导的炮弹。正是这个“导”字，它与电子计算机、通信、雷达发生了密切关系。

图 3-5 所示的是导弹在雷达、计算机精确控制下，腾空拦截敌方来袭导弹的情况。当来袭导弹飞向我空域时，很快被我方的地面警戒雷达发现，并测算出它的飞行高度和飞行速度。雷达将这些数据输入电子计算机，经电子计算机运算后，指挥导弹发射架于特定时刻，将拦截导弹推向空中，控制它在适当位置将来袭导弹打掉。

图 3-5 用导弹打导弹示意

图 3-6 所示的是制导武器用于自动化防空系统的实例。它是一种专门用来对付来袭导弹或其他高速飞行器的自动控制系统。该系统从目标的发现、跟踪、识别，到目标参数测定、威胁预测，直到己方武器的发射、引导等全部过程都是自动进行的。其具体工作过程是：由预警系统的远程预警雷达(作用距离几千公里以上)捕获远方来袭导弹或高速飞行器的情报,并迅速将情报传输给计算机中心，然后对目标进行跟踪并随之发出跟踪指令，最后发出截击来袭目标的指令，由引导雷达控制导弹击落来袭目标

图 3-6 自动化防空系统工作示意

导弹升空后，之所以能按预定航迹飞向目标，是由于它身上有一套精密准确的制导系统。这套系统中有两只“千里眼”(学名叫传感器或探测器)，能及时获取目标信息，并具有很高的分辨率。它有一个神奇的“大脑”，能对侦察和探测到的大量目标信息进行实时处理，迅速“拍板”。或根据导弹实际航迹和理论航迹的差别，通过自我调节，不失时机地修正导弹的航迹，以允许的误差接近和命中所要攻击的目标，直至将目标击毁。由此看来，没有制“导”，就没有“导弹”。

精确制导武器尽管种类繁多，包括雷达制导型、红外制导型、激光制导型、电视制导型、地形匹配制导型以及复合制导型等，但其控制和引导部分都离不开电子设备。而且制导精度愈高，对电子技术的依赖性愈大。正如一些军事评论家说的，“导弹本身并不复杂，它的神秘之处就是那个电子‘黑盒子’”，从发现目标到完成攻击使命的整个过程，都是靠精密电子系统控制的。正因为这样，精确制导武器中的电子系统，必然要受到敌方的电子打击。正像日本军事评论家藤井治夫指出的，“电子设备是精确制导武器的灵魂，而电子战是对付精确制导武器的最有效的手段。”第二次世界大战后，世界上发生的几次局部战争中，不少正反事例，都证明了藤井治夫的观点是正确的。

越南战争初期，为对付美国空袭，越南广泛使用了“萨姆-2 地空导弹”。一开始，越方导弹由于未受到美军的电子干扰，命中概率很高。平均每发射 10～15 枚“萨姆-2 地空导弹”就可击落一架美机。后来由于美军对它采取了电子干扰，萨姆导弹平均每发射 66 枚才能击落一架美国飞机。命中率由开战初期的 1%骤然下降至 15‰。

在中东战争中，也有类似的事例。第三次中东战争期间，埃及使用“冥河反舰导弹”袭击以色列的军舰和商船。在以色列未采取电子对抗的情况下，六发六中，取得了击沉以方一艘驱逐舰和两艘商船的重大战果。然而，时隔不久，到了第四次中东战争时，阿拉伯国家总共向以色列舰艇先后发射了 50 余枚冥河导弹，由于受到了以方的有效电子干扰，竟无一命中。相反的，以色列侦察到阿拉伯国家的舰艇未加抗干扰设施，随即使用“迦伯列导弹”对其发动攻击，一举击沉了埃及、叙利亚 12 艘导弹艇，使阿拉伯国家遭受了重大损失。

透过上述事例，无怪有人打了个比喻：精确制导武器好像一个拳击手的拳头。如果拳击手有眼无珠——精确制导武器的传感器受干扰而迷盲，或大脑和神经失常——精确制导武器的指令系统瘫痪，哪里还能出击呢？

四、电子角逐“三部曲”

人类自有战争以来，每当一种新的武器装备和作战技术的出现，与之相对抗的手段必然相继产生。攻防互寓，矛盾相制，此乃规律。号称“第四维战争”的电子战也不例外。

对敌方电磁源进行搜索、截获、识别和定位，进而查明其电子设备的技术性能，用电磁波进行扰乱或将其摧毁，此为“电子进攻”。“电子防御”则是指在敌方实施电子对抗的情况下，为保障己方电子设备和系统发挥效能而采取的措施和行动。于是，电子侦察与反侦察、干扰与反干扰、摧毁与反摧毁就构成了电子对抗的有机组成部分，成为密切相关的“三部曲”。

(一)侦察与反侦察

电子侦察是电子对抗的基础，是“知彼”的一种妙法。只有侦察到了对方电子设备的工作状况，才能有的放矢地进行电子干 扰和予以摧毁。

“电子侦察”通俗地说，是指使用各种电子侦察装置探明敌方电子系统并测定其各种参数。

衡量电子侦察的工作状况，主要有以下一些指标：

侦察概率——即在一定照射次数条件下，电子侦察设备截获敌方电子设备信号的概率。它主要包括两个部分：一是天线的截获概率，也叫方位截获概率。即侦察无线波束与被侦察电子设备的天线波束相遇的概率；二是侦察接收机的截获概率，也叫频率截获概率。即在照射时间内接收机选通所侦察信号的概率。从总体上说，侦察概率应越大越好。

侦察时间——指从欲截获被侦察目标的信号起，到侦察接收机指示和测定该信号参数所需要的时间。侦察时间应越短越好。

侦察距离——全称侦察作用距离。是指侦察设备能够接收和分析被侦察目标的信号的最大距离。

侦察的作用距离与很多因素有关，主要有：被侦察设备的无线辐射功率和增益、侦察天线的有效接收面积以及侦察接收机的灵敏度等。被侦察设备的天线辐射功率愈大，被侦察设备的天线增益愈高；侦察天线的有效接收面积愈大，侦察接收机的灵敏度愈高，侦察的作用距离也就愈远。我们要求，侦察的作用距离应越远越好。

电子侦察分“电子技术侦察”和“电子情报侦察”两大类。电子技术侦察，有的资料上也叫电子支援措施。

“电子技术侦察”，是指利用侦察设备详细查明敌方电子设备的技术性能，如雷达的工作体制、频率、脉冲宽度、脉冲重复频率、无线转速等技术参数，以及查明敌方电子设备的类别、数量、配置地点和变动情况，为制定己方干扰对策和研制电子干扰设备提供技术依据。后者，是指利用电子侦察设备从电子信号中，提取所传递的军事情报内容，以求获得敌方武器系统的配置、编制及行动企图等军事情报。

通信和雷达是电子侦察的主要目标，相应的有“通信侦察”和“雷达侦察”两种。通信侦察旨在侦听敌方各种通信和指挥联络信号，把敌方的通信密码、暗语及其他信息记录下来加以分析和破译；雷达侦察是为了捕捉敌方雷达信号“指纹”或特征，包括获取雷达设备的性能、用途和配置等情报。

无论是通信侦察还是雷达侦察，按实施电子侦察的时机来分，有预先侦察和实时侦察两种。预先侦察也称经常性的战前侦察。是指战前对敌方电子设备所进行的长期的或定期的侦察。其目的在于预先全面掌握敌方电子设备的有关情报及其发展动向，为全面制定电子对抗对策和实施直接侦察提供依据。

直接侦察是在战役、战斗发起前夕，或在其实施过程中，对战场电磁环境所进行的实时侦察，为电子对抗提供实时可靠的依据。

由于空间存在着大量的电磁波信号，要想在浩瀚无际的“波”海中筛选出有侦察价值的信号，犹如大海捞针，十分困难。随着侦察技术日益先进，这些困难已逐步迎刃而解。

1.形形色色的“侦察兵”

“电子侦察兵”是一个人口众多的庞大家族。根据它们的工作地点，分“地”、“空”和“天”三大族系。

地面侦察雷达(也叫战场监视雷达)早目前“地族”侦察雷达的代表人物。共有弟兄三个。老大叫“远程地面侦察雷达”，可以探测 20 多公里远的目标。由于块头大，体重 200 余公斤，总是乘车执行任务，别名叫“车载侦察兵”。老二叫“中程地面侦察雷达”，可以探测 10 公里左右远的目标，体重仅为大哥的 1/5，执行任务时可以乘车，也可由人背负。“近程侦察雷达”是小三的学名。它只能探测 3 至 5 公里远的目标，但个头小，体重轻，单兵就能携带。这哥儿仨，虽然个头相差很大，但都具有较高的侦察本领，能在雨、雪、雾、霾和夜暗等能见度不良的条件下进行侦察，可谓是名“全天候、全天时”的侦察兵。此外，它们探测精度高，尤其对探测运动中物体更拿手，所以一经问世，就受到部队青睐，广泛服役在各国军队的地面侦察分队、边防哨所以及观察站等处。

各式各样的电于侦察飞机(图 4-l 至 4-4)是侦察“空”族的代表。它们具有奇特的远视能力，能发现离它几百公里乃至几千公里以外的目标。

电子侦察飞机从机头到机尾，以及机身、机腹和两个翅膀的附近都装有天线(如图 4-5 所示)，可以全方位地侦察目标。

侦察飞机具有高度优势，居高临下。据测算，假设其飞行高度是 9000 米，那么，在以飞机为中心，方圆 400 公里之内的各种电磁信号，都能被它侦察接收。如果侦察飞机的飞行速度每小时为 800 公里，那么，一个小时就能侦察完 64 万平方公里之内的各

图 4-1　低空电子爬山察飞机

图 4-2 高空电子侦察飞机

种电磁信号。其本领之高强，是任何地面侦察站所无法比拟的。

在先进的电子侦察飞讥的机舱里，不仅装有先进的全波段通信侦察设备和全波段雷达侦察设备，还装有自卫时必不可少的电子干扰设备以及录音、照相、录像设备等。可以多手段的截收、处理敌方的无线电信号，为火力摧毁和电子干扰敌电子设备提供战斗诸元。

各种各样的空间侦察卫星，是侦察系统“天族”的代表。主要成员有：

图 4-3　无人侦察飞机

图 4-4　有人侦察飞机

图 4-5　侦察飞机上的天线

电子侦察卫星(图 4-6)——星体中安装有无线电侦察接收机，无线伸出星外。主要用来侦察敌方雷达和窃听通信。能把侦察接收到的敌方各种无线电信号记录并存储起来，用两种方法传回地面。一是“边侦边传”。在侦察到敌方无线电信号的同时，不延迟地迅即将它转发给自己的卫星地面站。另是“先侦后传”。将侦察到的电磁信号先存起来，等卫星运行到己方上方时，将信号发放给自己的卫星地面站。

图 4-6　电子侦察卫星

照相侦察卫星(图 4-7)——卫星中装有照相机，能大面积的

图 4-7　照相侦察卫星

拍摄地面物体，或用无线电波将所摄内容传回地面；或让卫星完成拍摄任务后立即返回地面。新型的照相侦察卫星具有很高的分辨力。据载，美国一种照相侦察卫星，从 150 公里高空，能分辨出地面一尺大小的物体，享有“飞行显微镜”之称。

预警卫星(图 4-8)——预警卫星的侦察手段很多，图 4-8 所示的是用红外望远镜作探测器的预警卫星的外形。它能在低温条件下工作，对一定波长的红外辐射非常敏感。

在侦察家族中，“航天侦察”是“后生”，迄今刚过“而立”之年。但它本领超群，大有独占鳌头之势。侦察卫 星最突出的特点是：侦察面 积大，侦察速度快。照相侦 察卫星能把比我国台湾省面 积还大的地面拍在一张照片 上。电子侦察卫星可以侦察 截收半径约为 3000 公里的圆形地区内的无线电信号。它们每天绕地球飞行十多圈。高速完成侦察任务非它们莫属。

图 4-8　预警卫星示意

2.五花八门的侦察方式

截收敌方无线电信号，对敌方无线电信号进行检测分析，测定敌方电台的方位；发现带有雷达的目标，测定雷达的参数，确定雷达的类型和用途，引导雷达干扰机工作等、这是通信侦察和雷达侦察的基本任务。根据这些任务，电子侦察通常有下列一些方法。

侦察方式
- 窃听
- 侦视
- 侦听
- 遥感
- 无源雷达侦察
- 测向定位
- ……

窃听通过窃听对方传输的信号获得情报信息，这是早期的电子侦察的主要手段之一。由于它比较简单，至今仍在战争中运用。

窃听电话是窃听技术应用的一个重要方面。通常有两种窃听方法：一是将装有微型无线电台的窃听器安装在电话机的附近，它能将用户讲话的声音原原本本地变成无线电波向室外发射出去。窃听者只要用一台收音机就能听得一清二楚。另是将窃听器安装在电话线附近(图 4-9)，或采取偷梁换柱等方法，将窃听器直接安装在电话线的杆上(图 4-10)。如有的将窃听器制成形似电线杆上的瓷瓶，以假换真，不易被人发现。当线路上通过话音电流时，就会在导线上诱起人眼察觉不到的电磁场。电磁场被窃听器感受后，随即转换成无线电波发射出去。窃听者用无线电接收机接收

图 4-9　利用窃听线窃听电话

图 4-10 将窃听器装在电线杆上

后，就能听到通话内容。这种室外窃听器用太阳能供电，几乎能全天候工作。因为通信线路上辐射出的电磁波能扩散很远距离，不仅在线路附近能窃听到信号，在离线路较远的金属体上(如晒衣服的铁丝、房屋的铁栏杆以及铁路铁轨等)也会产生感应电势，如果将窃听器安装在它的附近，有时也能听到。

普通明线电话容易被窃听，现在广泛使用的载波电话也不例外。因为不论何种程式的载波机，只是将话音频率人为地进行了搬移。只要通过一种设备进行反搬移，照样能听清通话内容。据刊物介绍，有些窃听者将窃听设备安装在汽车上，把窃听器的接收天线伸出车外，汽车沿着电话线附近的路上来回行驶，表面看跟正常行驶没有两样，实则是进行窃听。有的外国人装扮成来华访问的记者或旅游者的模样，经常在黄昏时分驱车到有电话线的一带欣赏自然景色，举起照相机拍摄黄昏风光。其实在照相机和他的提包中藏有一种微型窃听器，进行窃听活动。

由于众多的电话线架设在同一电杆上或裹装在同一电缆内，相互间就会产生电气影响，形成“串音”，就是打电话时，能清清楚楚地听到第三者讲话的声音。有些窃听者正是利用这种串音现象进行窃听。他们不时地拿起电话机装出打电话的模样，其实，打电话是假，窃听电话是真。

电话是日常生活中使用最多的通信工具，窃听电话几乎有了一个多世纪的历史，如今电话窃听术又有了新招，简直使人往往难以置信。据报载，国外常常有这样的情况：自动电话铃声响了，当用户刚拿起电话手机准备对话的时候，对方却彬彬有礼他说了声，“对不起，拨错号了。”殊不知，就是当用户将电话手机一拿一放时，就已经中了窃听者的圈套。原来，窃听者使用了一种特殊的窃听技术，在用户放下电话后，他的讲话声音照样能源源不断地送到了窃听者的耳中。

随着电子器件日益小型化和微型化，窃听器除用于窃听“电话”外，更多的是直接进行窃听“谈话”。目前，各式各样的小巧玲珑的窃听器，琳琅满目。发展的趋势可以概括成：伪装、隐藏、高效和光测四个方面。

为了不被人察觉，有的将窃听器伪装成钮扣、戒指、手表、打火机的样

子，有的将窃听器安装在钢笔、耳环、发卡、眼镜、假牙甚至苍蝇身上。据有关资料报道，为了窃获敌国的军事情报，窃听者将苍蝇通过门锁的钥匙孔，放进正在研究作战计划的房间内，充当“奸细”。为了避免苍蝇飞动时的嗡嗡声对窃听器工作的干扰和遭到拍打，在苍蝇执行任务前，给它服上毒药，使其进入房间后很快死掉，但并不影响窃听器正常工作。1945 年，第二次世界大战结束以后，前苏联为感谢美国在打败法西斯德国的胜利所给予的巨大军事和经济援助，向美国驻前苏大使馆赠送了一件非常精美华贵的礼物——美国国徽。美国大使将其悬挂在办公室墙上。但是他万万没有想到，在这个国徽内安装了一只窃听器，使前苏联掌握了美国许许多多军事、政治、经济和外交情报。这件“珍贵的礼物”在美驻前苏使馆一直呆了八年，1952 年才被美发现。窃听时间之长，实属历史上罕见。

现今的窃听器，灵敏度非常高。据测试推算，像在北京市最喧杂、最繁华的王府井大街，可以隔着马路窃听到对面办公室里人们谈话甚至伏案写字的声音。

激光的问世，使得窃听变得更隐蔽。我们知道，声音是由物体振动产生，这种振动又会引起邻近一些固体物质(例如玻璃)产生微小振动。当然，这种微小的振动，靠人眼是根本察觉不出来的，但可以被激光发现。窃听者只要在玻璃上投射一束细如头发丝的激光束，由声音驱使的玻璃振动，就会引起激光束发生相应的变化，通过一定的检测装置，就可把光波的变化演变成声音。由于激光束是不可见的，可以做到高度秘密。这种新颖别致的窃听方法，令人防不胜防。

随着电子抗争日益白热化，窃听方法已由“悄悄进行”逐步转向“明火执仗”。“窃听子弹”可谓是其中的一术。“窃听子弹”的弹头中装有一只微型高效拾音器和一部微型无线电台，它可以用普通的枪枝射击出去，射入敌方指挥部的墙内、屋顶上，或者落在指挥部附近。依靠其上的拾音器和无线电台就能将敌军指挥人员的谈话，转换成相应的无线电波发射出去，己方人员通过无线电接收机就能及时听到敌方指挥人员的谈话声音。

窃视随着电子技术的发展，电视侦察应运而生。号称“战争之神”的火炮，不仅是杀伤敌方有生力量的武器，而且已成了一名新奇的“侦察兵”。新近问世的“电视炮弹”就是其中的一员。

电视炮弹上装有一台小小的摄像机和一台微型的无线电波发射机，实际上好比是一座小巧玲珑的电视台。两军对阵时，一方将“电视炮弹”像照明弹一样，发射到敌方上空。弹头炸开后，悬挂着微型降落伞的“炮弹电视台”慢慢降落。在落地过程中，其上的电视摄像机鸟瞰敌方阵地，及时拍下阵地状况，并用无线电发射机将摄下的图象迅即发射回来。这时，己方指挥所可用电视接收机收视“电视炮弹”送回来的图象，对敌方阵地的兵力、兵器部署以及通信设施情况一目了然。如果在“电视炮弹”中再配装上一只高灵敏度的微型拾音器，还可同时传回有关敌方阵地的声音信息。可谓是既窃听又窃视，耳目并用。

侦听或叫监听，亦即通信情报侦察，是常用的侦察手段之一。各种电子侦听站肩负着这一使命。

通过无线电侦听，可以及时获取敌方部队的部署、调遣和作战意图。这方面的战例几乎比比皆是。在第一次反“围剿”胜利以后，

1931 年 2 月，蒋介石命令何应钦率领 20 万人马，采取“步步为营、分

进合击”的战略，向我红军发动了第二次“围剿”。毛主席、朱总司令要求我无线电台人员高度集中精力，侦听敌人的行踪。5 月 15 日黄昏，我电台截获到国民党军公秉藩师部发给该师留守处的电报：“明日出发到东固。”(当时国民党军没有想到红军会有电台，在发报中毫无顾忌地使用明码，无所不谈)电台人员马上把这份电报送到红军总部，我军立即给敌人布下了“大口袋”。

16 日，第二次反“围剿”的第一仗打响了，当日下午，敌公秉藩师全部被歼。战斗结束后，朱总司令热情称赞了电台工作的同志。第三次反“围剿”前，我红三军电台人员截获到敌总指挥何应钦发给各路部队的电报。根据电报内容，我军迅速作好作战部署，为反“围剿”的胜利起到了重要作用。毛主席在接见红三军电台干部时说：你们侦听到的何应钦的那份电报，对这次战役胜利很有价值。

侦听在国外军队用得也很多。第二次世界大战期间，1943 年，美军电台侦收到了日军的无线电报，经过破译，得知日本海军总司令山本五十六及其参谋部的高级军官，将于 4 月 18 日飞抵达布于维尔岛。

18 日，美军派出了 18 架飞机，在山本五十六乘坐的飞机降落前十分钟进行拦截，并将山本五十六乘坐的飞机击毁，飞机连人坠落在原始森林之中。

电子侦听站可以装设在地面固定建筑物内，也可装在车辆、舰艇、飞机上，成为“运动情报站”。人造地球卫星的问世，使得侦听效能更为显著。海湾战争期间，以美国为首的多国部队，通过电子侦察卫星和通信侦察卫星，直接侦听到伊拉克轻便无线电报话机通信和小分队之间的电话交谈，掌握了大量的伊军情报。

为了增强侦听效能，可以采用“以扰助侦”的方法。就是对欲侦听的敌方重要电台，在其工作频率上施放微弱干扰，使其收听比较困难，迫使敌方重复拍发电文或延长通信时间，增加无线电波在空间的暴露机会，以便于己方侦收。

遥感遥感是现代电子侦察的一种重要手段。顾名思义，“遥感”就是从遥远的地方去感受物质的映象。

用作电子侦察的遥感，是借助于专门的光学、电子学和电子光学等探测仪器，把遥远的通信、雷达等电子系统所辐射的或反射的电磁波信号接收、记录下来，再经过加工处理，变成人眼可以直接识别的图象，再现出这些电子设施的原形。

被誉为“心灵窗户”的人眼，只能感受可见光波谱段的电磁波。那些比可见光波波长更短(如紫外线)或更长(如红外线、无线电波)的电磁波，它就力不从心、无法察觉。但用遥感仪器都可以感受到它们。以往看不到的物体变得了如指掌，地球表面再也没有什么地方可以称为神秘的“区域”了。

遥感可以分成四类：一是根据侦察结果的形态，分成“成像遥感”和“非成像遥感”。前者能将电子通信、雷达设备成像，得到像照片一类东西；后者只能感受到电子设备工作时的温度、音响等物理量的大小。二是根据遥感器的工作特性，分成“主动遥感”和“被动遥感”。前者，指遥感器自身能向外发射能量并接收自目标反射回来的信号。后者，指遥感器只接收从目标反射回来的信号而自身并不辐射出能量。三是根据遥感器探测目标的不同，分成“声学遥感”(探测电子设备工作时发出的声音)、“光电遥感”(探测电子设备工作时辐射出的电磁波)等。四是根据遥感探测器工作的波长范围，可

以分成可见光遥感、红外光遥感、微波遥感等三类。

可见光遥感是最常用的一种遥感手段。照相机和摄像机可谓是其常规武器。可见光遥感是利用自然光及人造光源如阳光或照明弹、探照灯等，照射目标，经光学系统将从目标反射回来的光线收集起来、用感光胶卷或录像带记录下来，目标的原形就能一览无遗。

可见光遥感系统所用的照相机和日常生活中所用的普通照相机大不相同。用普通照相机照相，目标物是不能移动的，否则，照出来的相片就会模糊不清。因此，只能拍摄静止的图象。遥感用的照相机采取了先进的技术措施可以移动，地面上行驶的通信车、移动通信系统等“ 动中通 ”设施都逃不出它的“ 眼睛 ”。

与其他遥感技术相比，用可见光照相，直观清晰分辨力高。据 资料表明，从 160 公里高空拍摄的照片，能分辨出地面 0.3 米大的物体。在晴朗的白天，用光学照相机拍摄地面景物是最方便的。若天空被厚云层覆盖，或者没有光照的夜晚，光学照相就一筹莫展了。这得靠红外光遥感来帮忙。

红外光遥感主要用于探测物体的红外辐射能量，它的最大特点是可以在夜间工作。集群通信车和车载雷达隐蔽在密林里并“ 穿 ”上了迷彩服，虽然在一般的航空像片上是“ 销声匿迹 ”了，但在红外遥感图像上却印下了清晰的踪影；装有通信设备的潜艇游戈海底，自以为躲过了空中侦察，但却瞒不过红外遥感仪器的“ 眼睛 ”。是什么魔力使红外遥感有此威力？原来，红外遥感感受到的是物体的热辐射。据测计，红外遥感具有很强的温度鉴别能力，就连 0.01℃的温差也能在红外遥感图像上得到显示。因此，只要通信、雷达等电子设备一工作，哪怕是它们披上了伪装网，或进入坑道，或潜入水下，也会在红外遥感图像上留下了“ 蛛丝马迹 ”。

红外遥感虽功能非凡，但因要受气象影响，还不能成为全天候的侦察兵。在对付恶劣的气象环境方面，微波遥感高它一筹。

用微波遥感进行电子侦察，有两种状态：一是检测电子设备辐射出来的微波能量；另是微波遥感器发出信号，根据目标物对信号能量反射的多少进行检测。我们通常所说的雷达就是利用微波辐射原理进行工作的。本世纪 60 年代，在电子对抗领域中，问世了一种独具一格的机载雷达。它用的天线不是装在飞机的机头和机尾，而是装在机肚子底下，位于机身的两侧。它专往飞机飞行方向的左右两侧斜起眼睛看物体。所以取名为“ 斜视雷达 ”(见图 4-11)。

图 4-11　侧视雷达飞机的外形

随着飞图 4-11 侧视雷达飞机的外形机向前飞行,位于飞行两侧地区上的通信、雷达设施，就被它一览无遗。图 4-12 是侧视雷达侦察示意。

图 4-12 侧视雷达工作示意

微波遥感不受云、雾、雨、雪等大气影响，能夜以继日进行全天候工作。享有“ 神奇的眼睛 ”之美称。

现代遥感技术是一个遍及从地面到高空的观测系统。“ 航空遥感 ”是该系统中最常用的手段。一般遥感飞机的飞行高度在 10 公里左右，布设在 10～

30 平方公里的地面通信、雷达设施，都能被它看得一清二楚。本世纪 60 年代以来，由于空间科学的进展，遥感技术已由以飞机为主要运载工具的“航空遥感”，发展到以人造卫星为运载工具的“航天遥感”，使人们能从一个更新的高度——宇宙空间来观测地球。“航天遥感”的最大特点是“站得高，望得宽”。据计，当人造遥感卫星的轨道高度为 1000 公里左右时，能拍下约 190 平方公里的地面照片(大小相当于一个海南岛)，甚至可以把半个地球全拍在一张照片上。对地球上的通信、雷达设施，它都可映入眼帘。海湾战争期间，以美国为首的多国部队，通过航天遥感，甚至可看清伊军士兵们通过无线电步话机进行交谈时的情景。遥感卫星在天际间运行，通过连续遥测，不仅能及时反映现象，还可用来对比分析地面电磁环境的动态变化，为运筹帷幄，决胜千里提供依据。

通信情报侦察侦察根据其任务，通常分为战略侦察和战术侦察两大类。相应的侦察接收机也有两种：战略侦察接收机和战术侦察接收机。战略侦察旨在单纯获取情报，战术侦察则是为实施干扰和某项具体任务服务。战略侦察接收机强调的是信号参数测量精度，战术侦察接收机却强调对信号的截获概率。

各种无线电通信系统都有其接收设备，用来对微弱信号的接收、放大，然后将信息转换成相应的形态表现出来。例如，无线电话系统的接收设备，最后表现为声音；无线电报系统的接收设备，最后表现为电码符号。对无线电话接收机的要求，是听清已知联络对象送出的话音，对无线电报接收机的要求，是能发出清晰、准确的电码音响。

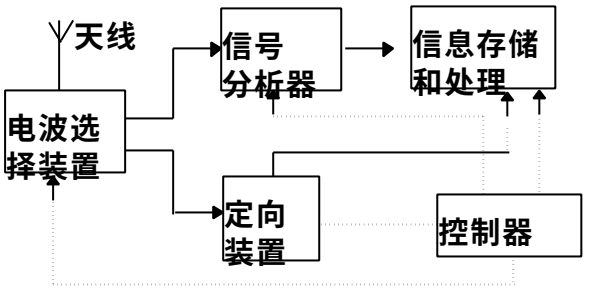


图 4-13　通信侦察接收机的组成示意

通信侦察接收机则与之不同，它是在极其广阔的电波海洋中实现对各种未知信号的接收，并随之对其进行分析(探测参数)和识别，进而查明对方无线电通信设备及其位置，掌握对方无线电通信的战术、技术性能等。据此，侦察接收机应包括电波选择装置(像收音机那样，只要电台广播，将调谐指针对准那个电台，就能收听到那个电台的广播)、信号分析装置、定向装置、信息存储和处理装置以及控制装置等五部分，它们的相互关系如图 4-13 所示(图中，实线箭头表示信息流，虚线箭头表示控制线)。

通信情报侦察接收机可以安装在地面无线电侦察站、电子侦察飞机和电子侦察船乃至电子侦察卫星上，也可制成便携型，安装在机动车上或随身携带。目前它已被广泛地应用在战场上。

随着电子科学的发展，侦察接收机已由电子计算机进行控制和信息处理。搜索、侦察速度可以达到每秒钟几万个信道。美国新近生产的 FSR—1000

通信侦察机，侦察频率可扩展到 12.5 吉赫，能探测到各种无线电信号，包括调幅信号、调频信号、连续波和单边带通信信号等。

图 4-14 雷达侦察机的基本组成

被动雷达侦察被动雷达侦察接收机是一种专门用来接收雷达信号的设备。它的基本组成如图 4-14 所示。从图中可以看出，要想完成侦察敌方雷达信号的任务，关键是要有一副灵敏高效的侦察接收天线。侦察接收天线有两种类型：非搜索式的固定天线和自行搜索式的转动天线。为了不漏掉目标，在发送波束上，侦察接收天线通常采取“先宽后窄”的方法。即平时先用宽波束寻找雷达信号，待发现和捕捉到信号以后，随即转用窄波束对目标进行精确地测定。

雷达侦察接收机为了能在宽广的电波世界中探测所需要的信号，完成对各种雷达的侦察任务，就必须具有接收各种雷达频率信号的能力，这就要求电波的波段覆盖范围要很宽，囊括米波、分米波、厘米波乃至毫米波。各种波段分别采用不同特色的天线，有的形似喇叭，有的制成螺旋状，如图 4-15 所示。

图 4-14 中的无线控制设备，是雷达侦察接收机的驱动装置。它用来控制天线的旋转，并使终端显示器中的荧光屏扫描线也一起同步动作，以指示雷达信号的来向。

图 4-14 中的接收机是整个雷达侦察设备的“心脏”。与普通雷达接收机比较，具有接收波段宽、作用距离远、动态范围大等特点。在灵敏度相同的条件下，能够接收比普通雷达远得多的信号。

图 4-15 形形色色的雷达侦收天线

a.水平极化喇叭天线；b.垂直极化喇叭天线；

c.圆极化喇叭天线；d.圆极化螺旋天线

无论接收来自远方或近处的信号，它都能通过自动增益控制等技术，使终端显示器有稳定、清晰的指示，不会出现信号小时(侦察远距离目标时)显示不清楚，信号大时(侦察近距离目标时)显示失真的现象。由于雷达侦察接收机的作用距离远，能保证在较远的距离上及时发现和测定目标，为采取电子对抗措施提供了比较充裕的准备时间。

图 4-14 中的终端设备是雷达侦察接收机的落地装置。它包括三个部分：“显示器”用以显示目标和其信号的参数。显示方式可做到声形并茂。能通过喇叭音响、灯光指示和屏幕图视、数码显示等形式进行。在一般情况下，喇叭音响和灯光指示起粗略预告作用，精确的显示目标参数；还得靠荧光屏幕(显示波形)和数码显示(给出数值)来完成。

“分析器”用来对接收到的雷达信号进行分析。包括测计出雷达脉冲的宽度、脉冲重复频率以及天线转动周期等。

“记录器”用来全面、实时地将侦察到的各种信号记录下来，保存或供事后详细分析。小型雷达侦察机通常用磁带记录，在大型雷达侦察机中还配备有照相记录、数字式打字记录或由电子计算机进行存储筹。

无源雷达侦察机可以安装在陆地上(主要配置在边境和海岸线上)，用于

国防警戒，称作“陆基雷达侦察机”；也可安装在飞机上，用来完成专门侦察任务或为自己侦察报警进行自卫(例如,驾驶员可利用雷达侦察机提早发现敌方雷达信号或制导信号，以便采取相应的自卫措施)，这叫“机载雷达侦察机”；也可安装在舰艇上，称“舰用雷达侦察机”；也可安装在人造卫星中(称“卫星用雷达侦察机)，当卫星飞临被侦察的区域上空时，能快速截获各种雷达所辐射的信号并自动记录下来，按照须置的自动控制指令，适时地将它传回地面。

在野战条件下，为实施机动监视，雷达侦察机可以制成轻便小巧，由少数人甚至一个人就可携带使用。

无源雷达侦察接收机实施侦察，最突出的优点是侦察距离远，获取目标信息多，预警时间长。但是它不像普通雷达接收机那样，接收的是射向目标的回波，而是敌方雷达发射的直接信号，因此，只能测向不能测距。同时，它的工作始终处于被动状态，获取情报完全依赖于敌方雷达的发射，一旦敌方采取静默手段，它就一筹莫展毫无办法。还容易被敌方发射的假信号所蒙骗。

除此以外，雷达侦察接收机为了完成对各种雷达信号的侦察任务，要求波段覆盖比普通雷达的波段宽得多。实际上，一部功能比较齐全的雷达侦察设备，往往要包括从毫米波到米波的许多个分机，构成一个庞大的接收系统，不易隐蔽，容易遭受敌方摧毁。

测向定位测向是一种重要的电子侦察手段，它借助于电子测向仪，测定出正在工作时刻的对方无线电发射台的位置，即获取无线电波发射源的角座标(方位)信息。为对发射源实施干扰或摧毁提供科学依据。

在电子侦察中，测向分“搜索测向”和“非搜索测向”两种方法。搜索测向法需要一定的时间对所侦察的空间进行搜索；非搜索测向法能够瞬时地测定出发射源的方向。不论采用哪一种测向方法，都离不开测向天线系统、信号处理放大系统和终端显示系统三个基本组成部分，如图 4-16 所示。其中，测向天线犹如一对触须，在全系统中起着先导作用。

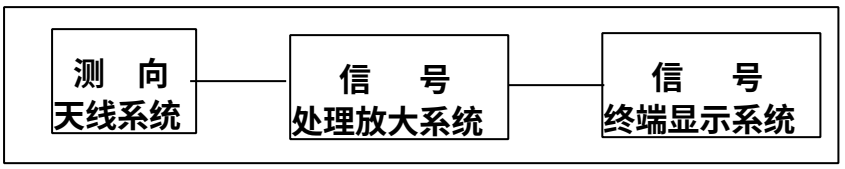


图 4—16 测向器的基本组成方框

在搜索测向法中，测向天线是可以旋转的。它发出的波束按一定的规律进行搜索借以确定发射源的方向。天线将所搜索到信号送给信号处理、放大系统，经处理放大以后显示在显示器上。这样就可探测出被侦察信号的方向。搜索测向法有点类似我们日常生活中用便携型收音机收听广播，将收音机的无线在空间自由旋转(实际上是在寻找广播电台的方位)，当收听到的声音最响时，广播电台通常就在这个方向上。

在非搜索测向法中，安装有多个固定的方向性天线(如图 4-17 所示)，分别接收来自不同空间的信号。每一个测向通道都有一组天线和与它相联接的

接收、显示设备，测向天线的波束无需来回搜索，就能同时迅速测定出数个发射源的方向。显然在测向范围相同的条件下，无线与接收设备的数量愈多，天线波束的宽度愈窄，测向的精度就愈高。

图 4-17 非搜索测向示意

探测被侦察的发射源，不仅要知道它的方向，还要确定其位置。这就要求在测向基础上进行定位。定位通常有直接定位和间接定位。直接定位技术要求高，利用人造地球卫星或飞机进行电子侦察时所用的垂直测量空间法，就是一种直接定位法。

间接定位法必须在不同地点设置两台或两台以上测向仪，同时对一敌台实施测向，通过在地图上交会，就能确定其位置。为了减少交会误差，要求交会夹角在 30 ° ～150 ° 之间。最佳交会夹角为 90 ° 。人工交会定位速度慢，约 2 分钟左右。若要快速定位，则需要借助于电子计算机控制，实行自动交会。目前利用自动化程度较高的测向定位设备定位，只需不到 30 秒钟就能完成。

图 4-18 所示的是对固定无线电台实施测向定位示意。图 4-19 示出的是利用两台测向仪利用三角测量方法确定发射源位置的示意。通过数字计算，不难求得电磁辐射源的具体位置。

图 4—18 对固定无线电台测向定位示意

图 4—19 三角测量定位法示意

巧设诱饵“ 巧设诱饵，以假充真，骗敌上钩 ”是现代电子侦察惯用的方法之一。在近期发生的几场局部战争中，为了诱使敌方开启雷达，有的以无人驾驶飞机或导弹的佯攻为诱饵；有的在飞机上加装雷达回波增强器，模拟战斗机群临空，中计者无独有偶。如中东战争中，贝卡空战前，以色列就曾用在无人驾驶飞机上加装雷达回波增强器的方法，引诱叙利亚将制导雷达开机。以色列以最快的侦察速度，迅速乘机查明了叙 SA—6 防空导弹的工作方式、技术参数及其配置、部署情况，尔后出动大批机群临空实施突袭，不到 6 分钟，就将叙利亚境内 19 个 SA—6 导弹发射阵地全部摧毁。

冒充冒充与欺骗是通信侦察常用的伎俩之一。第二次世界大战期间，在苏德战场上，德军无线电通信侦察人员常常冒充苏军无线电员与苏军电台通信、通过巧询妙问，查明了苏军无线电台位置及其隶属关系。统计材料表明，在第二次世界大战期间,德军无线电侦察部门几乎何大能截收苏军近 10 万份无线电报，并能从中破译 1/5 还要多。在大西洋之战中，德军无线电侦察部门也用冒充、欺骗等方法，截收与破译了英国海军部与英国运输船队之间的无线电通信，从中查明运输船队的航线和位置，进而判断出英军后勤保障计划与作战企图，并及时引导己方潜艇实施伏击，使英国运输船队遭到很大损失。

无线电通信冒充，在外军有的叫“ 无线电模拟迷惑 ”。这种“ 以假充真 ”的战法，是在掌握了敌方通信联络特点和部分通信资料基础上，运用类似于

敌方通信电台的信号、电报员的手法特点，使用敌台的通信联络规定，冒充故方无线电通信网中的某一个电台，与无线电网内的其他电台进行联络和通信。从而达到截取敌方无线电通信情报的目的。

实施无线电冒充，最关键的问题是要很快地使对方“上钩”。一要巧择适当的冒充时机。当战役、战斗最紧张的时刻，敌方使用的无线电通信遇到困难乃至久联不通时，突然进行无线电冒充，常能出敌不意，一诱就灵。二要充分准备，力求一次成功，否则，很容易露出马脚，遭敌识破。

3.抗侦察有方

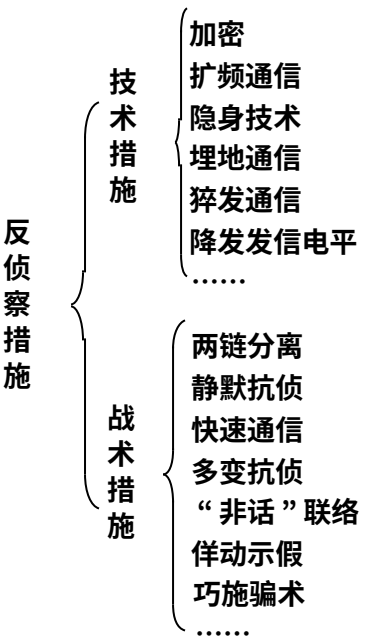
抗敌方电子侦察，就是防止己方电子设备的电磁辐射信号被敌方侦获，或者即使被敌侦获，但在一定时间内破译不了，难以从中提取有用的情报，从而失去了时间性和军事价值，使敌方无法有效地实施干扰和摧毁。

抗侦察的方法很多，概括他说，有技术措施和战术措施两大类型。

在技术措施方面，主要包括：采用低截获概率信号，如扩频信号，捷变频信号，旁瓣抵消技术、猝发通信、隐身技术等，降低无线电波的发射能量并对信息加密，使敌方不易侦察到，即使截获了信息，由于经过了加密处理，在短时间内也难识“庐山真面目”。

在战术措施方面，主要是想方设法控制电磁辐射和实施电子伪装。想方设法缩短无线电波在空间的暴露机会和时间，根据作战意图实施无线电静默；或为转移敌侦察方向组织无线电佯动；或进行无线电欺骗。用假电台、假雷达模拟指挥所；用建立假无线电网络，设置假电磁辐射源，拍发假电报等欺骗敌人。

反侦察的具体方法如下所示：



密传抗侦在军事通信领域里，信息的安全与保密关系到军事行动的成功和战争的胜负，加强通信保密以防敌特侦察显得十分重要。

通信保密通常包括两个方面：一是不让敌人侦听或截获到我方的通信信号，这是主动的保密措施；二是将信号变形，例如进行巧妙地编码，编码技艺越高超，密码结构、形式越新颖、离奇，窃听者越感到莫名其妙，摸不到头脑，因而不能破译我方信号的内容。这是目前通信保密研究的重点。

通信体制分为模拟通信和数字通信两大类，它们各有各的加密方法。模拟通信在信道中直接传输的是连续变化的电信号。它的频率和振幅完全模仿声信号而变化。也就是说，信道上传送的电信号是原始声信号的“化身”。普通电话都是“模拟电话”(图 4-20)。

图 4-20　模似电话示意

“模拟电话”加密的方法很多。“加杂音”是一种原始的加密方法。在发话端，电话机附加上“杂音干扰信号产生器”，用户讲话时，它就自动地发出干扰信号，与人的讲话声音掺混在一起送往线路。因为在线路上传输的既有真正的话音又有附加的杂音，“鱼目混珠”，即使被敌方侦察、窃听到，他也无法弄清楚。这就达到了保密的目的。在受话端，因为有消除杂音的装置，能“去粗取精”将对方送来的杂音去掉，真正的话音却能保全。

“变频率”是“模拟电话”目前最常用的一种保密方法。众所周知，我们讲话所以能发出声音，是由于喉管中声带振动的结果。每个人声带振动的快慢是不一样的，有的快(频率高)，有的慢(频率低)。但一般都是在 300 赫到 3400 赫的频率范围内。讲话时，如果把 300 至 3400 赫的话音频带原封不动地送往对方，敌特就容易侦听到我们的通话内容。要是将送出来的话音进行一番加工，例如将话音频丰前后进行“大颠倒”，把发话人送出的 300 至 3400 赫的话音频率彻底进行一次大翻个，让原先的 300 赫(低频)通过变频器变成 3400 赫(高频)，而把原先的 3400 赫变成 300 赫，这样就彻底改变了话音信号中各频率间的正常关系，人为地“以假乱真”。倘若把话音频率进行“小颠倒”，就是通话双方按事先约定好的时间将整段话音频率分割成若干小段，分别进行颠倒。由于话音频带中各频率的相对幅度起了变化，形成了严重的失真。敌方要想侦察、窃获都比较困难。但是接收端只要按事先规约，将颠倒了的频谱再颠倒回来，就可恢复成原来的话音。

事实上，分段的方法又是很灵活的，可以分成两段，也可以分成三段(图 4—21)、四段、五段，甚至更多些。段数分得愈多，置乱得愈严重，保密性就愈强。在实际通信中，将原始话音分成几段，以及采用何种颠倒方式，全由通话双方事先密定，并在通话过程中双方视情进行“随机应变”。由于电话采取了加密措施。用户虽然讲的是明语，在线路上传送的却是密语，这就叫“明讲密传”。

图 4-21 话音频带分段颠倒示意

数字通信在信道中传输的是一连串彼此离散的有电、无电(或正电、负电)的脉冲信号。它是用二进制数中的“1”和“0”的数字组合形式来表示原始话音的。图 4—22 是数字电话通信示意。在发话端，先将话音变成模拟的电信号(由送话器完成)，再把模拟电信号变成相应的数字信号组合(由模/数转换器完成)；受话端则相反，先将数字信号组合变回模拟电信号(由数/模转换

器完成)，再把模拟电信号变回话音(由受话器完成)。

数字通信在信道上传送的是离散的“数字串”，本身就具有很大的保密性(第三者听到的像一串串连珠炮，传输速率快时根本听不清)，为了密上加密，可进一步采取保密措施。数字通信与模拟通信的加密方法尽管大不相同，但都离不开一个“乱”字。前者通常采用“数字置乱”技术，后者采取“频谱置乱”技术。

“数字置乱”的基本概念是：在发送端设法将欲发送的信码组合搞乱，而且愈乱愈好。到了接收端，再将搞乱了的信码来一个“拨乱反正”还原成原信码。“搞乱”和“拨乱”信码的任务，通常由一种专门的“电子门”(叫“异或门”)来完成。图 4-23 是数字电话加密、解密示意。假设某一瞬间，用户送出的话音经过“模/数”转换后的数字信号组合(叫“信码”)是 10101

(→表示信息流向)，密码器送出的密码是 00100。它们分别加到“异或门”的输入端，根据“异或门”的逻辑运算功能(0⊕0=0，0⊕1＝1，l⊕0=1，1⊕1=0)，信码与密码经过“异或门”共同作用后，输出的信号组合是 10001，这叫“密信码”(意思是加了密的信码)，它已经不是原来的信码模样了 (见表 4—1)从而起到了加密的作用。

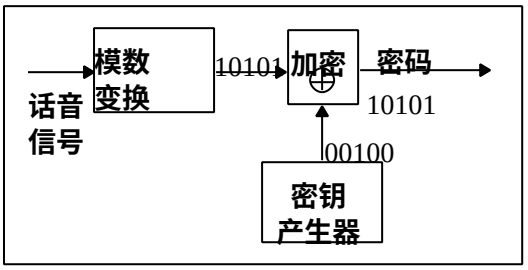


图 4—23 数字电话加密示意

到了接收端，密信码和对方密码器的密码(必须和发方的密码一样)又一次作用到“异或门”上。根据“异或门”的逻辑功能，还原出的信码刚好是 10101(见表 4-2)。从而起到了解密的作用。解密后的信码经过“数/模”转换，还原成模拟话音送给用户。

信码	密码	密信码
1	0	1
0	0	0
1	1	0
0	0	0
1	0	1

密信码	密码	信码
1	0	1
0	0	0
0	1	1
0	0	0
1	0	1

由于双方密码器是同步运转，而且密码本身又是无规则的，只要“ 底密 ”(也叫密钥)不暴露，敌人即使窃听到电话，在短时间内用一般的电子技术是很难破密的。密钥量越多，平均保密时间就愈长，破起密来也就愈困难。

在现代战争中，通常战术保密级的最低密钥量为 106(100 万个)，假定破译速度(变换密钥的速度)为每秒钟 1 次，则平均保密时间约为 6 个昼夜。通常战略级最低密钥量为 10，假设用电子计算机破译，破译速度为每秒 1 亿次，则平均保密时间为 100 万亿年，即使取它的一百亿分之一作为可靠时间，也可达 1 万年，这实际上就是不可破译的。

上面说的，无论是模拟通信还是数字通信，加密和解密全是由特制的保密机来完成。保密机在实际运用中，通常有两种用法：将保密机安装在用户端，为某一用户专用(图 4-24)；将保密机安装在传输信道两端，供通信网内各用户公用(图 4-25)。

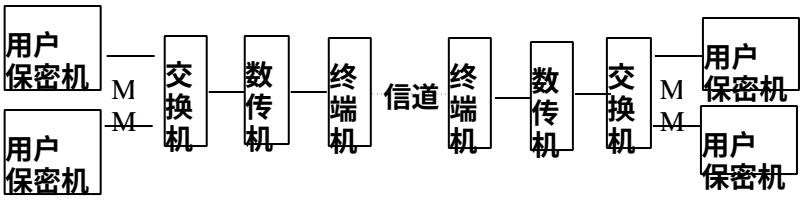


图 4-24　用户保密能信系统

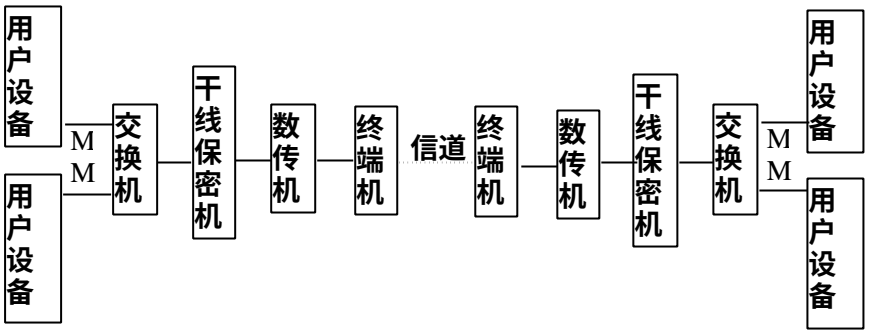


图 4-25 干线保密通信系统

保密通信最初用于有线电信道上，如今无线保密电台也已广泛用于战争。德国新近装备部队的无线保密电台具有扩频传输能力。能有效地防止窃听和测向。它所配备的密码机采用了数字话音信号和扩频算法进行加密，能达到“不可破译”的保密度。这种保密电台只重 1.5 公斤，个人就可携带。

无论是有线保密通信，还是无线保密通信，其关键都是建立科学的密钥体制，可以预言，随着科学技术的发展，密钥技术水平会越来越高，自动、多变、严密的密钥体制，将会给保密通信带来新的生机，在电子对抗中它必会产生愈来愈大的作用。

扩频抗侦扩频通信是扩展频谱通信的简称。指的是利用与信息无关的伪随机码，使无线电射频信号频带宽度远大于信息信号(称作基带信号)频带宽度的通信方式。扩频通信的射频信号频带宽度，可扩展到信息信号频带宽度的数倍到数千倍，扩频通信的基本工作原理，示意于图 4-26 中。

图 4-26 扩频通信的示意

由于经过扩频后的信息信号功率分散在很宽的频带内且隐蔽在噪声中，使一般接收机犹如在大海捞针那样，无法侦听到。即使用专门的接收机来侦听，也因无法事先知道随机而变的编码规律，不能进行解扩频，侦听破译起来自然非常困难，因而极大地降低了敌方截获的概率。

扩频通信技术有直接序列式、跳频式、跳时式以及它们的混合式。下面以直接序列式为例说说它的工作过程。

直接序列式扩频技术，就是利用二进制的伪随机序列直接扩展和解扩信息的频谱。以打电话为例(见图 4-27)，模拟话音经过模/数转换后变成了数字信号(图 4-27 是数字信号的某一小段)，它是窄带信号，其能量集中在比较窄的频率范围内，能量密度(单位频带所占的能量)比较高。图 4-27 中的 b，表示二进制的伪随机序列，能量密度比较低。图 4—27 中的 c 表示 a 与 b 经过模 2 相加(即“密传抗侦”一节中所说的“异或门”逻辑运算功能)后的另一宽带信号，其能量也分布在很宽的频率范围内，能量密度很低。这样的通信信号无论其波形和能量，在频带内的分布都与电子设备的热噪声相似，使得敌侦察设备很难截收和识别。

在本方的收信端，要将接收到的扩频通信信号进行解扩，本地必须产生出一个与发信端作同步运行的二进制伪通机序列信号

图 4-27　直接序列式扩频技术示意

图 4—27 直接序列式扩频技术示意(图 4-27 的 d)，它间接收到的扩频话音信码进行模 2 相加，从而还原成扩频前的数字话音信号，如图 4-27e 所示，结果数字话音信号的能量重新集中在比较窄的频带内，呈现为高能量密度。

就世界范围而言，扩频通信问世于本世纪 20 年代。

1956 年开始应用于军事。

60 年代中期，我国开始研究扩频通信。1985 年，在卫星通信系统中应用了直接序列扩频技术。扩频通信的发展趋势是，采用混合扩频方式；扩频通信技术与自适应技术、猝发通信技术相结合等。这对提高电子对抗水平，尤其是抗截获、抗干扰方面，将会起愈来愈大的作用。

隐身抗侦随着雷达、光学探测设备等相继问世，极大提高了电子侦察的精度。为了减少己方兵器被对方发现的概率、隐身(隐形)技术应运而生。

隐形技术最早是为了对付雷达侦察。我们知道，被喻为“千里眼”的雷达，是靠发射高频无线电波和接收从目标上反射回波，并在荧光屏上显示来实现对目标探测的(如图 4-28 所示)。如果能削弱反射回波的能量，或干脆设法不让它反射，那么，“千里眼”就会变成“睁眼瞎”。反雷达侦察的隐身技术正是基于这一想法进

图 4-28　用雷达测量目标高度和距离

行工作的。

“以隐抗侦”通常有以下几种途径：

一是赋形。人们在研究中发现，物体反射电磁波的强弱，不仅仅取决于它的几何截面积的大小，还取决于它的有效反射面积，即“散射截面”。散射截面与物体的外形有关。同样大小的物体。外形越圆滑，棱角、平面越少，散射截面就越小，就越不容易被雷达探测。一般飞机之所以容易被雷达发现，是因为它那宽大的机身，长长的机翼，高耸的竖尾和直来直去的机尾喷管和进气道等容易对电磁波产生强烈反射的物体。号称“空中巨霸”的战略轰炸机和“神魔之鹰”的隐形(隐身)飞机，由于巧施了“变形术”，改变了传统的外形设计，很少对电磁波产生反射。据测计，隐形飞机对雷达波的有效散射面积只有昆虫那样大小，美军 B-2 隐形战略轰炸机只有 0.02 平方米。

二是吸波和透波。即在飞行器对电磁波散射能力强的部位，涂上能吸收电磁波和透射电磁波的材料(如各种铁氧材料)，从而使入射的电磁波能量衰减，达到“障敌眼目”、“隐己之身”的目的。地面雷达不管从哪个方向照射探测，都会被飞行器吸波材料吸收或被透波材料散射掉，几乎不可探测。

三是消波。即采用有源和无源对消技术，在雷达探测目标的有关部位引入一个回波源，来抵消另一个回波源，使雷达无法显示目标。

四是降热。即降低热辐射。如飞行器采用弱红外辐射发动机，可大大降低红外辐射，使红外探测器无法探测。

综上所述，不难看出，“以隐抗侦”是一项多学科的综合性技术，只有综合运用各种技术措施才能获得最理想的隐形效果。在海湾战争中大出风头的美国 F—117A 隐形战斗轰炸机集赋形隐身、材料隐身、红外隐身等多种隐身技术于一身，巧妙避开伊拉克防空雷达系统的探测，神出鬼没如入无人之境。在无战斗机护航的情况下仍能准确投掷炸弹。它轰炸伊拉克总统府和电

报、电话大楼时，命中精度之高，令人瞠目结舌，竟然使被炸目标旁边的四星级饭店可以安然无恙。据美同军方的量化分析、统计，在海湾战争中，F—117A 一个架次一枚激光制导炸弹的攻击效果，相当于第二次世界大战期间，B—17，轰炸机飞行 4500 架次、投掷 9000 枚炸弹的效果。这其中，除了精确制导武器以外，飞机采取了“以隐抗侦”的种种措施也起了决定性的作用。

据外刊报道，美国国防部电子战研究中心，新近研制成功了一种可在敌方上空停留 4～6 小时的、不易被人发现的隐形侦察系统。这种被称为空投气球电子战系统的军用隐形侦察装备。悬挂在由电子计算机控制的氦气球下面，可由飞机携带到敌方上方投下，它在雷达荧屏上显示的目标非常小，很不容易遭敌侦察。

埋地抗侦电子侦察是借助于电磁波为媒介进行，而电波穿过地层时能量要受到很大哀减，有的无线电波遇到地层甚至一筹莫展寸步难行，这就为用埋地通信对抗电子侦察大开方便之门。

有线电通信目前大都采用电缆传输。由于电缆结构的原因，电磁能量不易从电缆散发到空间。尤其当采用一种新型的电缆——同轴电缆传输时，所辐射出的能量更少。这就为电子侦察造成了障碍。

组成一个通信回路，需要两根导线，在普通电缆中，这两根导线是并行排列的。同轴电缆却别具一格。它是将一根导线套装在另一根导线的外边并使它们保持轴心重合，“同轴”即由此而得名。见图 4-29。通常将外部的空心铜管称为“外导体”，内部配置的实心铜线称为“内导体”。通信时，电信号所产生的电磁场全部集中在同轴管内部，分布于内、外导体之间，几乎没有散逸到周围空间而形成辐射。因此，很不容易遭到侦测。如果将同轴电缆深埋地下，它的反侦察能力更强。试验表明，将同轴电缆埋入地下 1.2 米以上，就可以防止侦察和窃听。

图 4-29　用轴电缆结构

本世纪 70 年代，光导纤维通信(简称光纤通信)问世，使得电子侦察已无隙可乘。因为光寻纤维通信是一种以光波为信息载体，以光纤为传输媒质的通信方式，光波在细如发丝的玻璃纤维中传输不会向外产生辐射，不用说，用电子仪器无法侦察到它，就是用光学仪器也很难发觉它的踪影。加上光纤本身是绝缘体，外界电磁场对它毫无影响。如果将众多的光纤聚集成光缆，深埋地下，敌人要想对它进行侦察，简直是难上加难。

不仅有线电通信和有线光通信可转入地下工作，随着科学技术的发展，就是一向与空间打交道的无线电联络也可实现地下通过去，无线电通信一直是电子对抗的“弱点”，很容易遭敌侦察与测向。现在，将无线电收发信设备及其天线全部设置在地下坑道和工事内，相当于给它穿上一层能蒙住敌人眼睛的厚厚“地衣”。

地下无线电通信，有各种各样方法：一是以大地作传输电波的媒质。地质学研究告诉我们，地壳的表层是能够导电的，而且导电率比较高。如果将发信与收信天线，都伸到表层中，就可以表层为导体进行通信。它对坚守防御地域各级地下指挥所之间的通信，不失为一法。

二是以大地作无线电波的“反射镜”。科学研究表明，大约距离地球表

面 30 余千米处，有一层类似高空电离层的物体，它能反射无线电波。利用它对无线电波的反射作用，可以进行地下无线电通信。如图 4—30 所示。

图 4—30 地下通信示意

三是进行“地——天——地”通信，融“上天”、“入地”于一体。见图 4—31，当无线电波自埋在地下的天线辐射出来之后，首先向上穿透地层，然后“兵分两路”：一路以“地波”的形式，沿地表面传播作用于接收天线上；另一路以“天波”的形式，腾空而起，作用到高空电离层，并以它为“镜子”反射到接收天线上。其通信距离可达数百千米。图 4—31

“地——无——地”通信示意

四是借“线”传输。地下指挥所内往往布设有备式各样能导电的物体(例如各种动力电缆、运输铁轨等)，它们对无线电波都能产生电磁感应，因而可以成为地下指挥所内进行通信的“天线”。当无线电台的天线靠近这些感应线时，发射机发出的无线电波会在感应线上引起感生电磁场，于是信号沿线传播出去。作用到接收机上时就可实现通信。如图 4-32 所示。这种通信方式也叫“感应通信”。

图 4-32 感应通信示意

在现代电子抗争中，无线电地下通信可大显身手。它隐居地下，即使坑道内的密封门全部关闭也能维持通信。为减少无线电波的传输哀减，地下通信通常采用长波长工作。当采用长波工作时，因波长很长，敌方要想对其实施电子打击，必须使用很长的干扰天线，才能有效地辐射出干扰信号。这样，容易暴露干拢台的目标而遭火力摧毁。

第二次世界大战以后，随着电子对抗日益尖锐、复杂，美英和前苏联等国不惜投入大量的人力和物力开展地下无线电通信的研究，并研制成功了若干个通信系统用于作战指挥。本世纪 60 年代，美国为了对付前苏联的核攻击，在一些洲际导弹基地之间，采用以“地——天——地”通信方式，建立了地下控制中心与导弹发射井之间的地下通信系统。

1966 年，北美防空司令部在距离地面 500 米深的花岗岩下建起了具有抗核攻击能力的地下综合指挥中心，其中就有一条甚低频地下通信线路，作为对外联系的应急通信手段，朝鲜战争期间，中国人民志愿军曾使用敷设在坑道内的天线进行无线电通信。在海湾战争中，地下无线电通信也曾发挥过作用。“沙漠风暴”开始前 10 天，以美同为首的多国部队通过侦察对伊拉克军事目标进行了“地毯式”轰炸，空袭达 2 万多架次。伊军在遭到连续空袭、地面通信设施被严重破坏情况下，仍能通过无线电通信向部队发号施令，这与伊拉克经过多年建设，有一套较完备的、坚固的、隐蔽的地下通信设施分不开。军事分析家们指出，在电子对抗日益尖锐的今天，地面通信设施会不可避免地要遭到敌火力摧毁以至面临完全中断。随着指样机关转入地下指挥所，地下通信显得格外重要。只要地下指挥机关不被摧毁，它就能保证把最重要、最紧急的信息接收下来发送出去，从而在最困难、最险恶的情况下，确保作战指挥不间断。有朝一日，被誉为“电子侦察克星”的地下通信，将戴上“最后的通信手段”和“打不断，炸不烂的信使”的桂冠。

“善守者，藏于九地之下；善攻者，动于九天之上，故能自保而全胜也。”这是《孙于兵法·形篇》中的名句。抗侦察隐身术种类繁多，运用广泛，但归结起来也不外乎“藏于九地”和“动于九天”。“以埋抗侦”可谓是为孙子兵法的“藏于九地”思想注入了新的内容。

猝发抗侦　“猝发通信”是“以快致胜”的战术在通信中的应用。它通过“快报终端”先将欲传递的信息，进行压缩编码贮存起来，然后寻找适当时机和信道，以迅雷不及掩耳的速度“猝 发”出去。收端收到后，进行相反程序的处理，即可读出报文。

“猝发通信”因为发报的速度很快(一般要比人工报快 60 倍，是电传电报的 20 倍)，信息在空间停留的时间很短，往往使敌方侦察和测向造成很大困难。

猝发通信特别适合于前沿侦察分队或特种作战部队使用。海湾战场上，美军特种部队就曾使用了一种高速数据猝发加密通信系统，取得了明显的抗侦察、抗干扰效果。该系统传输速率为每秒钟 266.6 比特至 16 千比特，每次可发送 10 份(每份 300 个字符)报文，还可接收 5 份报文。英国使用的短波无线电台的猝发传输装置，可存储 1000 个字符的待发送信息和 16 份接收信息(总长度 2000 个字符)。

“猝发通信”可以看成是时域上的一种抗侦察、抗测向措施。目前使用的快报终端是调制式的，容易受天线信道带宽的限制以及多径效应、衰落、随机噪声等因素的影响，特别是易受突发干扰的影响，因而使得信号传输速率不能太高，通常为 600 波特至 1200 波特。随着电子技术的发展，9600 波特的快报终端即将问世。那时，信号在空中暴露的时间将更短，甚至短于敌方侦察设备截获、分析和识别所需要的时间。由于发射出去的无线电波在空中稍纵即逝，敌方要想侦察是非常困难的。

降低发信功率 侦察的效果和距离与辐射源的辐射功率有关。为防止敌方侦察，在保证通信的前提下，应尽量使用小功率电台和低功率发信，严格控制大功率电台的使用，用小功率通信芳是有困难，可采用中间转信的方法，即联络双方通过其他电台(中介台)收转通信内容。如图 4-33 所示。

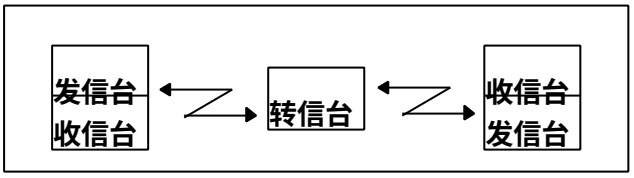


图 4-33　转信示意

分链抗侦 通信网络是作战指挥的经络系统，它通常有两种组织方式：一是按作战指挥关系组网，另是按作战地域组网。

按作战指挥关系组网(见图 4-34)时，通信是在各指挥所之间直接建立，指挥链与通信链重合，通信枢纽与指挥机关相伴配置。每个指挥机关既是实施作战指挥的场所，又是一个庞大的通信中心。按这种通信体制建立通信联络时，由于通信线路纵横散布，天线、车辆密集和通信体伴有电磁辐射，容易暴露指挥机关位置，易遭敌方侦察，不利于隐蔽。

组织通信网络时，如果将指挥机关和通信中心分开配置，使指挥链与通

信链相互分离，就可大幅度地减少指挥所的电磁辐射

图 4-34 指挥链与通信链重合

源；各种通信设施也可寻找有利的地形地物进行疏散配置。因而，不容易被敌方测向、定位，有利于隐蔽指挥，大大提高了指挥机关和通信设施的生存能力。

静默抗侦 无线电静默就是在规定的时间和地区内，禁止无线电台发信，以切断敌方进行侦察之“源”。无线电静默是实施电子防御的常用方法，是无线电台通信伪装的主要措施。它虽然以暂时停止无线电通信为代价、但可以有效地隐蔽军队的行动企图和隶属关系，避免过早地暴露军队指挥机关的位置。尤其在战斗准备时节、变更作战部署、部队实施机动、秘密接近敌方或设伏、撤离战场等情况，运用无线电静默尤为必要。在通信过程中，有时突然实施静默，不仅可以使敌方顿时失去目标，还可起到扰乱和迷惑敌人的作用。

利用无线电静默避敌侦察的战例很多。日本奇袭珍珠港的战斗可使我们窥见一斑，那是1941 年 11 月 26 日，由大型航空母舰、战列舰、巡洋舰等 31 艘舰船组成的日本庞大机动舰队，在日本一名海军将领指挥下，极其秘密地东绕西转，从千岛群岛直奔瓦胡岛，于同年 12 月 8 日出奇不意地打响了奇袭珍珠港的战斗。如此庞大的战斗舰队在太平洋上长途跋涉，历时 12 天，为什么美国军队毫无察觉。这不能不说是日本采用的“哑吧”战术——无线电静默起了作用。原来，日军为防止无线电透露消息，将舰船上的无线电发信台全部封存，有的大功率发射机甚至拔掉了保险丝，连电键也锁进了电讯长官的抽屉。庞大的舰队无声无息地在洋上航行，瞒过了美军的“耳”、“目”，对突如其来的横祸毫无准备不知所措。就这样，日军施展的“哑吧术”使美军吃了“哑吧亏”。

1986 年 4 月，美军空袭利比亚时，无线电静默也起了很大作用。美军为了“以静护动”，空袭发起前，用代语发布了“实行全无线电静默”的指令，在此期间严格全面禁止使用无线电通信。利比亚首脑卡扎菲此时还对一名意大利记者说，他不认为美国人会向他们国家发起进攻。殊不知，在他谈话后几个小时，美军由 30 余艘舰船组成的机动舰队，从利比亚的一个友好国家的眼皮底下悄悄地驶进了利比亚的海域，出其不意地打了一场空海一体化的漂亮仗。进攻发起后，利比亚的广播电台还摸不清头脑，竟说，“这里正在发生一场战争，但是我们不知道是谁在和谁打”。

海湾战争中，以美国为首的多国部队也广泛使用了无线电静默，“沙漠风暴”爆发前，美国暂停了无线电通信，切断了所有易遭伊军侦察的无线电波辐射源。当第一次“战斧”式巡航导弹在伊境凌晨爆炸时，巴格达灯火亮如白昼，夜生活热闹非凡。伊军对多国部队的战前动态毫无所察。

无线电静默是指无线发信而言，静默时，无线电台必须保持全时守听。必须通信时，可用其他通信工具传递。

迅通抗侦 为了尽量减少无线电波在空中的辐射时间,不给敌方以可侦之机，应严格控制无线电台使用。要减少报量，缩短报文，简化通信内容。报话员在通信联络中，应做到短呼叫，沟通快；短报文(会话)，通得快；出现干扰时，要反应快、改频快，同时要广泛采用无线电信号通信。不发送与工作无关的信号，即便是一点一划，也不轻易在空中暴露。

多变抗侦 为了迷惑敌人达到反侦察的目的，组织与实施无线电台通信时，应着眼于“变”。通信中电台程式要变，通信联络规定要变，通信频率要变，工作种类要变，工作习惯要变，通报手法要变，通话口音要变，形成变化多端令敌难于捉摸的局面。力避出现某些独特的工作习惯，易被敌掌握，对其实施侦察带来方便。

佯动抗侦为迷惑敌人，隐蔽自己的真实意图而采取的虚假行动，“军语”称为佯动。无线电通信中的佯动，是指在通信中巧妙地制造假象，欺骗和迷惑敌方的无线电侦察，造成敌判断和行动的错误。这是一种积极的反侦察措施。

佯动迷敌巧在制“假”：

一是佯东真西。当部队调整部署或实施机动，集结他地时，可让无线电台留在原地佯动，或在非真实部署地域、非机动方向上、非集结地域内建立假的无线电通信，以迷惑敌人隐蔽我军的真实行动。

二是佯东真东。就是采取“真中掺假”的方法，在无线电通信网内设置佯动电台，建立假的联络对象，使敌难以判别部队的编成和部署。如果适时改变佯动台的联络对象，更能造成敌对我行动的错觉，增强以假掩真的效能。

三是佯真相当。就是佯动电台的联络对象、通信容量要与真实的电台相似，并执行同一通信规定，这样更能增加隐真效果，紧紧地牵住敌方的侦察鼻子，分散其侦察、干扰力量。

利用无线电佯动，隐蔽军事行动企图的战例中外皆有。1962 年，台湾海峡局势紧张，我军一些部队调至福建地区。部队在升进过程中，根据战略需要，无线电通信网始终开放，故意让台湾国民党军队侦听和测向。当我部队开进福建驻地后，台湾电台就广播我军行动的消息。我军完成任务以后，在撤离福建过程中采取了无线电佯动，台湾国民党军队始终没有得到我军撤离的情报。

第二次世界大战期间，l944 年 6 月。英美联军在法国诺曼底登陆，开辟了对德作战的新战场。早在登陆一个月前，英美联军用电子对抗手段，实施大规模的战役伪装和佯攻。它们在多佛尔地区设立一个假司令部，不时地向外发出一份份内容适当的假电报和假的无线电信号，使德军误认为英美联军要在多佛尔大量集结，甚至连德军头目希特勒也认为“联军不会在诺曼底登陆”。在登陆作战的准备阶段，英美联军首先通过电子侦察，详细地查明了德军设在法国海岸的 120 多种雷达的工作参数和部署情况，然后用航空兵和火箭将德军雷达和干扰站摧毁 80%以上，保证了英美联军雷达和无线电通信的正常工作。在战争发起的前夜，英美联军在佯攻方向的布伦地区，施放了各种干扰，一群群装有反射器的小船拖着涂铝的气球，使德军雷达误认为是一艘艘大型军舰。在小船的上空，英美联军用飞机投掷了大量的铝箔片，使德军雷达荧光屏上显示出的好像是大批机群临空。虚假的海情和空情，使德军造成错觉，以为英美联军在大批护航机掩护下要在布伦地区登陆，于是调集大量的海军和空军向布伦方向增援。殊不知佯攻在此，真攻于彼。在登陆战役开始时,英美联军在真正登陆方向上用 20 余架干扰飞机对德军雷达施放干扰，掩护了大批机群在英格兰上空编队集结和顺利飞向欧洲大陆。成功地完成了在诺曼底登陆的任务。谱写了大规模地实施“以佯抗侦”的成功战例。

海湾战争期间，美军在发起代号为“沙漠军刀”的地面进攻之前，为了达到声东击西的目的，采取了“金蝉脱壳”的战术。方面，大规模地实施电

子佯动，与此同时，将部队迅速调到沙科边界西部侧翼的伊军防御的空挡地带。伊军受到多国部队无线电通信的蒙骗，难辨美军的行动企图。使美军在几乎兵不血刃的情况下，以出其不意的攻势，一举解除了伊军几十万驻科部队的武装。

巧施骗术进行无线电佯动实际上也是一种骗术，它通常是指建立假的联络对象，达到以假护真的目的。这里所说的“骗术”，是指在真刀真枪的情况下制造假象，诱敌受骗。主要有两种骗法：

一是示次隐主。通信联络根据其任务，组织与建立时有主次方向之分。为了将敌方的侦察重心导致错误方向，可以在次要方向的无线电通信网中频繁地进行假通报，使敌方难以从通信工作量的多少上来判断军队行动的主攻方向。这样，就可掩护主要方向的无线电通信联络。

二是示假隐真。为了混淆敌方的电子侦察，使其对我方的作战行动和意图作出错误判断，可以在通信网中适当地拍发一些貌似真实并具有一定情报价值的密码电报。敌方尝到了“甜头”，就会受命于我，按我们的预案行事，从而保证了真电报的顺畅传递。

在“示假抗侦”方面，伊拉克在海湾战争中的一些做法值得借鉴。

海湾战争开始不久，以美国为首的多国部队凭借着航天和航空侦察优势所获得的军事情报，过早地宣称，伊拉克军队的指挥中心和通信系统在美军强大的电子打击下已遭全部摧毁，整个战争机器已经停止运转。然而，正当美军及多国部队洋洋得意欣赏“战果”时，伊拉克总统萨达姆却发表电视广播讲话，声称要对美国进行全面报复，同时，伊拉克的飞机频频升空，“飞毛腿”导弹接二连三地射向以色列和沙特阿拉伯等国。无可置疑的现实，迫使美军重估“战果”，不得不承认美军及多国部队的空袭和电子打击效果不是想像那样理想，伊拉克仍有很强的战斗力。

原来，伊拉克对美军和多国部队的电子空中侦察早有准备，采取了许许多多“以假抗侦”的措施。据资料介绍，早在两伊战争期间，伊拉克就不惜重金从国外购进了一套陆地卫星多光谱像片，认真判读、分析了本国重要军事目标的识别特征，随之进行了有针对性的严密伪装和隐蔽，采取了一系列的反侦察措施。结果大见成效，海湾战争期间，接连不断地使美军及多国部队上当受骗。多国部队尽管运用了最先进的电子侦察手段，也难辨真伪。

海湾战争中，伊拉克的“飞毛腿”导弹基地和游动发射架，曾是多国部队电子侦察和空袭的重点目标，但由于伊拉克在战前布设了大量的“飞毛腿”导弹“替身”目标，吸引了多国部队的空中火力，取得了隐真示假的效能。据有关资料披露，伊拉克在战前，曾从意大利、德国等购进了一大批仿真导弹。这些假导弹有热源，可摸拟导弹发动机，能吸引红外探测；有电磁波源，可摸拟通信和雷达，能吸引电磁侦测；外壳还涂有一层反射雷达波的材料。无论是用空中照像侦察、电子侦察，还是采用红外、热成像等当令最先进的侦察技术，都会认为它确实是导弹发射装置，以美国为首的多国部队虽然大动干戈，却击毁了大量的假目标，而使许多真目标漏了网。

“非话”联络用话语沟通联络，即便是使用了密语，也会被敌方侦猜出通话内容。敌方也往往通过无线报话员的音调和口音，分析出我方无线电台的配置等情况。为了防上敌方通过语言因素对无线电通信实施侦票，沟通联络时可采用非语言信号。就是用手指有节奏的轻轻敲击送话器的外壳或向送话器吹风等。实践表明，报话员采用非语言信号沟通联络，是防敌电子侦察

的有效措施之一。这种方法，在许多电影、电视上常可看到。

以警抗侦敌台为侦察、截取、削弱、扰乱我方无线电通信。常采用冒充欺骗的方法。但敌人对我无线电台进行冒充，不可能将其真象隐蔽得十分彻底，多少总会露出一些蛛丝马迹。只要我们在电台工作中提高警惕，保持高度警觉，从无线电信号、拍发电报的手法以及电台工作特点等方面及时发现异常现象，适时采取必要措施，就能识破其芦山真面目。

如同从事秘密工作的地下交通，接头时要对暗号那样，无线电台通信时也要使用暗令。敌台冒充时，怕我问其暗令，往往在沟通联络以后抢先问暗令；为摸清我暗令的密钥，在工作中故意多向暗令；当我方间其暗令时，则故意借口干扰大。信号小闭而不答暗令，甚至反问暗令。诸如此类使用暗令的反常现象，必须引起我们高度警觉。

我们要正确使用识别暗令。对熟悉的联络对象可以少问暗令，以防敌人窃听；与新的对象初次联络时必须问清暗令，严防敌台冒充；当对方假装种种原因不答暗令而反问暗令时，应不回答而要其先答暗令，以防上当。

此外，要熟悉联络对象的手法特点、电台的信号特征及频率误差等。变换联络对象、遭敌干扰改变频率、中断后恢复联络时应特别注意辨别对方的手法特点、信号特征与通常有无变化。

(二)干扰与反干扰

电子抗争是一个完整的作战过程。如果说，电子侦察与反侦察是前沿战斗，那么干扰与反干扰，好比是战斗发展到纵深阶段。它虽然是以无形的电磁武器去杀伤敌方的有生力量，但其激烈程度和对战局和影响，不亚于短兵相接时的白刃格斗。

本世纪 80 年代，世界上爆发了一条令人震惊的新闻，巴勒斯但解放组织中仅次于阿拉法特的第 2 号人物、武装力量副总司令阿布·述哈德遇刺身亡。事后据有关部门获悉，事件发生时，整个出事地点的电话线全部被切断。一架以色列的电于对抗飞机一直在距突尼斯领空大约 55 公里的国际走廊上徘徊。阿布·述哈德住地与外界的无线电通信，遭到了强烈的压制性干扰，不能与外界沟通联络，以致陷于瘫痪。显而易见，阿布·述哈德遇难，很大程度上是由于电子干扰的缘故。

电子干拢，顾名思义，它是通过电子手段“干涉”和“扰乱”敌方电子设备的工作。确切地讲，它是指有意识地发射或转发某种电磁波，或用某些器材反射电磁波，以扰乱和欺骗敌方的电子设备，使其不能正常工作，甚至完全不能工作。

电子干扰的基本原理，可以用“同频相克”来描述。就是当干扰信号的频率与敌方电子信号的频卒相同或近似时，敌方接收设备就会收到干扰信号与电子信号相迭加的信号，从而失去了正常工作的能力。

要达到能压制住敌方电子设备的干扰效果，必须满足三个基本条件：频率对准、功率超过(即在敌方接收设备的输入端的干扰功率超过对敌台有用信号的功率)和样式适合(即收发双方的调制方式要相适应，如用调幅干扰信号去干扰调幅制通信信号)。

电子干扰是一种积极主动的电子进攻手段，根据进攻对象和方式不同，有各种各样的分类方法：

按干扰对象的不同，通常有通信干扰、雷达干扰、精确制导武器系统干扰以及指挥自动化系统干扰等。通信干扰是指用通信干扰发射机发射干扰信号，使被干扰的敌方通信接收设备失去正常工作能力。图 4-35 所示的是最简单的干扰发射机的组成。功率振荡器直接产生所需要的大功率射频信号，并

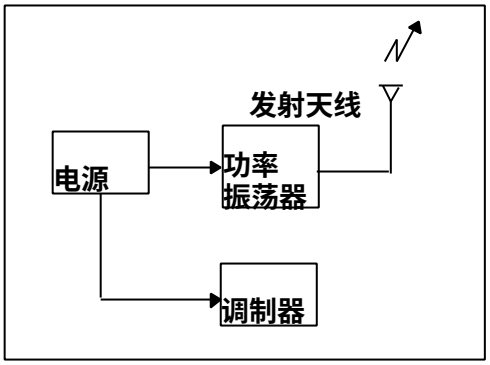


图 4-35 最简单的干扰发射机

进行干扰样式的调制，因此，它输出的就是受到干扰调制的大功率射频信号。这种干扰发射机可产生数百瓦至千瓦级的连续波功率。如果再加上放大设备，甚至

可以得到上千瓦乃至数千瓦的连续波功率输出。这对提高干扰效能、延长干扰的作用距离，无疑会起重要作用。

雷达干扰是指利用电子设备或器材，干扰敌方雷达的工作。敌方雷达受干扰以后，轻者使工作效能降低，雷达手难辨目标的真伪；重者，会使雷达工作完全失效。

精确制导武器系统干扰和自动化指挥系统干扰，是指用电子设备去扰乱它们的正常工作，使武器失控、指挥失灵。

按产生干扰的方法不同，通常分为有源干扰和无源干扰。有源干扰也叫积极干扰，就是有意地发射或转发某种电磁波去干扰敌方电子设备工作，无源干扰是指干扰物本身并不产生电磁辐射，但它可以改变电磁波的传播特性或改变雷达回波特性。

按干扰的性质不同，分为压制性干扰和欺骗性干扰两大类。按干扰频谱的组成不同，可分为瞄准式干扰和阻塞式干扰。按干扰作用的强度大小不同，可分为弱干扰和强干扰等。总之，干扰类型繁多，由此引出了各式各样的干扰物和形形色色的干扰方法。

1.各式各样的干扰物

干扰物是产生或引起干扰的物体。它通常分有源干扰物和无源干扰物两大类。

(1)有源干扰物

有源干扰物是指自身能产生干扰电磁波的物体。它通常是指各类干扰机。

干扰机根据所干扰的对象和任务，具有各种不同的电气性能、调制方式和使用方式。就使用方式而言，主要可分为：

固定式——主要用来实施远程干扰，其干扰功率大。

车载式——主要用来实施中距离干扰，干扰功率较大，干扰范围广。通常载于越野汽车、装甲输送车上。

背负式——主要用来实施近距离的机动干扰，干扰功率较小。干扰设备轻便可由人背负。

飞航式——主要用来由高空向地面、海面实施干扰，干扰功率较大，干扰距离较远，干扰范围大。通常由无人驾驶飞机、直升飞机等运载。

投掷式——通常通过飞机、军舰、火箭、大炮等，投掷干扰装置。干扰范围小，干扰点突出。一般情况下，可利用定时器或无线电指令信号启动干扰机工作。

投掷式电子干扰设备，一旦投掷出去就不再回收，所以也称“一次使用型电子干扰设备”。

(2)无源干扰物

无源干扰物通常指的是本身并不产生电磁波，而是通过反射电磁波来扰乱敌方电子设备(主要是雷达)正常工作的物体。

干扰物常用的有五种类型：

一是涂覆金属薄层的纸、玻璃纤维、尼龙丝等。人所共知，高档香烟盒中有一层锡箔包装纸，它是用来隔潮防霉变的，也许有人没有想过，在电子对抗中，它还可以用作无源干扰。

二是金属丝、金属带、金属片、金属线等。凡是金属物都可用来反射无

线电波进行干扰。由于金属干扰丝很轻，留空时间长(即干扰持续时间长)，且对雷达电磁波具有较强的反射特性，所以使用比较广泛。在战术使用上可作为飞机(舰艇)电子对抗自卫用。如果高密度地投放金属丝，能够对雷达波产生强烈反射，以至使敌方雷达接收机饱和，而无法显示目标。

三是投放能在空中产生电离的金属和金属化合物微粒，他像“ 天女散花 ”般的飘飘洒洒由天而降，可使一大群雷达迷盲。

四是投放假目标，扰乱敌方雷达的视线。

五是设置其他各种形体的反射物。如形形色色的角反射器等。

干扰物一般用飞机、火箭、火炮等，投射施放到相应的作战地域(空域)。每次投放的数量取决于被掩护目标的大小和性质。现在出现了一种专门用作干扰的炸弹，叫“ 干扰物炸弹 ”(内部装有干扰物的炸弹)，由飞机投放，用以干扰敌方雷达侦察，以保护飞机。

也可将干扰物制成包裹状，悬挂在降落伞上由飞机携带投放。这种干扰包装有定时装置，可以延时打开，用来欺骗敌方雷达。为了同时干扰不同频段(如米波、分米波、厘米波等)的雷达，可以将各种不同长度的干扰丝(片)、干扰绳。带)，按一定比例组装在一起。为了“ 虚张声势 ”，可以根据需要多装一些干扰丝，将其投入空中后，可以产生与飞机有效反射面积相当或为其数倍的有效反射面积，似庞大的机群压境。

看来并不起眼的金属干扰物，在实战中得到了广泛应用。当将大量的干扰物投入空中后，就散发开来呈云雾状。因此，称为“ 干扰云 ”，也叫作“ 干扰走廊 ”。在干扰云的干扰下，受干扰雷达的显示器上就会形成一条长长的亮带。有了这条带子作掩护，在“ 走廊 ”中飞行的目标就可安然无恙，免遭敌方雷达的探测。

无源干扰物所特有的神奇功能，使得它能在现代军事技术的激烈竞争中争得一席之地，并受到兵家的青睐。与那些耗资巨大的有源干扰机、飞机、军舰等相比，它虽然不值几何，但其实战价值却能与之等价齐观。

下面着重说说，在无源干扰群中屡建功业的三大件——箔条、角反射器和假目标。

箔条　干扰箔条是干扰丝和干扰片的一种，其长度一般约等于被干扰雷达波长的二分之一。但有时也远远超过雷达的波长。这种干扰物能对被干扰雷达的工作频率产生谐振，通过反射敌方雷达的回波而形成干扰。

干扰箔条大规模地用于电子对抗，最早要追溯到第二次世界大战期间。1943 年 7 月 25 日，英美联军大规模空袭德国汉堡时，首次使用了代号为“ 窗户 ”(window)的无源干扰箔条 250 万盒，每盒为 2000 根。每盒箔条所反射的电磁回波，足可在雷达荧光屏上持续将近半小时。参加空袭的英美联军轰炸机本来只有 790 架，由于金属箔条的反射作用，使德国的雷达操纵员看成了几千架，致使德军的防空部队只能盲目射击，结果英国皇家空军 2300 吨炸弹准确地倾泻在了汉堡港口和市中心闹区。由于战斗效果出人意外，此后，英文词典中的“ window ”一词，便添增了一条“ 金属干扰带 ”的词意。

说来也巧，首先发现金属箔条对雷达有干扰作用的竟是德国人自己，他们的专家早在第二次世界大战爆发前就知道了这一秘密。殊不知，这项发明成果被人利用最后砸了自己的脚。

据报道，第二次世界大战期间，英美联军仅在欧洲战场上投放的金属箔条就有数万吨，取得了近 500 架轰炸机免遭击落的效果。各种飞机自身进行

点投的干拢箔条，形成比飞机本身还强数十倍的反射回波，以摆脱雷达的跟踪。

战后，在朝鲜、越南、中东、海湾等战争中，干扰箔条仍发挥过巨大作用。例如，1973 年，第四次中东战争中，当以色列飞机上的无线电干扰机不足以对付埃及防空系统中新频段、新体制的雷达和导弹控制系统时，就由美国紧急空运大量包括箔条在内的金属干扰丝作为它的主要干扰手段，从而减少了飞机的损失。这次战争还表明了，干扰箔条在舰艇自卫对付反舰导弹的袭击上同样有着极其显著的效果。

在举世闻名的英阿马岛战争中也有同样的例证。战争伊始，英国特混舰队“ 无敌 ”号航空母舰和“ 普利茅斯 ”号护卫舰，成功地使用舰上“ 乌鸦座 ”无源干扰发射器发射出了大量的干扰箔条，使“ 飞负 ”导弹偏离了射击目标，“ 谢菲尔德 ”号驱逐舰却因没有及时采取干扰措施而葬身海底。

特别需要提及的是，干扰箔条如果与佯动战术结合，其战果更诱人。诺曼底登陆战役中，英美联军施展了“ 调机离山 ”计，利用空中散发的箔条，诱使德军大量飞机集结在预设空域，使德机在虚无缥缈的干扰云里白白盘旋了 3 个多小时，结果连英美联军飞机的影子也没见着。

光阴荏苒，转瞬间小小干扰箔条在现代电子战中已经成了无源干扰物的骨干。伴随着科学技术的发展，干扰箔条正向“ 四化 ”方向发展：

多型化——已问世了谐波产生箔条、充气箔条和再入大气层箔条等，干扰效能愈来愈高。

有源化——新型箔条不仅留空时间长，而且有的还能主动辐射电磁波。

自动化——新型的箔条投掷器可根据预警机测得的敌方雷达波长，自动对箔条长度进行切割，使之与雷达波长相适应，因而大大提高了干扰效果。

一体化——为发挥电子干扰的整体效能，现在可以将箔条连同曳光弹、电子干扰弹等一起投放。研制中的金属箔条还具有防护电磁脉冲袭击、实施无线电空中中继通信的功能。

角反射器角反射器也是一种常用的无源干扰物。它通常由三个互相垂直相交的金属导体平面构成，而金属导体平面对电磁波能呈镜面反射，它可以将敌方雷达射来的无线电波反射回去。如图 4-36 所示。

角反射器根据其结构形状不同，可以分为三角形角反射器、矩

图 4-36　利用角反射无线电波

图 4-37 各种形状的角反射器

形角反射器和圆弧形角反射器等多种类型，如图 4-37 所示。为了迷惑圆锥扫描雷达，现在已问世了一种可以转动的角反射器。它能够产生类似调幅波的回波信号，对雷达能产生很大的干扰作用。

在激烈的电子抗争中，角反射器也有过辉煌的战史。前己提到在诺曼底登陆战中，箔条模拟大批机群，迷惑了雷达的眼睛，其实，这次规模宏大的登陆战斗，是空海一体化的战役行动。模拟舰艇的正是角反射器。战役开始前，一群群装着角反射器的小船乘风破浪直驶海岸，造成了大批舰队登陆的假象。使德军像丈二和尚那样摸不着头脑。只得服服贴贴的调兵遣将听从英

美联军指挥。当年，英国政府的首相温斯顿·邱吉尔，在他的回忆录中，评论几次登陆战役所采取的电子对抗措施时说，我方在进攻发起日前和以后采取的种种迷惑敌人的措施，其目的就在于牵着敌人的鼻子走。这些措施的成就是惊人的，并且在战争中产生了深远的后果。

假目标假目标是一种用作无源干扰的诱饵，旨在欺骗雷达工作。最常用的假目标是带有雷达回波增强装置的小型飞行器。其雷达有效反射面积与飞机的雷达有效反射面积大致相等或者更大些。

为了迷惑雷达，施放假目标时，通常采取“先发制人”的方法。在战斗中，攻击机未飞行到雷达探测距离时就提前把它发放出去，结果使敌方防卸系统在受到真正攻击时注意力分散，或因目标过多而无法对付。

图 4-38　雷达显示器的假目标图象

图 4-38 是雷达显示器上的假目标图象

2.干扰有法

箔条、角反射器和假目标等无源干扰物，通常都是用来反射敌方雷达辐射出的电磁波。一旦敌方雷达不工作，它们就难以发挥其干扰功能。为了对敌方电子系统实施主动干扰，可以采取以下种种有源干扰方法：

点干扰学名叫瞄准式干扰。指的是针对敌方电子设备某一频率点(信道)实施频率瞄准干扰。由于干扰重点突出，干扰功率能得到有效利用，干扰距离远。

为了最大限度地施展干扰效能，干扰信号的频率范围(频带宽度)应约等于或略大于被干扰信号频带的宽度，使信号能完全被干扰信号“吞没”，如图 4-39 所示。

带扰法学名叫阻塞式干扰。指的是能同时干扰工作在同一频段内不同工作频率上的多部电子设备。由于它能同时干扰一大片，需要比较大的干扰功率。在功率相同情况下，由于干扰信号功率分散，因此，其干扰强度减弱，干扰的作用距离缩短。但与瞄准式干扰机相比，阻塞式干扰机不需要频率瞄准装置。

图 4-39　瞄准式干扰示意

为了对众多的电子设备同时实施干扰,干扰信号的频带可以做得很宽(一般为几十兆赫兹到几百兆赫兹)。它像一条带子那样将所有的被干扰信号都包容在一起，这叫“宽带阴塞式干扰”，如图 4-40 所示。

图 4-40　宽带阻塞式干扰示意

阻塞式干扰，也可采取“各个击破”的方法。即时被干扰信号一个一个地进行干扰。因为它形似头发梳子，因此.也叫“梳形阻塞式干扰”，如图 4-41 所示。

骗扰法它有三个别名，叫模拟式干扰、假目标干扰和迷惑性干扰。说的是人为地发射、转发或反对电磁波，用以扰乱或欺骗对方的电子设备，使敌

方得到错误的信息，作出错误的判断和举措。具体方法有：

一是发送假电文或发送模拟敌方的通信信号，使敌方受拢受骗。

图 4-41　梳形阻塞式干扰示意

二是发送假回波信号。这多半用在雷达系统中。干扰机收到雷达信号以后，发射与目标回波信号相同的假信号，使敌方雷达操纵员分不清真假目标或上当受骗，得出错误的目标信息。

图 4-42 所示的，是在雷达显示器上同时出现真假目标的情况。

发送假回波信号进行欺骗性干扰，也叫“回答式欺骗干扰”。目前，有一种专门用于欺骗的电子干扰机。干扰机上有接收和发射两部分。收到雷达信号后，发射出一个或几个与雷达频率相同(或接近)，并经过虚假信息调制的干扰脉冲。干扰机发射干扰信号，因为是在收到敌方雷达信号以后进行，也可理解成为是“回答”。“回答式欺骗干扰”由此而得名。这种干扰设备简单，功率利用率高，迷惑性强，敌方非常不容易识破。可使敌方炮瞄雷达、制导雷达跟踪到假目标上去，大大降低了高饱和导弹的命中率。

图 4-42　欺骗性干扰示意

回答式欺骗干扰包括角度欺骗干扰，距离欺骗干扰和速度欺骗干扰三类，使敌方雷达得出错误的距离、角度和速度等信息。

角度欺骗干扰，使雷达产生错误的角度跟踪；距离欺骗干扰，使雷达产生错误的距离跟踪；速度欺骗干扰，使雷达产生错误的速度跟踪。如果干扰机产生多个在距离上不同于真实目标的假回波，使雷达接收这些假回波以后分不清真假。图 4-43 所示的就是雷达受到多个假回波干扰以后在显示器上所显示出来的画面。画面中众多的脉冲有真有假(只有一个脉冲代表真实目标)，令人真假难辨。

图 4-43　多个假止标干扰图象

三是发送干扰脉冲。如在雷达干扰中，干扰机朝敌方雷达不时地发射虚假目标干扰脉冲，使敌方雷达分不清真假目标和目标的个数。在通信干扰中。干扰机发射出一系列类似于被干扰设备的虚假脉冲信号，以扰乱和破坏敌方的通信信息。

图 4-44　杂乱脉冲干扰图象

干扰脉冲可以是有规可循，也可以是杂乱无章。图 4-44 所示的是杂乱脉冲干扰图象的情景。

噪扰法学名叫噪音干扰，或杂波干扰。即用电子干扰机朝敌方电子设备(系统)发射出阵阵噪杂信号，以遮蔽雷达回波信号或破坏其跟踪系统的正常工作状况。在无线电通信中，借助于噪杂信号，对敌方的无线电通信信号进行压制或扰乱。

图 4-45　噪音干扰图象

图 4-45 所示的是图象信号受噪音(杂波)干扰的情况。从图中可以看出这种干扰可使雷达显示器的局部甚至全部呈现一片白色，使雷达操纵员看不清目标，更无法测定目标的距离、方位和高度。

图 4-46 噪音调制干扰机组成方框

噪音调制干扰机是一种产生噪音信号的常用设备,图 4-46 示出了它的方框组成。主要由侦察接收机、频率引导装置、射频振荡器和调制器等组成。侦察接收机负责探测出敌方电子信号的频率。频率引导装置根据侦察接收机测得的频率，控制射频振荡，使其工作在所测的频率附近。噪音调制器产生噪音信号，并对射频振荡器输出的振荡信号进行调制。或改变其信号幅度，称“ 噪音调幅 ”；或改变其信号频率，称“ 噪音调频 ”；或同时改变其幅度和频率，称“ 噪音调幅调频 ”；或改变其信号的相位，称“ 噪音调相 ”。无论采用哪种调制方法，射频振荡器输出的就是噪音调制的干扰信号。它像一串串无形的电子炮弹，朝敌方电子设备的某一频点轰击出去，使敌方的电子信号淹没在噪音大海之中。

扫扰法　学名叫扫频式干扰。它本质上是属于瞄准式干扰，不过它不是死盯住敌方电子系统某一个频率实施干扰，而是间隙地干扰在某一频率范围内工作的不同频率的多部雷达。图 4-47 所示的是扫频式干扰的示意。

图 4-47　扫频式干扰示意

扫频式干扰是一些宽频段电子调谐器件出现以后产生的一种干扰方法，其干扰频率能在比较宽的频段内由低到高或由高到低作周期性的变化。由于这种方法可顺序地集中干扰功率，能够达到足够高的功率密度，因此，在扫频范围内的所有雷达都会受到强烈干扰。造成雷达显示器画面闪动，无法观察和显示目标。只要合理选择扫频速度和频谱密度，可以取得很好的干扰效果。

扰时法随着高新技术广泛应用于战争，时间的军事价值日显重要。协同作战、部队进入战斗、各类兵器的发射乃至军队的衣食住行等等，无不与时间有关。时间失准会直接导致战斗失利，乃至一败涂地。

随着各类电子表和电子钟纷纷步入军营，成为指挥员贴身之物时，一种能够影响和干扰电子表(钟)走时的电波发射控制装置，已在国外悄然兴起，并已开始应用于战争。据报载，海湾战争中，以美国为首的多国部队在刮起“ 沙漠风暴 ”的同时，就曾使用这种发射控制装置，打乱了伊拉克军队的时间表。伊军在多国部队开始进攻时，表现出来的极端混乱的现象，与多国部队使用的这一新招术不无关系。

电子战招术具有广泛的渗透性，其作用范围既包括通信、雷达、制导武器和自动化指挥系统等“ 大件 ”，也囊括了电子表等“ 小件 ”，总之，一切有电子运动的地方都在敌电子攻击之列。

3.反干扰有策

电子反干扰，是电子防御措施的重要组成部分。它旨在减弱或消除敌方

干扰对己方电子设备(系统)所造成的不利影响，保障电子设备(系统)始终处于良好的工作状态。

电于反干扰是一项涉及面较大的工作，从总体上说，有战术性抗干扰措施和技术性抗干扰措施两个方面。

反干扰的战术性措施，是指为实现反干扰目的，在一定的时限内所采取的组织措施和战术措施。主要包括：

——建立隐蔽的无线电通信网络或无线电专向 建立勤务无线电网络(专向)或复式无线电台通信；组织实施无线电转信等。

——采取一些形式多变的以假护真的措施。如进行无线电佯动；实施无线电静默；适时变换无线电台的工作种类、工作方法等。

——使用反干扰联络文件。包括适时改变电台的呼号；规定相应的备用频率和规定自动改频的时间与次数；暗令的识别与选用以及通信勤务暗语的选用等。

——纵式通信网络可视情采用“双主台”和“异步属台异频”工作等。

反电子干扰的技术性措施，主要包括选择有利于反干扰的频率和电子设备的程式等。

反电子干扰的具体对策有：

隐网抗扰为保证在主要方向上的无线电通信顺畅，在建立基本通信网的同时，应伴建相应的隐蔽通信网。隐蔽通信网应尽量使用与基本通信网不同程式的电台。当基本无线电通信网遭受敌方强烈干扰无法工作，而又有重要、紧急的电报和无线电信号需要拍发时，可以应急启动隐蔽通信网。隐蔽通信网应突然出现，迅速沟通，短促工作，千方百计减少遭敌侦察、干扰的机会。

为了掩护隐蔽通信网不受敌方侦察、干扰，在隐蔽通信网开通期间，基本通信网应继续保持工作，以迷惑敌人。

隐蔽通信网应尽量使用不需要临时寻找频率的无线电收发信机，并经常处于“热备用”(即平时始终加上电源)的待命状态，以求“一联就通”。

综合抗扰根据长彼、短波、超短波无线电台以及卫星通信、微波接力通信和有线通信、简易信号通信等各种通信手段抗干扰能力的不同特点，合理搭配、综合运用，组成多手段、多频点、多层次的通信体系，做到此扰彼通，着力提高通信系统的整体抗干扰能力。

复网抗扰 为保证无线电通信在受敌方干扰情况下也能正常工作,对重要的通信方向应建立“双轨制”的通信联络，叫“复式无线电台通信”。就是用两套以上的无线电台或两个以上的通信波道来保障同一联络对象的通信。它有别于隐蔽通信网的建立。“隐网抗扰”指的是“一明一暗，以暗顶明”。而“复网抗扰”中，两套电台通常都是工作的，皆处于“明”的状态。用复式组网是保证无线电台通信免遭瞄准式干扰的有效方法。

为了提高复式无线电网的抗干扰能力，两网通常应使用各种不同程式的无线电台。如有的用短波电台，有的用超短波电台；有的用调幅制电台，有的用调频制电台；有的用双边带电台，有的用单边带电台；有的用手键报，有的用印字报等，由于程式不一，频段繁多，工作方式各异，敌方要想施加全面干扰是非常困难的。

变频抗扰进行频率捷变，是抗电子干扰的有效措施。所谓频率捷变，是指以极短的时间间隔变换频率，或由一种频率的脉冲立即变为另一种频率的脉冲。

当雷达在某一频率工作受到干扰时，通过“频率捷变”装置，能够自动快速跳到另一个频率上工作(超过于扰信号频率改变的速度)，及时将干扰甩掉。这是对付瞄准式干扰的一种良策。

对无线电通信来说，“变”的含义更多：

一是改变工作频率。在无线电通信遭受敌方强烈干扰时，报务人员应视情快速改变频卒或进行大幅度的异常改频。利用每次改频敌方尚未发觉和跟踪不及的短暂间隙，争分夺秒地进行工作。

无线电台改频可有两种方式：一是收发双方按预先的规约自动改频；另是临时通过密语进行改频。频率一变，敌方就失去了干扰目标，它又要重新进行侦察和跟踪。往往事过境迁，我方早已结束了联络。

二是改变工作种类。例如，由通话改为通报，或由通报改为通话；由通等幅报改为通调幅报，或由通调幅报改为通等幅报，由通印字报改为通移频音响报，或由通移频音响报改为通印字报等。

三是改变工作方式。例如由“单工”(同一时间内只能一方发话)改为“双工”(同一时间内双方都可发话)，或由“双工”改为“单工”等。

四是改变报务员的手法特点，或报话员的口音等。

只要灵活善变，就能收到以变抗扰，以变求通的效果。

“双主”抗扰组织和建立无线电台通信，有两种基本方式。一是无线电专向，二是无线电网络，无线专向是指两部电台之间使用共同的联络规定，进行通信的组织方法；无线电网络是指三部以上电台之间使用共同的联络规定进行通信的组织方法。见图 4-48 和图 4-49。

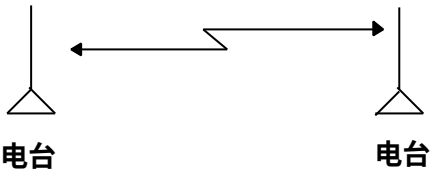


图 4-48　无线电专向通信示意

图 4-49 无线电网络通信示意

纵式无线电台通信网络通常由主台(上级台)和属台(下级台)组成。一般情况下是一个主台，数个属台，而且各属台采用同一频率工作。在遇到敌方干扰而又无法摆脱时，可以在通信网中临时设立两个主台。其中，一个是真正的主台，另一个可作为佯动台使用。这样，可分散敌方的电子对抗力量，牵制敌方的通信干扰。达到以佯护真的目的。

“近战”抗扰

“同频相扰”这是实施电子对抗的基本章法。据此，可根据己方电子侦察的情报，使用与敌方无线电台相近的频率进行工作，以阻挠敌方的电子干扰。因为敌我双方电台的频率靠得很近，敌方想干扰我们等于干扰了自己。如同近战战斗那样，由于双方短兵相接，直接影响了火力的发挥。

调零抗扰天线调零技术是一种有效的抗干扰措施。其方法是：根据敌方

干扰信号的特点，将天线对准干扰台方向调零，以降低干扰功率，形成“心形”天线辐射图，如图 4-50 所示。

目前，美军和北约部队的一些军用短波和超短波电台中，都装有天线调零处理设备，可以自动地将干扰信号强度降低到己方接收信号功率电平以下。在海湾战争期间，这种带有调零技术的无线电台，为海湾前线至美国本上间提供了可靠的抗干扰保密通信。美国海军使用的 FRQ 高倾自适应调零系统，可以自动识别传输信号和干扰信号，在海湾实战使用中效果很好。美国 ECI 公司

图 4-50 调零抗干扰示意

为美军研制的无线电通信系统，在采用调零技术的同时，还使用了大功率放大器来增强抗干扰能力，受到美军的重视和推广。

巧用天线 天线是无线电通信的“门户”，对提高抗干扰能力影响很大。在保障通信联络顺畅的前提 F，应尽量缩短天线长度，低架发信天线和采用定向天线。

定向天线是一种方向性很强的天线。使用这种天线，即使不提高发信机的输出功率，也能在接收点获得较大的信号电平。因而可以提高接收机输入端的信号/干扰比，保持了在干扰条件下的通信稳定性。

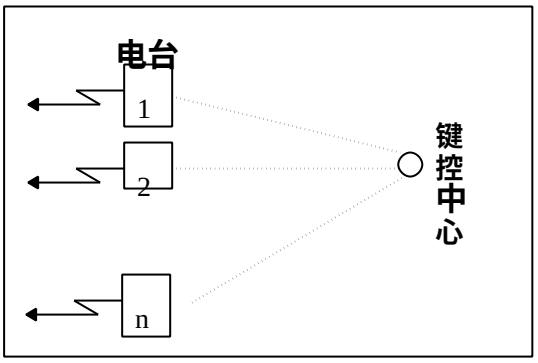


图 4-51　一键多控示意

多频抗扰为了分散敌方的电子干扰力量，必要时可以使用两部以上发信机，由一个键控设备控制，在不同频率上同时进行发信(如图 4-51 所示)。收信端则在几个不同频率上有选择地进行接收，以筛选出最好的信号来。

为使敌方干扰顾此失彼，键控的各无线电台，宜选用不同频率范围、不同调制方式和不同工作种类。如果因器材条件不具备，也可以使用同一类型的电台，但是应该选用各种不同的工作方式，如有的用“话”，有的用“报”；有的用移频音响报，有的用印字报；有的用单边帝话，有的用调幅话等。由于五花八门，敌方要想进行多方面的干扰是很不容易的。

屏蔽抗扰 从屏蔽角度看，抗干扰的措施有两种：一种是“物理屏蔽”措施，即充分利用地形、地物，避开敌方干扰机对己方电子系统的直接辐射干扰。另一种是“电磁屏蔽”，即采用一些抗电磁设施保护电子系统正常工作。应使用金属薄板(网)和金属套管，屏蔽电子通信设备和外部线缆，条件许可

时，最好将安装电子通信设备的工事和车辆全部屏蔽。有了屏蔽措施。好比是给电子系统穿上了一套防干扰的服装。可将敌方干扰的影响减低到最小限度。

以“硬”抗扰 在实施反干扰斗争中，“硬抗”是一项较有力的措施。它融通信人员机智、意志和过硬的本领于一体，特别是在情况紧急，来不及采取其他措施或采取其他措施无效时，必须坚持硬抗。对越自卫还击作战中，就有一个这样的范例；在夺取某高地的激烈战斗中，一天，我指挥所正在和前沿部队通报，越军向我电台施放了强烈干扰。“改频”(即通报双方临时改变通报的频率)来不及了。某部报务员凭着平时练就的高超的抗干扰技术，采取“压码抄收”(就是将听来的电报电码，临时在头脑里作适当储存，待判断准确后，再抄写在电报纸上)，用“硬抗”的方法对付。在几股强烈的干扰信号中，硬是“滤”出了指挥所发出的电码信号。越军报务员眼看一计不成又生一计，他们加大了干扰台的发射功率，企图用强大的信号“压倒”我台。我部报务员机敏沉着，迅速用暗令告诉对方快速改频，与越军展开斗智进行周旋。在新改的频率上刚刚开始联络，越军又施展了“跟踪干扰”，我报务员将计就计，先用暗语告诉对方静默，为了迷惑越军，再假意通知对方“改用五号频率”，越军信以为真，立即将干扰信号转移到五号频率上。稍事静默后，我军电台突然又在原来的频率上恢复了联络，巧妙地甩掉了对方的干扰，终于将敌情通报出去。我炮兵立即按电台报务员所报的方位，摧毁了该高地上的越军主要火力点，我军随即攻占了这一高地。这是电子抗争中，“硬抗”加“巧抗”的胜利。

(三)摧毁与反摧毁

在高技术战争中，电子战仅仅依靠电子干扰这一软杀伤手段已不能满足作战需要，必须在采用软杀伤的同时，大量采用硬杀伤手段。即在电子侦察的配合下，对敌方的电子设备(系统)，尤其是一些高价值目标，实施电子、火力摧毁，使之永久失效乃至完全破坏。

为了做好对敌方电子、火力摧毁的防护，必须采取各种抗毁措施，尤其要使己方的通信、雷达等电子设备能经受第一次电子打击或大批次空袭的破坏。

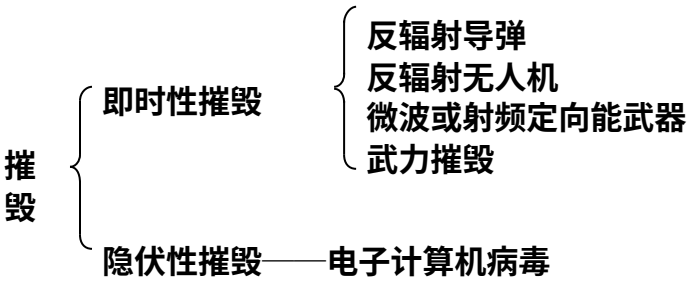
1.别具一格的摧毁“弹”

摧毁敌方的电子设备和系统，除了使用爆炸能武器外，还大量使用了电磁能武器和电子计算机病毒。其中包括反辐射导弹、反雷达导弹，高能激光器、粒子束武器、微波(毫米波)射束武器和等离子射束武器，以及电子计算机战武器等。这些别具一格的杀伤武器，具有威力大、难防护等特点，是电子战武器库中最富有攻击力的代表。

2 摧毁有术

对敌方电子设备(系统)实施硬摧毁通常有两种状态：一是即时性摧毁，二是潜伏性摧毁。

“即时性摧毁”是指摧毁武器作用到电子设备(系统)后，会立即使电子设备(系统)受损乃至摧毁；“隐伏性摧毁”是指摧毁武器作用到电子设备(系统)后，并不立即使食摧毁，而是潜伏在电子设备(系统)中，伺机发生摧毁效能。如下所示。



对敌电子设备(系统)实施硬摧毁的具体方法很多，主要有：

引弹入室这里的“弹”主要是指反辐射导弹。这是一种专门用于击毁敌方电磁辐射源的导弹。

我们知道，通信、雷达等电子设备作为保障作战指挥的电磁辐射体，一旦开机工作，就形成了一个很容易被敌方侦察定位的辐射源。这就给反辐射导弹以可击之隙。

反辐射导弹属于精确制导武器，通常由导引头、战斗部、发动机和控制系统等组成。这种导弹主要用来对付雷达，并利用雷达射出的波束进行自动制导的。一旦当飞机被雷达的波束“跟踪盯梢”，飞机就会立即采取“以攻

对攻”的方法，放出反辐射导弹，迅速、自动顺着雷达的波束直奔雷达打来，令雷达防不胜防。图 4-52 表达的是反雷达辐射导弹攻击雷达设备的示意。用反雷达辐射导弹对付雷达，犹如朝在黑暗中打着手电筒的哨兵射击那样，命中率极高，几乎是弹无虚发。

新型的反辐射导弹上都安装有记忆储存装置，即使雷达在被发现后关机，也不能幸免于难。这就告诉我们，谁向外辐射电磁波，谁就会被反辐射导弹“咬住”并随之跟踪，从而“引弹入室”遭到灭顶之灾。

反辐射导弹最早应用于战争，是 1965 年在越南战场上，使越南北方的雷达损失率激增。1986 年，美国空袭利比亚时，使用了

图 4-52　反雷达辐射导弹攻

反辐射导弹这把“手术刀”，一举摧毁了利的雷达防空体系，为美军攻击机群开辟了安全的空中走廊，打了一场有史以来罕见的“外科手术式”的战争。海湾战争中，美国的标准轰炸机上都普遍装备有反辐射导弹，对摧毁伊拉克的雷达系统发挥了很大作用。

反辐射导弹问世以来，经历了三代产品。第一代以美国的专打炮瞄雷达的空地导弹——“百舌鸟”为代表。由于它频率覆盖面窄、精度差、威力小，到 70 年代初期即被第二代所替代。这代产品对雷达频率覆盖面加宽了，并加装了记忆电路，可赁预先输入的记忆信息攻击关机后的雷达。但设备体积大，不便于机动。

第三代产品采用了最新的微波技术、信号处理技术和集成电路宽频带导引头，可采用陆地、海上和空中三类载体进行发射，可捕捉、跟踪和攻击地面的、舰载的和机载的各种雷达。这种新型的反辐射雷达导弹，在 1986 年至 1987 年的乍得和利比亚冲突中首次用于战场。乍得军队使用这种导弹有效地压制了利比亚的防空雷达系统和防空导弹系统。在 1991 年的海湾战争中它又显神通。

兵由于降　反辐射武器是一种进攻性的“硬杀伤”武器，除了反辐射导弹外，还有反辐射无人机。它们都是利用雷达的电磁辐射对雷达进行寻的、跟踪，直至摧毁。

反辐射无人机，是在无人驾驶飞机上装配被动雷达导引头和战斗部。它的运用方式通常是在战场上空巡航。比反辐射导弹造价低、使用灵活，具有很强的摧毁力。

执行任务时，反辐射无人机先飞临敌方上空，居高临下地鸟瞰敌地域内的雷达设施，搜索和识别其电磁辐射信号，然后，按优先等级对敌方雷达实施攻击和摧毁。反辐射无人机上天后，若未发现攻击目标，就在敌方上空盘旋飞行。只要目标一出现，便“兵由天降”对其实施攻击。

反辐射无人机自本世纪 70 年代未开始起步研制，目前已在军旅中服役，并已被派往海湾战场上。预计，90 年代反辐射无人机将陆续装备部队。据报道，美国正在研制一种取名为“默红”的反辐射无人机，其频率覆盖面达 35 千兆赫以上，不久即可投入使用。

反辐射无人机和反辐射导弹，从诞生至今时间并不长，但己发挥重要作用。今后，随着各种先进技术的运用，发展融电子侦享、电子干扰和反辐射武器为一体的软硬结合的杀伤手段，对敌方指挥控制系统和雷达系统进行压制和摧毁，将是一个明显的趋势。

发射隐弹　为了一次性的摧毁敌方的 C3I 系统，现已出现了一种隐形、高速、超远程和智能化综合一体的导弹。其效果比用隐形飞机搭载精确制导武器更好。能自动搜索、识别和攻击目标、装有微型雷达和高速电脑的隐形智能巡航导弹也将问世。

病“毒”武器　由于电子计算机广泛运用于作战指挥系统和其他军事领域，并成为指挥、控制的神经中枢，因而破坏电子计算机的正常工作，已成为电子战的新目标。国外有些军事部门正大力研制一种旨在破坏电子计算机正常工作的新式武器——计算机战武器。它是把电子计算机病毒注入对方武器系统和电子设备中的计算机，隐藏在计算机的操作系统中，也可潜伏在数据文件中，利用系统的数据资源进行繁殖，并通过系统数据共享的途径进行传染，使其不能正常工作。计算机病毒武器的具体情况，详见本书“电子战族绽新蕾”一节中的“毁脑幽灵”。

微“波”武器　指的是以微波为武器，对点状的电子目标实施杀伤。

微波是一种波长很短的电磁波。具有传播速度快，穿透能力强等特点。随着高新技术的发展，微波技术已由通信、探测、跟踪、制导等方面的应用扩展到杀伤武器领域。“微波”武器就是利用强微波束能量杀伤目标的一种武器。它的工作原理和微波雷达相似，但其能量要大于微波雷达上千倍乃至万倍以上。微波武器系统由超高功率微波发射机、大型发射天线以及其他辅助设备组成。超高功率微波经过天线聚集成一束很窄的电波，像一把锋利的尖刀，以极高的强度“刺”向对方的电子设备。并以高能量辐射场覆盖被攻击的点状目标。在目标内部的电气元件和电子线路中产生致命的电压和电流，击穿或烧毁电路系统中的敏感元件；使电脑存贮器丧失所存贮的信息，软件毁损。据测计，每平方厘米 0.01～1 微瓦的微波能量，可以有效地干扰相应频段的雷达和通信设备的正常工作。每平方厘米 0.01～ 1 瓦的微波能量辐射，足可使通信、雷达、导航等系统的电子设备失效或烧毁。每平方厘米 10～100 瓦的微波辐射所形成的瞬变电磁场可使卫星和导弹等武器系统中的电子设施受到破坏，不管这些设备是不是工作在微波频段。

本世纪，80 年代以来，特别是海湾战争以后，世界各发达国家的军队正在加紧研制开发微波炸弹的技术，一种“按需要释放能量”的微波炸弹即将步入战争舞台。

此外，国外近几年出现了一种电磁波脉冲产生器，其效应与高空核爆炸的作用类似。只是作用的范围局限于一个有限的区域。这样，即使在不发生核战争的情况下，电子设备(系统)也会受到电磁波脉冲袭击的危险。

武力摧毁　在电子侦察的基础上，运用兵力与火力相结合，摧毁敌通信、雷达和电子对抗设备，这是一项重要的制敌方法。

运用武力摧毁敌电子系统可利用深入敌纵深的侦察和穿插渗透分队，以及地方武装进行捣毁，也可利用各方面的电子情报，及时判明敌方电子设备数量、功能和配置地点，引导我炮兵、航空兵火力予以摧毁。这方面的战例几乎顺手可拾。

1082 年，英阿马岛战争初期，阿军对英军的无线电通信施加了强大的电子干扰，破坏了英军的指挥、控制系统，取得了胜利。战争末期，英军“以牙还牙”，使用了先进的电子侦察设备，在极短的时间内迅速测定阿军的电台方位，并用强大炮火进行摧毁，使阿军指挥失灵，终于战而胜之。

3.反摧毁有招

电子设备(系统)免遭敌方摧毁，有战术性措施和技术性措施两个方面，就当前科学技术水平而言，反摧毁方法主要是几个“建立”，如下所示：

反摧毁措施
- **建立多信道传输网络**
- **建立综合通信系统**
- **建立机动通信体系**
- **建立电子计算机防病毒设施**
- **建立雷达透饵阵**
- **建立掘壕入洞通信**
- **建立交换开机的战术程式**

具体地讲，反摧毁措施有：

巧织网络

通信网络的结构形式如例，直接影响到通信系统的抗毁、生存能力。

日常生活中有许许多多类似这样的现象：甲乙两地倘若只有一条公路联接，一旦公路遭敌轰炸，两地间交通就会中断。如果有数条公路联接，就可做到此断彼通。交通是如此，通信又何尝不是这样。

通信网络通常由用户终端、传输信道和交换设备三个部分组成。其中，交换中心(也叫通信节点)和传输信道，在通信网络中处于主干地位。

如图 4-53(a)，当四个交换节点彼此联通组成格形网络时，假设当 1、2 交换节点间的信道中断，可以通过 3、4 交换节点进行迂回通信；当四个交换中心按栅格网(图 4-53b)联接时，迂回通信的路由较格型网增加；当四个交换中心按网状网联接时(图 4-53c)，

图 4-53　通信网络的结构形式

迂回通信的路由最多。运用排列求和公式。

路由数 $(R)=\sum_{k=0}^{n=2} A_{n-2}^{K}$

n——交换节点数

K——交换转接的次数

可以算出，从通信始端到通信终端的路由共 5 条(图 4－54a)。由于路由较多，当通信网内的传输信道和交换中心局部受损时，只是影响用户一定的呼损率，仍能保证生存用户的通信。不像辐射式通信那样，当某些重要通信枢纽、台站或传输信道被毁，会影响通信联络的全局。辐射式网也叫树型网，见图 4－55 所示。

图 4-54　网状网的通信路由

同理，当 5 个通信节点进行“点点互联”时，从通信始端到通信终端共有 16 条路由(图 4－54b)；当 6 个通信节点互相联接时，从通信始端到通信终端共有 65 条路由(图 4－54c)。由于路由众多，既有直达路由又有迂回电

路，信息多径可传，能有效增强通信系统的抗毁性。

综合抗毁就是采用综合通信系统实施抗毁。这是“东方不亮西方亮，黑了南方有北方”的游击战术在通信对抗中的运用。

图 4-55　辐射式网络抗毁能力低

“综”有四层含义：一是综合运用各种通信网络，包括平面网和立体网两大范畴，建立起平面与立体相结合的网络体系。平面通信网有地域通信网(图 4-56)，局域通信网，广域通信网，移动通信网和固定通信网等。立体通信网是指将通信交换中心设于空中(包括设在直升飞机上或系留气球中)，或置于通信卫星上。

图 4-56　地域通信网组成示意

利用安装在系留气球、直升飞机和通信卫星上的通信设备进行空中转信，如图 4-57 所示。当地面通信网络受毁时，可通过空中转信站维系通信。

图 4-57　空中转信示意

二是综合运用各种通信方式，主要包括有线电通信，有线光通信，无线电通信，无线光通信，无线电接力通信，卫星通信等：三是综合运用各种通信手段，包括电话通信以及电报、传真、数据传输、图文电视、话音信箱、电子函件等”非电话通信”等；四是综合运用各种工作方式，包括双工、半双工和单工等。

在综合通信系统中，由于信息多径可传，此断彼通；多种手段运用，此阻彼达；通信要素分散配置，此毁彼存。有效地提高了通信系统的生存能力。

机动抗毁　即广泛运用机动通信，增强快速机动能力。建立通信联络时要“动静结合，以动力主”。大力发展车载、机载和用户移动通信系统，做到“动中通”。实战表明，发展机动通信。是提高通信生存能力不可缺少的有效途径。

掩蔽抗毁　掩蔽泛指各种通信设施要构筑掩体，以及建立地下通信和构筑地下工事等。在通信枢纽的建设上，必须充分注意研究提高抗毁性和稳定性。做到地上与地下相结合，固定通信系统与野战通信系统相结合，有线电通信与无线电通信相结合。一些大、中型通信枢纽一定要建在地下，而且要具有抗轰炸、防核电磁脉冲冲击、防敌电磁侦察、防太空电磁侦察、防电磁干扰和摧毁等措施。一些重要通信枢纽和雷达设施应做到地上地下互为备份，并具有由地上迅速转入地下的机制。

在掩蔽抗毁方面，海湾战争为我们提供了有益的借鉴。海湾战争开始的前 10 天，多国部队对伊拉克的空袭就达 2 万多架次。伊军在遭到连续空袭，地面通信设施遭到严重破坏情况下，仍能通过既设的通信系统向部队发号施令，这是与伊拉克经过多年建设，有一套比较完备的、坚固的地下通信设施分不开。正如权威人士指出的，从海湾战争看，地下工事很重要，以美国为首的多国部队出动了那么多的飞机，投下了那么多的炸弹，但没有从根本上解决问题。

设卡防毒　随着电脑病毒的出现，许许多多防毒、解毒的招术应运而生。概括地说，有“检、消、堵、变、防、清”六术。即电子计算机开机后，先用病毒检测软件进行检测，确认其无病毒感染后，方可投入运行；计算机“病毒”有别于正常运行的软件程序，所以它在侵犯健康“肌体”，必然会露出马脚，要立即采取隔离措施予以消除，切莫使它作祟；严格控制软件来源，切实堵塞电脑病毒的各种传播途径；改变电脑运行时间，以防病毒发作(如躲开十三号星期五，避免“黑色星期五”病毒发作)；给电子计算机配装“电脑病毒预防卡”，如置一名“守门卫士”，可将电脑病毒“拒之门外”，从而极大地增强了电子计算机的免疫、防病能力；对计算机设备及其软件和磁介质，要经常进行清理，以防患于未然。随着科学技术的发展，各种“以毒攻毒”、“以毒治毒”的方法将会搬上战争舞台，到那时，抗击计算机病毒侵袭将会发生突破性的进展，电子对抗将步入一个新的时代。

五、光电对抗展雄姿

光电对抗是电子对抗中的一个重要分支。论资历，它比通信对抗和雷达对抗都浅，迄今还不到“不惑”之年。但它发展甚为迅速，并具有很大的后劲，在电子对抗领域大有独占鳌头之势，成为现代战争中不可缺少的作战手段。

光电对抗是随着各种光电技术武器、装备的迅速发展而发展起来的，它所以特别惹人注目，并成为现代战争中电子对抗的发展方向，是由于它对付的不是一股的“人物”——光束制导武器。

(一)光束制导有短长

在世界现代武器库中，军事专家们常将精确制导武器喻为武库的“皇冠”，“激光制导武器”则是皇冠上的明珠。激光制导武器与激光武器不同，激光武器是以“激光”作“弹头”，而激光制导武器，用于杀伤和摧毁目标的不是激光束，而是一般的炸弹、炮弹和导弹。这种用激光制导的方式，相当于给各种弹头安装上一对“火眼金睛”，使它们像狗追兔子一样，紧紧盯住目标，穷追不放，直到将它摧毁。

图 5-1 所示是激光制导导弹作战示意图。射手首先借助于“激光目标指示器”，用激光束照射目际，激光束在目标上产生漫反射，总有一部分激光反射到导弹上，被导弹的“寻的器”所接收。于是，导弹就可根据目标慢反射的激光能量，自动搜索、捕捉、识别和跟踪目标，直至将目标打掉。

激光束是当今世界上方向性最好的光，它几乎是一束平行而准直的细线，发散角极小，因此，激光制导武器的命中精度极高。

图 5-1　激光制导导弹作战示意

它刚问世时,激光制导炸弹的圆误差概率大约只有 3 到 6 米(常规的炸弹则为 300 米左右)，随着制导技术的发展，命中精度愈来愈高。据战场上的慨率统计表明，激光制导武器的首发命中率，现在几乎是百分之百，“打出去不用管”、“指哪打哪”。加上激光束跑得很快，每秒约 30 万公里，这在数百米乃至数百公里距离内几乎是“实时”的，使人防不胜防。其作战效能要比无制导武器起码大 200 倍以上。

激光制导武器应用于战争是从 1972 年美军在越南战场上首次投下激光制导炸弹开始。据报载，美军曾为轰炸越南北方桥梁出动飞机近 700 架次，投弹数千吨，结果“抓鸡不成反蚀一把米”。不仅桥未被炸毁，反而自己付出了毁机近 20 架的代价。后改用激光制导炸弹，取得了惊人的效果。不到两小时，炸毁桥梁 17 座，而飞机无一损伤。1986 年，美军飞机利用夜幕长途奔袭利比亚，在先进的机载前视红外装置、激光测距机和激光目标照射器引导下，用激光制导炸弹准确地对卡扎菲总部和驻地实施轰炸，成功地取得了“外科手术”式的作战效果。海湾战争中，以美国为首的多国部队运用激光制导炸弹炸毁了大量的伊拉克用钢筋混凝土等严密加固的飞机库，有近五分之四座桥梁被摧毁。美军事首脑评价说，在第二次世界大战期间，要摧毁一个钢筋混凝土隐蔽部需要用近 10000 枚炸弹，在越南战争期间，要用 300 枚，而现在用 F-117A 飞机载一枚激光制导炸弹即可完成任务,战场效费比变化之大，令人瞠目结舌。图 5-2 所示的，是激光制导炸弹击中地面目标，直飞汽车驾驶室的瞬间情景。

图 5-2　激光制导炸弹击中地面目标的情景

然而，任何技术武器系统，哪怕是高技术武器系统都不可避免地有它的弱点，总可以找到对付它的办法。制导用的激光束，因波长单一旦极细窄，虽难以被敌方截获和干扰，但它易受大气，如云雾、雨雪、浮尘和大气流、烟雾等的影响。轻者降低信号传输质量，重者造成信号中断。因为光是直线传输的，传输距离易受自然的或人为障碍的限制。如果，在光电装备使用的

工作光波中，掺进人为的假信息，或采用特殊方式隐去目标的光学特征，使依赖光信息工作的光电装备无法识别，同样也使其不能正常工作。甚至出现不听招呼，瞎导一气。此外，光电装备上的光敏器件通常都比较脆弱，它所能承受的光强度有一定的限制，一旦超过限值，就会使光敏器件过载、失效，甚至完全被损坏，使整个光电装备瘫痪。

光电武器和光电侦察器材上述这些弱点，正好为光电对抗提供了可乘之机，旨在使对方的光电武器系统失灵、光电侦察器材迷盲的光电对抗技术正是在这种情况下应运而生，并得到了迅速的发展。

(二)光电对抗话哥仨

在“电子对抗媒质多”一节中，我们曾经提到，光辐射是一种普通的自然现象。光波与无线电波是一类东西，同归属于电磁波大家庭。所不同的仅是“波长”或“频率”有异。光波波长范围在电磁波谱的 0.

06 微米到 1000 微米之间。光辐射中，有人眼看得见的，也有人眼感觉不到的。按视觉和波长差异，光波通常还可划分为紫外光、可见光和红外光三个波段。在可见光与不可见光中，都可产生激光。所谓“光电对抗”；通俗地说，是指敌对双方在红外光波、可见光波、紫外光波等波段，利用光电设备、器材或其他设施所进行的电磁斗争。斗争的范畴，又部涉及激光、红外光和可见光三个技术领域，所以，人们习惯上又把光电对抗分为激光对抗，红外光对抗和可见光对抗三种。它们犹如光电对抗中的哥仨，各具特色。

由于红外光、可见光和激光三种光波的发光机理是不同的，因此，对探测者所引起的视觉效果和光电对抗中采取的探测手段，也各有所异。

红外光的发光机理是基于物体分子振动状态改变发出的辐射，不能引起视觉效应。但它具有明显的热效应现象。因此，可借助于温差电偶、光敏电阻、光电管等器件进行探测。

可见光的发光机理是基于原子或分子运动状态改变发出的辐射，可以引起视觉，用目视的方法即可进行探测。

激光的发光机理是基于原子中的电子，在外来光或电进行激发时，因能级发生变化所释放出的光子。其发光波长可选在可见光波段，也可选在不可见光波段(例如，选在红外光波段)。前者，可引起视觉，后者不能引起视觉，需借助于光电器件进行探测。

就电子战的战法而言，光电对抗如同一般的电子对抗那样，在攻的一方，有光电侦察，光电干扰和光电摧毁；在防的一方，相对应的有反光电侦察，反光电干扰和反光电摧毁。正是这三部曲，奏响了光电对抗的乐章。

(三)侦察——干扰——摧毁

侦察、干扰和摧毁是实施光电进攻的完整过程。它是指敌对双方在红(紫)外光波、可见光波等波段，利用光电设备、器材·获取对方光电武器的工作信息，然后采取相应措施，削弱、破坏其作战效能，并保护己方人员和光电武器的正常工作。使自己耳聪目明，使敌人耳聋目瞎。

1.光电侦察

光电侦察的具体方法很多，概括起来有两大类，即被动侦察和主动侦察。

(1)被动侦察

侦察结果最终要作用到人眼或探测仪器上。如果被侦察的目标本身有光电辐射，这种侦察属“被动侦察”。这时，利用各种探测器甚至人眼，就可接收到对方的光电辐射，达到侦察的目的。激光侦察机、红外侦察器就是常用的一种被动式光电侦察工具。

利用激光侦察机可以直接截获对方激光系统发射出的激光束，通过光电转换装置将探测到的激光能量转换成电信号，经过电子计算机和信号处理装置，从而获知对方激光束的技术参数，如波长、带宽、重复频率、编码等，以便采取对抗措施。

利用红外侦察器可以侦察和探恻导弹的飞行轨迹。当红外侦察器接收到导弹飞行过程中所辐射出的红外线时，便以声或光的形式发出报警信号。利用目标的红外辐射特性的差异还可鉴别出目标的性质与类型。

现在世界各国军队普遍使用的红外夜视器材，也是红外侦察技术的应用领域之一。它是利用目标自身辐射出的红外线实现成象观察的。红外夜视探恻技术早在第二次世界大战期间就得到了广泛应用。德国军队率先在运输车辆上安装了红外夜视仪，利用夜暗成功地避开了同盟国军队的监视与空袭，巧妙地将导弹迅速输送到前线。进入 80 年代，红外夜视器材不仅没有逊色，使用更为广泛。英阿马岛战争中，英军凭借着先进的红外夜视器材，在“伸手不见五指”的夜晚发起总攻，使阿军惨遭失败。高度发达的夜视器材，使单纯利用夜幕掩护夜战的方法失去了以往的光彩。

(2)主动侦察

光电“主动侦察”，是指利用对方光电装备的光学特性而进行的侦察。即向对方发射光束，再对反射回来的光信号进行分析和识别。因为不同的光学系统具有不同的反射特性，这样，就可以确定对方所用光学系统的性能、类型等。

这种利用被侦察光学系统的回反特性进行的侦察，又称为逆反射技术”。号称“雷达新蕾”的激光雷达就是根据这一原理进行工作的。

普通雷达采用微波波段工作，需要庞大的天线系统，天线直径大的达几十米以上，小的也要几十厘米到几米。由于激光的频率比微米高，它的波长仅为微波波长的几万分之一，无线可以做得小巧，只需几厘米即可。激光亮度高，单色性好，射向直，射束窄，用它进行侦察、测距、测角，精确度很高，分辨力很强，是当今电子对抗领域中的佼佼者。图 5-3 所示的是激光雷达的外形。

2.光电干扰与摧毁

光电干扰的具体方法很多，概括起来，有“积极干扰”和“消极干扰”两类。

(1)积极干扰

图5–3 激光雷达

积极干扰也叫“有源干扰”，它是用强光束(或强信号)直接瞄准对方的光电接收系统中的“眼睛”——传感器。令其错误工作或无法工作，以致彻底将它摧毁。

积极干扰是当前激光对抗中最有效的杀伤手段，它处于主动对抗地位。图 5-4 所示的是来袭激光制导导弹攻击飞机时，飞行员用强激光束(反导激光束)照射导弹，使导弹上的光电探测器件顿时失灵。结果，导弹致盲失控，坠毁自焚。这种光电对抗手段也称“致盲压制式激光干扰”。据报载，美军早在 1989 年，使用这种“光枪”，首次成功地击落了在新墨西哥洲沙漠上空，高速飞行的一个目标。

图 5-4 激光主动对抗示意

强激光束除了会使传感器致盲外，还会直接伤害人的眼睛，使其视网膜大面积出血甚至完全破坏。试想，一个双目失明的人在现代战场上是很少有战斗力的。此外，若视觉系统受到突然冲击和破坏，还会危及大脑神经系统引起全身受损。

在光电对抗中，除了以“光”为“弹”先发制人外，还常采取“以骗扰敌”、“以假乱真”等手法。

“以骗扰敌”，是一种“回答式欺骗干扰”。就是当接收到对方的激光束脉冲后，以相同的脉冲形式“回敬”对方，但在时间上稍许错开，使对方的光电系统受骗，造成误动。打个比方，当我们发现敌激光制导导弹将袭击我地面上某个战略目标时，就用与敌制导导弹所用的激光束相似的激光，去照射被袭目标附近的别的地物，或特设的反射镜、角反射器等物体，它们反射的激光中作用到敌导弹上，就能有钞地诱骗导弹改变方向，去攻击其他目标。

“以假乱真”是人们对“激光诱饵”和“红外诱饵”的形象写照。说的是，当发现对方使闸激光(或红外)制导武器时，可采用有源干扰技术给制导武器发送假信息。制导武器的寻的装置此时同时收到真目标和干扰机的信息，致使制导的信号混乱，从而不能准确导向真目标而使弹头脱靶。

如果确认对方使用的是激光制寻武器，可用与对方激光目标指示器特征参数相同的激光器，照射同真目标相距较远的、具有较强反射特性的假目标，形成一个能量比真目标反射能量强约 10 倍的反射光锥束，达到将对方制导武器引向假目标的目的。这种“以假乱真”的干扰方法又称为“激光诱饵”。

如果确认对方使用的是红外制寻武器，可以适时施放红外干扰弹(又称为红外诱饵弹)，它是一种能朝制导武器辐射出比真目标辐射红外能量大数倍的热体。其辐时的波长与真目标相似，这样，就可以使来袭制导武器优先跟踪干扰弹，真目标则趁机得到保护。在越南战争期间美军就曾施放红外诱饵弹对付越南使用的红外制导导弹。图 5.5 所示的是红外干扰设备的实物。

图 5.5 红外干扰机

在一定的气象条件下，大气对激光束具有较好的散射作用。为了有效地干扰对方的光电系统，可以用多台激光干扰机组成大规野的大气散射，相当于在空中撒布一只“激光网”，只要对方激光制导武器进入“网”内，就会受到干扰。

“引弹自毁”也是“积极干扰”的一种战术。此处的“弹”，是指“反激光辐射导弹”。这种导弹类似于电子对抗技术中的反辐射导弹——“百舌鸟”导弹。反激光辐射导弹能自动沿激光束直接追踪并摧毁对方激光系统。

(2)消极干扰

光电对抗中的“消极干扰”，是指采用涂料、烟雾等物痤的方法，以掩盖目标的真实特性，使对方的侦察设备产生错觉甚至失灵。“消极干扰”虽是一项古老的技术，但由于它独具特色，仍是当前光电对抗中的一种重要手段。

消极干扰也叫“无源干扰”。尽管其方法很多，但都是环绕这样两个问题做文章，即怎样吸收或分散光波辐射能量？如何人为地改变目标的光学特性。

在军事目标(如车辆、飞机、舰艇等)上涂上具有高吸收率的涂料，当对方激光器照射到目标上时，绝大部分的能量都被目标吸收了，使回波能量大大减少，从而降低了对方激光系统的作用。如果涂上高反射特性的材料，可以将绝大部分的入射光反射回去，同样可以达到目标免受攻击的目的。

激光、红外光和可见光有怕烟雾的弊病，利用这一弱点，可用施放烟幕尘沙等方法，对敌方的光电侦察实施干扰。越南战争期间，美国空军采用激光制导炸弹攻击越南许多重要桥梁和地面目标，一开始，命中率很高，后因越南适时施放了烟幕，竟使美军轰炸河内某发电厂时，投掷了数十枚激光制导炸弹而无一命中。尘上对光波也有根强的遮蔽能力，现在有的坦克、汽车上安装了一种“尘土产生器”，能自动地将坦克、汽车在行驶中履带、车轮扬起的尘土收集起来，快速烘干、粉碎，然后再施撒出去，弥散在坦克、汽车的周围，使对方向坦克、汽车发射的激光受阻，能量很快衰减。据计，在一定浓度情况下，衰减率可达 95%以上。

“以烟障目，战而胜之，”这是一项传统战法。伴随着科学技术的发展，军用烟幕的迷盲性能已今非昔比。

早期的军用烟幕，只能干扰与遮蔽可见光与近红外光，这时工作频段己向中远红外甚至毫米波方向扩展的现代光电探测技术来说，已遮蔽不了它们的“眼睛”。因此，大力发展具有“全彼段”(从可见光到红外光)“障目”能力的军用烟幕己引起了世界各国军队的普遍重视，并已广泛应用于作战车辆。美军在海湾战场上所使用的坦克和战车上，大都装有这种发烟榴弹。作用波段从可见光一直到远红外甚至毫米波的新型第二代发烟机，近来已被北约国家研制成功。

早期的军用烟幕成烟速度慢，烟雾浓度低，持续时问短，而且都是单色的。如今，军用烟幕发射后 2.5 秒钟，就可在发射车外 25 米处筑起一道宽 60 米、高 8～10 米的“烟墙”，在时速 24 公里的风力下可以持续 3 分钟。美国新近研制的 XM-57 型发烟机和英国研制的 SG-18 型发烟机，“障目”效

能更好。发烟后很短时间内，即可在战场上形成一道高 50 米、宽 30 米至几千米、持续时间几分钟到几十分钟的抗远红外“ 烟雾堡垒 ”。能有效地使坦克和装甲战车避开目视和目前所有热成像装置、光学瞄准具以及激光测距仪的观察，极大地提高了战场生存能力和战斗力、成为现代战场上一种高效费比的“ 软防御 ”手段。此外，彩色烟幕也已研制成功。可根据不同的使用环境、地形背景施放不同颜色的烟幕，从而，更加提高厂其 ”‘ 障目 ”作用。敌方要想寻找真正目标那是非常困难的。

近来，在光电对抗领域中，还广泛使用了金属箔条。就是在军事目标上空，投放类似于电子对抗中用的干扰丝、干扰条，”它们对激光具有强叵射的作用，以此产生假目标，扰乱对方视线进行欺骗干扰。

(四)反侦察——反干扰——反摧毁

光电对抗领域中的反侦察与反干扰、反摧毁是指防御敌方对己方光电装备的发现，探测和干扰、摧毁，而采取的相应措施。具体的战法很多，有如：

伪装抗侦“巧施伪装”是现代战场上抗敌光电侦察的常用方法。我们知道，不论哪种日视器材(包括夜视器材在内〕，都是利用目标与背景反射或辐射光线的差别成像来分辨目标的。而伪装正是减少目标与背景间叵射或辐射光线之差的有效措施。实战表明，无论采用天然伪装(包括利用地形、地貌和植被伪装等)、就便器材伪装、制武器材伪装和迷彩伪装均能有效地对付主动红外夜视仪的侦察和探侧。据试验，利用颜料和染料进行迷彩伪装。可降低红外夜视器材观察效果的 40%左右。利用伪装，对付激光夜视侦察和对付热像仪侦察，均能取得良好的效果。实战表明，用微光夜视器材侦察地形地物，伪装的比不伪装的，能降低观察效果接近 40%。

编码抗扰　为避免激光制导武器受到外界光照干扰而迷盲，可以给激光制导信号通过加密措施进行编码，只要对方不知密钥，干扰机发射的激光束不是与它相同的密码脉冲，制导武器就绝不会被迷惑。因而大大地提高了抗干扰能力。如果在此基础上，再采用复式制导方式，其抗干扰能力则就更强。“复式制导”是指用多种方式对制导武器同时实施制导，当某一种制寻方式夫效后，另一种制导方式就会自动接替仍起作用，继续将导弹引向目标。

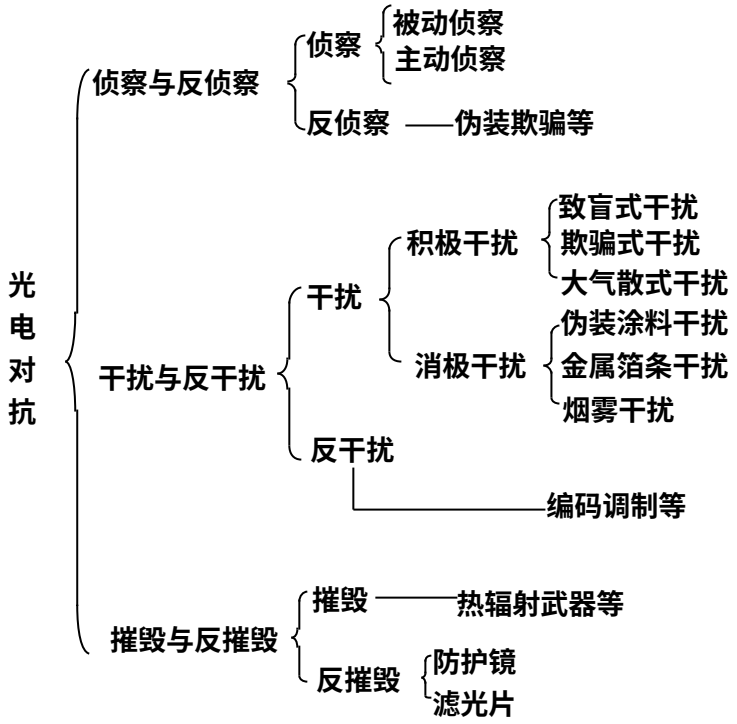
滤光抗毁　为避免激光致盲武器对人眼的伤害，可以在望远镜上配用各种激光波长的滤光片。滤光片好似一只“光筛子”，能阻止某些波长的激光通过，或将它们反射掉(图 5-6)，或将它们吸收掉，可以允许通过的激光为数甚少，对眼睛无甚危害。

不仅可以给战场人员配戴激光防护镜，各种光学仪器同样也

图 5-6　反射型防护镜

可戴上。目前，不少国家的军用光学仪器上都配备有变色镜，当强激光照射到透镜上时，透镜能在很短的时间内自动析出大量的银质粒子，对激光产生强烈的反射作甲而阻止其通过。当强激光消失后，透镜又恢复透明状态。

综上所述，光电对抗的基本方式，大致如下所示：



由于光电对抗具有一般电子对抗所不及的独特优点，在近几年来发生的局部战争和武装冲突中大出了风头，它在实战中所表现出的惊人效果，引起了世界各国军队的高度重视。纷纷不惜血本，投入了巨大的人力、财力和物力，使越来越多的光电对抗设备走出实验室步入战场。

用不了许久，一种融侦察、干扰和摧毁于一体，工作频段覆盖整个光域并将与雷达对抗“联姻”的光电对抗“杀手锏”将独树一帜，登上战争舞台。

六，电子战族绽新蕾

伴随着现代技术，特别是高技术的迅速发展，电子对抗设备不仅花样翻新，数量激增，其对抗功能与作战效能，更是今非昔比。无论是在电子侦察与反侦察、干扰与反干扰、摧毁与反摧毁领域中，都绽放出了不少新蕾，显现出一派后继有人欣欣向荣的景象。下面介绍的，仅仅是电子战家族新秀中的几个“代表人物”。

(一)“空中司令”——预警机

预警机不是一架普普通通的飞机。它是一种集警戒、指挥和控制于一体的高度自动化的“空中指挥所”，是现代战争(包括电子战争)中十分重要的武器装备。或者说预警机相当于将雷达站、通信系统和 C^3I 系统搬到了空中。享有“空中司令”之称。

从电子战角度看，预警机之所以能成为出类拔萃的新秀，是由于它具有超群的本领。

一是作战功能多。它既能对常规武器和敌方动态进行战略预警，又可在紧急情况下执行战区雷达警戒任务，或者用于战术侦察。它能及时提供敌方攻击的警报，以防止战略袭击，对己方战略部队的生存至关重要，对夺取战场主动权有着举足轻重的作用。

二是雷达侦视范围大。预警机带着搜索雷达升到空中，居高临下，视野宽阔，避开了地球曲面的影响和地形地物的遮挡。预警机可以对高空、低空、地面和海上的活动目标进行有效的实时监视。据测计，当预警机在 6000～9000 术高空飞行时，雷达发现中，高空目标的距离 400—600 公里；发现低空目标为 250～400 公里。它的监视覆盖面积可达 60 余万平方公里。对来袭目标，能提供 30 分钟以上的预警时间，相当于普通地面警戒雷达可提供预警时间的 5 倍。雷达在无严重的背景杂波影响下，可清晰地分辨出航行中潜艇的潜望镜和排气管。

三是通信手段全。预警指挥设备由雷达、通信、数据处理、数据显示、敌我识别和导航等 6 个分系统组成。其中，通信分系统包括高频、甚高频、超高频，能实施对空、对地和应急情况下的话音/数据通信。借助于机上安装的大容量、高速度的电子计算系统，可同时处理近 1000 个跟踪目标的数据，预警机还可作为通信中继站，实施远距离的空中转信。

四是抗干扰性能好。预警机上的雷达采用了频率捷变、多频工作以及低旁瓣天线等抗干扰措施，还装有红外、激光对抗装置和自卫干扰机、箔条投放器等设施，有效地提高了电子对抗的能力。

五是作战效能高。预警机凭借高功能的雷达、通信和多种侦察手段，能对瞬息万变的战况作出及时反应，加上它“看得远”，一旦发现受敌进攻，就能以非常快的速度，迅速指挥己方防空截击机升空迎敌，指挥地面炮火攻击。因而大大提高了作战效能。据统计，有了顶警机以后，可以使防空系统的效能提高约 30 倍。换一句话说，使用预警机后，在保持相同防空能力条件下，可以减少配置近 70%的防空截击机。无怪乎国外有人称预警机是“奇异的财富”。

六是生存能力强。预警机由于搜索、监视的距离远，通常只需在本上上空活动，或在敌方地空、空空战术导弹难以攻击的安全区内飞行。具有很强的抗毁性能。

预警机由于具有以上种种独特的效能，一经问世，就备受世界各国军队青睐，并已在近期发生的局部战争中崭露头角，显现神通。在美国、利比亚之间发生的武装冲突中，电子对抗占据了显要地位，美国的预普机也大出了风头。

为了炫耀美军实力，美海军第六舰队在白宫授意下，进行了一次名为演习实为“钓鱼”的军事行动。美军派出 3 艘航空母舰在飞机群掩护下，冲进

锡德拉湾，向利比亚施加军事压力引其上钩；与此同时，美派出预警飞机和各种电子战飞机，对利比亚沿海一带的雷达、通信等电子系统进行了周密不问断的侦察，截收、测定和分析出了许许多多高价值的电磁参数，为下一步作战作好了“ 电子准备 ”。

利比亚因下识其计，终于上钩。他们从锡德拉导弹基地向美国侦察机发射了导弹，这一举措很快被美国的预警机捕捉，美预警机将有关信息迅速传给了电子干扰机，干扰机随即对利比亚的制导雷达系统实施大功率、限制性的电磁干扰，使利比亚的制寻雷达荧光屏上“ 雪花飞舞 ”白茫茫一片，根本无法辨清真假目标。在预警机的指挥下，美国又对利比亚发射出的导弹，实施假目标欺骗干扰，使其偏离飞行路线，最后坠人海底。

在海湾战争中，预警机也得到广泛应用。“ 沙漠风暴 ”开战的第一天，美军就动用了五六架预警机。发起空袭前，美军利用各种专用的电子对抗飞机，在空中顶警机的指挥下，不间断地对伊军实施了远距离电子干扰，使伊军的通信和雷达预警系统失灵，为攻击飞机打开了通道。海湾战场上“ 爱国者 ”导弹与“ 飞毛腿 ”导弹对弈激烈，在“ 爱国者 ”拦击“ 飞毛腿 ”的空战中，美国预警飞机也立下了汗马功劳。据报道，每当“ 飞毛腿 ”导弹离汗发射架升空时，马上就被在高空巡逻的多国部队预警机发现。预警机将探测到的信息通过卫星通信信道迅速传至远隔万里位于澳大利亚的大型计算机数据处理中心。经高速电子计算机运算、处理后，通过国防数据通信网传送到“ 爱国者 ”导弹发射基地，指引导弹发射、跟踪并摧毁来袭导弹。在“ 沙漠风暴 ”的 42 天行动中，多国部队共出动各种类型的飞机 11 万架次，平均日出动量为 2700 架次，最多一天曾达 3100 架次，完成了侦察、干扰，摧毁伊拉克电子系统、空战、对地攻击以及纵深轰炸等一系列作战任务，形成了全方位、多层次的空中“ 电子网 ”和“ 火力网 ”。其电子打击和空袭强度之大，密度之高实属史上少有。所有这些行动，在很大程度上是有赖于空中预警机。“ 如果没有预警机这个‘ 蜂王 ’，非打乱仗不可。 ”不难看到，在未来战争中，如果能首先摧毁敌方预警机，或者对其实施反干扰，将对敌方构成致命威胁。

图 6-1 所示的是世界各国使用预警机中的一种。

图 6-1　预警机

(二)侦察“明星”——相控阵雷达

“雷达”是个外来语。它是英文 Radio Detection And Ranging 的缩写 Rader 的译音。原意为“无线电探恻和定位”。意思是用无线电波发现并测定目标的空间位置。故别名又叫“无线电定位”。

从雷达一词的含义中，我们不难了解雷达的出世与电子侦察密切相关，它的侦察原理，通俗地说，是利甲被侦察的目标对电磁波的反射(二次辐射)来完成的(图 6-2)。

图 6-2　雷达靠电磁波反射雪现目标

雷达有各种各样的体制，最简单的是脉冲式雷达。它通常由发射机、接收机、天线、天线收发转换开关、定时器、显示器、电源等部分组成。如图 6-3 所示。

图 6-3　肪冲式雷达的组成

发射机用于产生高频振荡信号；接收机用于放大、变换处理回波信号，最后送入显示器。雷达天线是一种方向性很强的定向辐射和接收电磁波的天线，有的形似图 6-3 脉冲式雷达的组成口朝天的大铁锅，有的制成阵列式或引向式等(如图 6-4 所示)。

图 6-4　各种普通雷达天线

天线控制器用于控制雷达天线水平旋转和进行俯仰角度的调

天线收发转换开关用于使雷达的发送与接收部分共用一副天线，做到发射时不接收，接收时不发射。

定时器是触发脉冲产生器，它产生一系列的等时间间隔的触发脉冲，使雷达各部分能按照共同的时间节拍协调一致的工作，相当于能进行自动调控的“电子钟”。

显示器用于显示目标的参数，例如，离雷达的距离、方位、高度等。它通常包括距离显示、平面显示或高度显示等。通过雷达发出的“主波”和从目标反射回来的“回波”间的时间隔距可以测计出目标的有关参数(图 6-5)。

图 6-5　雷达的工作波形

雷达对地面或海面上的目标实施定位时，只需要测出距离和方位角两个数据就可以了。如果要确定空中目标的位置，则需要侧出斜距离、方位角和高度三个数据(图 6-6)。

图 6-7 示出了用雷达探测飞机位置的情况。假设，已知侦察雷达的无线仰角θ为 45°，从雷达天线至目标之间，电磁波往返所需时问 T=2×10^{-4} 秒(该时间可以从显示器上的射标测计出)。因为电磁波在空间的传播速度为每秒钟 30 万公里，通过解三角函数方程式，我们不难求得雷达站至目标的斜距(D)

和目标距地面的高度(=H＋雷达中心点离地面的高度)。

伴随着科学技术的发展，在原有脉冲式雷达的基础上，涌现出了许许多多新型的雷达。在众多的雷达新秀中，最惹人关注的是号称“雷达尖兵”的“相控阵雷达”。

图 6-6　目标方位的极坐标表示

“相控阵”三字是“相位可以控制的干线阵”的简你。普通雷达干线采用的是机械扫描。即由马达等动力驱动，不时地对空间进行有规律地探测，好像人体摆头观察周围事物那样。相控阵雷达扫描方式别具一格，它是用相位移动代替机械扫描。图 6-8 显示出了双面相控阵雷达中的天线阵。

图 6-7　用雷达探测 目标举例

相位阵雷达的天线也可制成圆顶形，像一顶帽子那样扣在雷达上(如图 6-9 所示)。它可以看到周围 360°范围内的目标。

相控阵雷达，集雷达技术之大成，具有许许多多普通雷达所不能比拟的优点。概括他说，是“多”、“快”、“远”、等三个方面。

多——由于相控阵雷达采用了多个发射单元，可以在一定空域内实现多点取样。能同时对抗多个目标，同时完成对不同目标的远警、引导、跟踪或侧高等任务。可谓是雷达门庭的“多面手”。

图 6-8　双面相控阵雷达

快——相控阵天线的突出优点是波束控制灵活，能瞬时地改变波束指向，或用极短的时间扫过需要的空间。扫描过程无惰性，反应时间短，数据卒高。能适应密集的目标环境。据统计，相控阵雷达用相位移动代替机械扫描，可以变化 30 多种扫描波束，其转换周期不到 100 毫秒。

图 6-9　圆顶相控阵雷达

远——相控阵雷达能以很高的分辨力不间断地探测位于很远距离上的目标。据测计，就是对像篮球那样大小的目标，它最大探测距离可达 3700 多公里，对大型卫星可有近 47000 公里的作用距离，“相控阵雷达”的远视功能，堪称“现代高明”。有了像“相控阵雷达”那样侦察明星，相当于给一个国家的领空和领海，配备了一名机警的哨兵。

(三)抗扰能手——跳频通信

众所周知，传统的无线电台通信都是采用“固频”工作的，由于它设备简单，仍广泛使用在现今战场上。

所谓“固频”(也叫“定频”)，指的是无线电台在发信时，信号载波频率是固定不变的。在现代战争中，固频无线电台很容易遭受以下三种电子攻击，受到严重挑战。

一是容易被窃听，二是容易遭测向(只要载波频率是固定的，不管是否采用了信息保护措施，仍会被敌方测向)；二是容易受干扰，严重时使通信中断。

然而，有矛就有盾。对付窃听的有效方法，是采用通信保密设备进行保密通信。对付测向的有效手段是采用猝发通信。对付干扰的有效措施是采用扩频技术，用的较多的是“跳频通信”。

“跳频”是指载迭信息的频率(载频)按照一个编码序列的指令，离散地在一组预先指定的频点上跳变。通俗地说，跳频通信是一种通信频率不是固定在某一数值上，而是按照一定规律和速率来回跳变的通信方式。跳频司以是机械跳频，也可以是电子跳频。机械跳频连续变化的速度慢，目前都使用后者。

根据单位时间内频率跳变的次数，跳变速率分慢速跳频、中速跳频和快速跳频三种。对跳频速率的大小目前尚没有统一的明确规定。一般认为慢速跳频(慢跳)为每秒钟 10～50 次，快速跳频(快跳)为每秒钟 500 次以上，介于慢速跳频与快速跳频之间的为中速跳频(中跳)。据计，现在世界上大多数跳频电台的跳变速率为“中跳”。

无论是固频通信还是跳频通信，都是利用电磁波传递信息。由于无线电波是沿空间传播，通信时，除了自己的联络对象能收到外，敌方也能窃获。敌方还可使用无线电测向、定位设备，侦察我无线电台的位置，对我通信施加电子干扰，或用火力将我电台摧毁。在电子战环境中，通信必须在有干扰的条件下保证畅通，在这一方面，跳频电台可谓是一名能手。

前面已经提到，无线电波干扰通信通常分瞄准式干扰(点干扰)、带宽阻塞式干扰(面干扰)和跟随式干扰三种。对跳频电台来说，前两种干扰都不是主要威胁。这是因为瞄准式干扰机工作在一定的频率上，即使它能干扰跳频电台的其中一个或几个频率，影响也不是很大。采用宽带阻塞式干扰机干扰跳频电台，要消耗巨大的电功率，而且往往要影响己方的通信。例如，某跳频电台在 500 个频率上跳变，发信功率是 100 瓦，那么，干扰机要想对其实现地毯式干扰，功卒必须高达 5 万瓦，这显然是不易实现的。

跟随式干扰固然可以干扰跳频电台工作，但是及时、准确地捕捉跳频电台的频率并相应地将干扰频率调谐到跳频电台的频率上不是一件容易的事，犹如大海捞针那样困难。往往干扰技术的实现难度要比实现跳频技术大得多。由于跳频电台的通信频率变幻莫测，是用瞬时信道传输，不易遭敌窃获，即使被敌窃获也仅仅是瞬时信息，不致影响全局。因而具有根强的保密性。

跳频电台通信的基本原理说起来并不复杂，与普通的单边带电台和调谐电台基本相同。它是在普通无线电短波电台的基础上增加一些控制频罕跳变和解跳的设备。在发信端主要是增加一个“码控跳频器”，它是跳频通信的“心脏”，旨在由伪随机码(即近似随机出现、有一定规律并可复制的码)控制跳变，使发信机发射出的载波成为一个随机跳变的频率序列。图 6-10 是跳

频通信发送部分原理示意图。

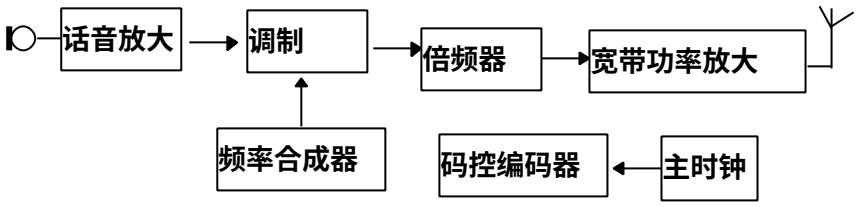


图 6-10　跳频通信发送部分示意

跳频通信的接收系统与发送系统是一个相反的过程，为使接收端很好地跟随发送端工作，使“解跳”以后能准确地接收发方送来的信息，接收端用的编码序列必须与发送端完全相同，只有这样；当通信发射机连续地发射出不同工作频率的信号时，接收机可同步地接收这些相应的频率的信号。第三者如果不知道电台设置的具体频卒和频率跳变的规律，就无法跟踪、捕捉，窃听或干扰其信号。图 6-11 是跳频通信接收部分的原理示意。

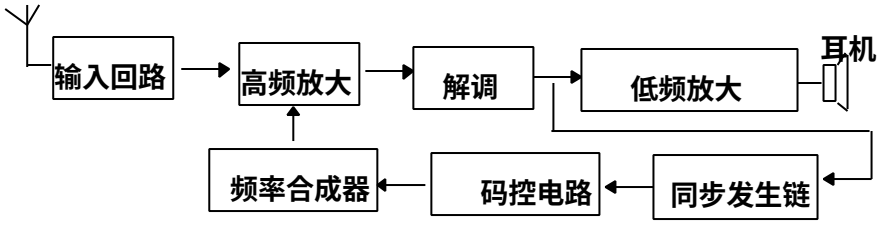


图 6-11　跳频通信接收部分示意

跳频通信的工作方式一般以话音为主，也可传输数据。跳频通信是数字式的，如果是模拟通信，信号发送前需要进行“模——数”变换，将模拟信号变成数字信号；到了接收端再经“数模”变换，将数字信号还原成原信息。

跳频电台主要用于战术无线电通信,是本世界 80 年代以来出现的一种新颖的通信方式，它广泛应用于现代战争中。为了提高战地电子对抗能力，存举世瞩目的“沙漠风暴”期间，法同率先从本国紧急空运了一大批跳频电台以供急需，确保了通信联络的顺畅。随后，美军也紧急采购了几千部跳频电台，广泛装备到美军的军、师部队，直至执行战斗任务的连、排、班，以及坦克、战车、直升机、榴弹炮等战斗小单位。以美国为首的多国部队不仅利用跳频电台进行战场指挥、维系己方通信外，还用它作为电子干扰机去干扰伊军通信。

美军当查明伊军无线电台的工作频率和信号特征以后，就利用跳频电台发出相同频率的、能量极强的信号，对伊军电台实施压制性的干扰，从而使伊军无线电通信一筹莫展，几乎处于瘫痪状态。

英制“美洲虎”是世界上最早研制成功的跳频电台。1981 年刚刚投入使用时，它还只是一种单一的窄频带电台，现已发展成宽、窄频带俱有。由于它融尖端的现代电子技术、电子计算机技术和数字处理技术于一体，具有很强的杭干扰能力和反窃听的本领，在海湾战场上曾一展风采，多国部队各军兵种之间的通信联络大都采用了这种电台。“美洲虎”不仅具有根强的电子

对抗能力，处理数据的速度也非常快，经过海湾战争检验后身价倍增，成了供不应求的抢手货，享有“战地通信骄子”之美称。目前，”美洲虎”已在世界上近 40 个国家和地区落户。

侮湾战争以后，美、法、英等国军队都加强了对跳频电台的研制，相继问世了一批高抗扰性、高保密度，适合战术条件下使用，可背负、车载、机载和手持的跳倾电台。英国目前正在推出一种性能优异、采用数字传输，被称之为是当今世界上第一种全军用袖珍式 VNF-FM 跳频无线电台。这种新型电台体积很小(只有 247×75×38 毫米)、重量轻(含电池共重 1 公斤)，输出功率为 1 瓦，采用 150～200 次/秒的中速跳频速率，用 25 位的八进编码注入编程器，能提供 10^{22} 组排列。具有很高的保密度和抗干扰能力。

目前，各式各样的跳频电台，正如潮水般的涌向战术通信行列。军事专家们预测，跳频电台将是未来战术电台中最具有吸引

图 6-12　国外生产的高频跳频电台

图 6-13 国外生产的甚高频跳频电台

力的军用电台，可望成为电子战场上最有希望的佼佼者。

图 6-12,6-13 所示的是国外目前生产使用的高频和甚高频跳频电台的外形。

(四)毁“脑”幽灵——电脑病毒

“计算机病毒”也叫“电脑病毒”是一种新型的电子战武器，是当今攻击以电子计算机为核心的指挥、控制和通信系统的最可怕敌人。

计算机病毒是一种人为制造的隐藏在电子计算机软件和磁介质中的特别程序或某种密码，被喻为21世纪计算机犯罪的五大手段之一(排序为第二)。它好比隐居在电子计算机系统中的幽灵，很难被发现。它具有很强的传染力，能反复自我增殖、蔓延，以人们始料不及的速度，像病原体一样，从一台计算机迅速扩散，传染到另一台计算机。在计算机网络中，只要有一台计算机遭到病毒感染，就会像瘟疫那样危及其他各机工作，可谓是“一机中毒，全网遭殃”。

计算机病毒具有很大的破坏力。染上病毒的电子计算机，轻者降低运算速度，像“老牛拉破车”一样，影响工作效率；重则破坏系统的工作和程序，抹除掉所贮存的全部数据并使计算机“死机”。1988年末，美国爆发了震撼世界的事件：“计算机病毒”侵入计算机网络，并使该网络的600多台电脑全部“罢工”；成了一堆“高级废铁”。参与联网的美宇航局、海陆空三军重要军事基地中的电脑全部停止运行。其直接经济损失达上亿美元。各国计算机专家、国家安全部门及军界等为此大惊失色。他们由此想到战争，惊叹道，“硅片能够打败钢铁”，“用电脑病毒进行战争比用核子武器更为有效。”有的美国军界人物认为，“要摧毁美国，中断其神经中枢，不需挥戈动武，只需干扰其电脑系统一秒钟即可。”

计算机病毒作为电子战的一种新式兵器，具有多渠道的传播方式。常用的“放毒”途径有四条：一是利用无线电磁波恃播，即将电子计算机病毒调制到电子通信设备发射的电磁波中去，从而将计算机病毒注入到敌方无线电波接收设备中，并在其内随波逐流任意扩散开去；二是利用电子通信系统的配套设备(如天馈系统、电源系统、传感系统以及驱动系统等)传播，使之成为直接与主设备中的电子计算机相连接的病毒传播媒介：三是通过各种有线电通信信道传播，使所有通过有线电线路联网的电于计算机都染毒患病；四是，仿用“派遣特务，长期潜伏，伺机启用”的手法，采取微电脑芯片的“病毒固化”技术，制造“固化病毒”。并将其悄悄地置于所出口的电子通信、雷达以及传感装置等系统中，长期潜伏在其计算机程序内。一旦需要，可通过自控或遥控方式，将其激活。“固化病毒”一旦活化后，犹如“孙行者钻进铁扇公主的肚子里”一样，将电子系统中的电脑程序搞得天翻地覆，给作战指挥带来不堪设想的灾难性后果。1991年春，海湾战争爆发前夕，伊拉克从国外购买了一批用于其国土防空系统的电脑打字机，准备从某国首都中转运到巴格达。五角大楼通过侦察系统迅速获取了这个情报，当即指使有关人员采取偷梁换柱的方法，将一套带有病毒的芯片换装到该电脑打字机中。几天后，当以美国为首的多国部队开始对伊拉克实施大规模空袭时，芯片中的病毒自行发作，使伊拉克的防空指挥系统一片混乱。这是世界上首次进行的“自控式计算机战”尝试。随着科学技术的发展，“遥控式计算机战”也正悄悄走向战场。

计算机病毒武器的问世，大大拓宽了电子对抗的内容栅方式，并使其发生了新的变化。传统的电子对抗主要是用一般的电磁信号去干扰敌方的通信、雷达和其他电子设备，使亡们不能正常工作。用计算机病毒袭击电子系

统，所造成的危害要比一般电子干扰大得多。它会出现电报误传、电话误接、电路误联、网络误控、信息“瞎传一气”，甚至使“中毒”的各种兵器无法自动操纵，导弹失去目标或提前爆炸，……如果说，一般的电于干扰会使敌方的指挥、控制系统成为聋子、瞎子、瘫子、哑巴，那么，计算机病毒的出现，还会使它变成呆子和疯子。

此外.普通电子战手段只能对敌方的电子系统造成短期影响和破坏,而计算机病毒武器则不同，它对敌方电子系统和计算机系统的破坏和影响是长期性的和潜伏性的。

七、电子对弈智则胜

电子对抗自用于战争之日起，就不单是一种纯技术的较量，而是像幽灵那样，充满着诡诈和欺骗，是一场谋略运用之争。外军认为，要成功地进行电子抗争，“不仅需要科学技术上的优势和智慧，而巨需要战术方面的智慧”。海湾战争期间，以美国为首的多国部队在电子战方面的运用，可使我们看到现代战争中，电子战法的一些特点。

(一)谋事在先 成事于后

海湾战争中，以美国为氢的多国部队采用了多手段、多波段、多层次的综合电子对抗系统，这套系统的建立并非一日之功。

通信建设是电子战场建设的基础。美国为了在战争中实施强有力的电子打击，早就着手了在该地区的电子通信系统建设。“ 沙漠盾牌 ”行动之前，这套系统业已基本建成。

为了加速电子信息的传递，在海湾地区美国建起了众多的通信节点，可把在该地区的所有指挥、控制系统接入美国国防通信系统，并能为中央总部和国家指挥当局以及全球的话音数据通信提供接口。

为了确保对参战部队的指挥与控制，美国在海湾地区设立了固定指挥中心、移动指挥中心、机载指挥中心、车载指挥中心和许多指挥所，借助于先进的通信网络，可直接沟通国家指挥中心与前线陆、海、空三军间的通信。

这次海湾战争首次出现了导弹战。导弹战的问世，把交战双方的距离空间拉大，由过去的“ 短兵相接 ”拉到了“ 千里之遥 ”，因而要求通信必须具有远程保障能力。短波无线电台通信，建立迅速，便于机动，传输距离远，成了海湾美军作战指挥的重要通信手段。

1990 年 8 月，伊拉克入侵科威特后几小时，美空军部队就将高频快速反应通信车运往沙特，建起了短波通信信道，用以处理电话和电报、数据等业务。该短波通信系统拥有近 30 万条电路，有多种工作方式，能与多种军标设备接口、互通，有利于美国各军兵种间以及和各国部队之间的协同通信。后经实战检验，短波通信系统在电子斗争中，以及协调上下、友邻间的关系和申请火力支援、空中支援等方面，都发挥了重要作用。

伊拉克入侵科威特之后，美针对海湾地区的突发事态，为配合“ 沙漠盾牌 ”行动，迅速制定并实施了代号为“ 恒源 ”的计划。其核心内容是：全面调用军用卫星系统，为实施电子侦察、为作战部队的各级指挥人员提供作战指挥以及后勤保障所需要的情报信息和通信联络。按此计划，美对外层空间部分卫星的位置和运行轨道进行了调整，使固定在海湾或运行中经过海湾上空的卫星达 15 颗以上。

美军在海湾地区建立的卫星通信主要有三大系统，国防卫星通信系统、舰队卫星通信系统和地面机动部队卫星通信系统。此外，还有“ 导航星 ”全球定位系统，以解决在海湾沙漠地区因参照物少难以进行定位的困难。在海湾战争打响后,美国计划对伊拉克的 1000 个左右的牟事和战略目标实施电子打击和火力摧毁，由于地面机场有限，且距伊拉克境内较远，飞机完全靠从陆上起飞远远不能满足作战需要。为此，美国调集了近 10 艘航空母舰，数百架舰载机，以增大攻击能力。为使海上舰载机与陆上飞机联合出击，协同作战，美国还专门部署了好几颗舰队通信卫星。由于美国位于大西洋上空和印度洋上空的军事通信卫星之间没有星际线路，海湾战争爆发前，美国将在该地区建立卫星通信中继站作为重点。与此同时，美军在第三代国防通信卫星上专门搭载了一个属于空战指挥的转发器，解决了空军卫星通信系统没有自己星体的困难。

周密、完善的通信战场建设，为作战指挥、电子对抗创造了良好条件。海湾战争爆发后，以施瓦茨科普夫将军为首的中央总部前线指挥部一到沙特首都利雅得，便在其司令部驻地，用一个只有 0.5 米左右口径的伞形天线的

卫星通信终端，迅速开通了与远离战区一万多公里的美国本土中央总部之间的通信联络。据统计，海湾战争期间，由美国国防通信局负责处理的从沙特到美国的通信业务中，有 90%是通过卫星通信系统传送的。在这些信息中自然包括用于指挥电子对抗和实施电子对抗的信息。

在加速海湾地区电子通信战场建设的同时，以美国为首的多国部队大力加强了在该地区的电子作战部队和兵器的部署。其中，包括配置电子作战飞机、空中预警机、通信干扰飞机、战术情报侦察飞机、反雷达飞机等空中电子战力量；在地面与海上配置预警雷达、海上侦察船；在空间施放高空侦察卫星、照相侦察卫星、通信侦察卫星。建立起了与整个海湾地区作战的相应的电子作战体系。借助于各种电子侦察手段，在海湾战争爆发前的半年时间里，美国即开始将伊拉克全部高频、甚高频、超高频、特高频信号截获与分析，处理了数百万条信息，掌握了大量的军事电子情报。

为了提高电子作战的自我防卫能力，美国还完善了自卫电子战系统，美国派往海湾的所有作战飞机上，均装有先进的自卫电子战设备。在美国的精心策划下，从东西南北四个方向、海陆空

图 7-1　电子战飞机（指挥机）

图 7-3 电子战飞机(战术干扰飞机)

图 7-3　电子战飞机（战术干扰飞机）

天四维空间，形成了对伊拉克的电子合围。为实现美国以电子战为先导，对伊拉克实施“闪电突击，协调进攻，纵深打击，速战速胜”的战术，提供了强有力的电子支援。

“决胜之策，在于运筹；高敌之着，以计为先。”这一兵家格言已被海湾电子战所检验。

图 7-4　电子战飞机（电子干扰飞机）

图 7-5　电子战飞机（高空高速战略侦察机）

(二)兵马未动 侦察先行

现代局部战争总是由电子战拉开帷幕，而“电子侦察”是其前奏曲。海湾战争期间，美国将其“空地一体战”理论用于电子侦察，采用了“四维一体，立体部署”的侦察战术，取得了明显收效。

早在“沙漠盾牌”行动期间，以美国为茵的多国部队动用了各种电子手段，对伊拉克进行了多方位的电子技术侦察。据报道，多国部队除利用空袭兵器自身携带的电子侦察设备外，还专门出动了 60 余架电子战飞机、高空侦察讥等进行“航空侦察”；利用 20 余颗电子侦察卫星、照相侦察卫星、雷达成像侦察卫星和预警卫星等进行”航天侦察”，并伴以为数众多的海上、地面电子作战部队和近 50 个地面无线电侦听站，形成了地面、海上、空中、太空多层立体的四维电于作战部署。这些具有高科技特点的侦察工具，具有全大候(不管风、雪、雨、雾)、全灭时(不管白天黑夜)、近实时(几乎与事件同时发生)和高分辨率等侦察能力。有的能辨认出直径仅为 30 厘米至 10 厘米的物体，即使在层云密布的日子里，甚至在伸手不见五指的黑夜、从两万米高空都可拍下通信车的牌号。有的能探测到位于地下几米深的通信设施。有的配装红外线遥感设备，能昼夜不停地侦察到任何散热的物体，就连一个装在通信、雷达设备中的普通电脑所发出的热辐射，也逃不出它们的“眼睛”。美国为了加强海湾战区的侦察力量，以及时获取伊军情报，战前，还对太空中原有的侦察卫星，临时地进行了调用。将原部署在东亚上空的两颗侦察卫星调整到海湾地区上空。将原用于监视前苏联和东欧的多颗侦察卫星转而监视海湾地区。通过它们可将所需的战地图象很快送到指挥员的案头。

以美国为首的多国部队借助于“四维一体”立体部署的侦察手段，对伊军的战略目标、兵力部署、战斗行动，以及通信、雷达设施等电子系统了如指掌，乃至伊军土兵手持步话机联络的情景，全在他们的窥视探知之下。以美国为首的多国部队把从伊拉克领土上侦察收集到的数百万个有关指挥、控制、顶警、通信、雷达等系统的信息输入电子计算机，进行分析、处理，详尽地制定了用电子打击伊拉克通信和雷达系统的“白雪”计划，为向伊大举发动战略空袭和实施电子轰炸打下了基础。美国布什总统以从卫星侦察到的情报，说服沙特允许美国迅速派兵进驻该国。将沙特变成进攻伊拉克的“桥头堡”。

(三)先发制人　攻其要穴

1991 年 1 月 17 日凌晨 2 时，夜幕笼罩下的伊拉克首都巴格达，万籁俱寂，一片宁静。以美国为首的多国部队先发制人，向伊拉克发起了大规模的战略空袭。近百枚“ 战斧 ”式远程巡航导弹和“ 哈姆 ”式反雷达导弹一起射向目标，100 多架多国部队飞机飞临巴格达上空。当时巴格达市灯火通明，40 多分钟以后才实行灯火管制。是什么原因使伊拉克不察秋毫挨了一顿“ 闷棍 ”？“ 电子轰炸 ”不失是美军得胜的一个重要原因。可以这样说，海湾战争是硅对钢的胜利，它的第一次空袭，实际上是“ 电子轰炸 ”。

原来，“ 沙漠风暴 ”开始前 24 小时，以美国为首的多国部队，根据战前侦察，摸清了伊军阵地上的各种电磁辐射信号、辐射源的位置和辐射源的特性与用途，对伊军地面通信、雷达等电子设备的技术参数一清二楚，因而很有针对性的采取了“ 点面结合 ”的方法，对伊军的“ 要穴 ”——指挥通信系统，实施了大规模的“ 电子轰炸 ”。一方面针对伊方无线电通信和雷达的某一工作频率发射大功率高能量的嗓音信号，进行“ 点干扰 ”。由于干扰信号的频率与伊方电子设备的工作频率相同，迫使伊军电台、雷达形同虚设，无法工作。另一方面，向伊方阵地发射多频段的干扰信号，同时干扰伊方几个不同频率的无线电台和雷达，即进行“ 面干扰 ”。多国部队的“ 电子轰炸 ”严重破坏了伊方的作战指挥系统。在美军的强烈电子干扰下，伊拉克对美军战前的频繁军事调动和无线电通信往来一无所知，雷达操作员根本看不见美机的出动和飞越巴格达上空。伊方由于防空电子预警系统受到严重手伤，在美军空袭发生后，无法找到来袭目标，也无法指挥防空武器还击，飞机不敢升空作战，防空火炮只有盲目射击，数于枚防空导弹基本未发挥作用。据美军中央总部披露，在向伊第一次空袭时，伊不但“ 没有飞机升空迎战 ”，甚至“ 很少听到防空炮火 ”。多国部队首次战略空袭，一举获得成功。

伊军由于指挥通信系统濒于瘫痪，在群龙无首的情况下，虽有众多的兵力兵器，也未能免于失败。直到 1991 年 3 月 2 日，海湾早已停火三天，而进入科威特地区的伊拉克士兵由于失去通信联络，还不知道已经停战。

(四)隐真示假　软硬兼施

动用高科技武器展开战略空袭是海湾战争的主要作战样式。在海湾地区，以美同为首的多国家调集 30 多种飞机，出动飞机约 3000 架左右。其中，最引人注目的要算 F-117A 隐形战斗机(图 7-6)。

1991 年 1 月 17 日，就是这种飞机担负了战略空袭的首攻任务，投下了海湾战场上的第一颗重磅炸弹。战争打响后，F-l17A 隐形战斗机袭击了伊拉克的纵深目标，重创了伊核生化生产能力和以共和国卫队为主体的战略反击能力，大大挫伤了伊军士气。这仲当今世界上可称得上最先进的战斗机，不仅具有很强的突防能力和杀伤威力，在电子作战中还有一套防身的绝招，即很善于隐形(隐身)，被喻为电子角逐场上的“ 秘密战士 ”。它外形结构特殊，身上涂有可吸收雷达波的材料，很不容易被伊军地面防空雷达发现。飞机上取消了发射大功率的微波雷达，改用前视红外雷达和全球导航接收机，也增加其隐形能力。由于它具有良好的隐形性能，加上利用夜暗(1 月 17 日正是无月之夜)作掩护，使得伊拉克部队无法‘ 看到 ’它的来临就惨遭大灾。F-117A 隐形战斗机命中率很高，在首袭伊拉克时，投下的激光制导炸弹，几乎百分之百地落到伊总统府的屋顶上，作战效果十分明显。它对巴格达电信大楼的攻击，也达到了直接命中的最佳效果。

图 7-6 隐形战斗机

以美国为首的多国部队除了瞒过伊方防空雷达的“ 眼睛 ”进行“ 隐真 ”外，还采用了各种“ 示假 ”的方法，以迷惑伊方视线。它们利用专用电子战飞机在伊拉克上空抛撒雪花般的、能对无线电波起反射作用的金属干扰物，使伊方雷达发出的电磁波照到金属于扰物上，就被反射回去，形成假的回波信号。于是，在雷达荧光屏上出现了许许多多密密麻麻的、无规则分布的亮点，似有成千上百架飞机临空。由于雷达迷盲，无法正确指示目标，机群如入无人之境，伊高炮邵队只能漫无边际的“ 乱放炮 ”，命中率很低。在两伊战争中曾显赫一时的“ 飞毛腿 ”导弹，不是被多国部队击落，就是被干扰得偏离攻击方问，落入荒郊。

以美国为首的多国部队在对伊军雷达、通信设施进行大规模的电子“ 软杀伤 ”，使其处于又瞎又聋又哑又瘫的被动状态的同时，还动用了各种高速反辐射导弹和高速反雷达导弹对伊军的通信、雷达实施强烈的“ 硬摧毁 ”。只要伊军无线电台和雷达一工作，就会立即被反辐射导弹和反雷达导弹捕捉、跟踪以至摧毁。在多国部队软硬毁伤、双管齐下下，伊拉克的通信、雷达设施开机工作可能遭到摧毁，不开机又无法沟通联络和引导各种防空武器拦截，其防空部队陷入了进迟维谷的境地。

伊拉克军队不仅在电子战技术装备上不如美国，在电子战战术上也居下风。伊军由于缺乏电子战战术意识，在与美军电子战斗智斗术中，屡屡上当受骗。如在海湾开战以前，美军为探测伊军的无线电台和防空雷达的阵地配系、技术参数，常常派遣一些无人驾驶飞机深入伊拉克腹地领空进行诱骗性飞行，而伊不知是计，届时就立即开启相关方向的警戒雷达和无线电台，殊不知，正中美军下怀。使美军对伊拉克军队中处于“ 前台当班 ”的雷达和通信设施了如指掌。

美军为进一步摸清伊拉克军队隐蔽的、备用的雷达和无线电台的底细，在对伊发起大规模空袭前 24 小时，发动了一次旨在引“ 蛇 ”出洞的电子佯动。对已探明的伊军电台、雷达进行了压制性的全面干扰。伊军不知美军施的是“ 声东击西 ”的计谋，又急忙开启一些备用的雷达、通信设备，结果将家底和盘托出，又中了美军的圈套。使战场上为数众多的无线电台和雷达成了美军电子打击的“ 活靶子 ”。

军事领域一向就是产生谋略的土壤，用谋施略历来是夺取和把握战场主动权的重要手段。“ 谋高一筹者胜 ”，这一用兵之道，古今中外的战争(包括高技术战争)概莫例外。电子战的产生与发展，给谋略运用提供了新的物质载体，开辟了斗智斗谋的新大地。

八、电子抗争话明日

电子技术高度发展并应用于军事，对现代作战样式和战场环境产生了极大的影响。电子作战已经突破了通信、雷达对抗的范畴，扩展到指挥、控制、制导以及光电、水声等领域，并由一种作战保障手段发展为积极的重要作战手段。电子战设备已从自卫和监视装备发展成进攻性的软、硬结合的杀伤武器。

展望 21 世纪的电子战争，新的电子对抗领域将不断开辟，新的电子对抗手段将不断涌现。21 世纪的电子战场将在地面、海上、空中、水下和空间激烈展开。电子对抗手段将从单一性的发展到多功能的综合系统，电子进攻能力将获得迅速提高，电子防御手段将取得重大进展。环绕着争夺第四维战场的主动权，世界各国将展开全方位的激烈斗争。这种斗争必将刺激电子对抗技术和战术的发展，使电子对抗跃进到一个崭新的阶段。

(一)发展“三杭”通信系统

军事通信系统是遭敌电子打击的重要目标，为了保障作战指挥、维系各军兵种间的协同通信,研制和建立具有抗侦察、抗干扰和抗摧毁(以下简称‘三抗”)的军事通信体系势在必行。随着科学技术的发展，特别是高技术广泛运用于军事领域，中微子通信、蓝绿光通信和流星余迹通信等新型通信手段，将在电子对抗领域中崭露头角，大显神通。

1.中微子通信

中微子通信之所以能成为未来“三抗”通信的新秀和主力，是由于中微子身怀绝技，有着非凡的特点。

“中微了”，顾名思义，是指微小的中性粒子。人所共知，世上万物都由原子组成，原子包括原子核和绕核旋转的电子。原子核内又有质了和中子。“中微子”，通俗他说就是质子或中子发生衰变时的产物。它是一种体积极小的粒子，竟小到比电子的质量还要小近 10 个数量级。

在迄今己发现的 300 多种基本粒子中，中微子是一种奇特而稳定的粒子。这种粒子并不少见，在太阳光、宇宙射线中都有它的踪影。用人工的方法也可获得中微子，1962 年，美国有三位教授(利昂·莱德曼、杰克·斯担伯格和梅尔文·施瓦茨)，曾利用纽约附近新建的粒子加速器人工产生了中微子，首次在基本粒子隐居栖身的微观世界里，掌握了获取中微子的钥匙。

中微子具有敢于与光速较量的神奇本领和不费吹灰之力穿越地球的拿手好戏。它沿直线传播，在传播过程中不发生反射、折射和散射现象，几乎不产生传输衰减。据计算，中微子束即使穿越地球，其能量也仅衰减一百亿分之一。“中微子”这些神奇特性，极大地触发了科学家们对它应用研究的灵感。于是“中微子通信”脱颖而出。

“中微子通信”是一种采用中微子束来代替电磁彼传递信息的无线通信方式。它的通信过程和普通微波通信相仿，有发射和接收两部分装置。在发送端，将欲传递的信息对中微子束进行调制，使载有信息的中微子束，按入的旨意朝一定的方向传向目标。到了接收终端，借助于光探测器，把原来由中微子束所携带的信息解调出来，从而达到通信的目的。

“中微子通信”具有许许多多其他通信无法比拟的优点，突出体现在一个“强”字上。

它能克服普通电磁波不能钻地、入海的“先天性不足”的瘤疾，可穿透地层、进入深海进行直线传输，因此不容易遭受侦察、干扰、截获和摧毁，保密性强，抗干扰能力强。非但敌方用电和磁影响不了它，就是热核爆炸引起的巨大辐射也奈何不了它。“中微子通信”可以冲破电磁波通信不可逾越的地下和水下两大禁区，即使在发生核战争的恶劣的环境条件下，也能够借助于中微子束，向游戈在大洋深处的核动力潜艇发送信息。

“中微子通信”现在已经走出了实验室。

1978 年，美国华盛顿海军研究所，首次在世界上进行了利用中微子作为信息载体的通信试验(试验的距离是 6.4 公里)，并获得了成功。尔后，他们又在华盛顿和伊利诺斯州之间进行了长达 2700 余公里的地下通信试验。1986 年，美国还与前苏联合作，以中微子为“利箭”，逢山开路进行了芽透地球的试验，获得了许多宝贵的数据。可以预料，随着高技术研究的不断深入，

中微子通信的实际应用已指日可待。

2.蓝绿光通信

第二次世界大战期间，1941 年 3 月 7 日至 17 日，希特勒指使他三个最得意的“ 屠手艇长 ”，驾驶三艘代号为 U-47、U-99 和 U-100 号的潜艇潜海航行。当这三艘潜艇上浮到浅海与海岸沟通无线电联络时，迅即被英国海军用无线电测向技术侦察，并随之遭到火力摧毁。它们破摧毁的消息，大大打击了希特勒的嚣张气焰，挫伤了其“ 海中之狼 ”的锐气。

潜艇被毁的现实使科学家们积极开始寻找能使潜艇安全通信的新招，被誉为潜艇“ 千里眼、顺风耳 ”的“ 蓝绿光通信 ”应运而生。

蓝绿光通信是激光通信的一种，它采用的光波波长为 0.45～0.57 微米，介于蓝光和绿光之间(见图 8-1)，称作“ 蓝绿光 ”。

图 8-1　蓝绿光波长

长期以来，水下(尤其是茫茫深海)一直是被视为无线电通信的“ 禁区 ”。这是因为普通无线电波要被海水吸收，能量很快会损耗掉。除非是用甚低频(频率为 3～30 千赫)和较低频(频卒为数十赫至数百赫)，但它们穿透海水的能力，充其量只有 30 来米。何况当频率愈低，要求大线的尺寸愈大(约需 200 来公里长)·通信速率极低(据统计，发送一组三个字母的信号约需 15 分钟)，因此，实际上很难实现。核潜艇同地面进行通信联络，只好上浮到接近海面时进行，但这又要冒遭敌侦察、干扰和摧毁之险。如果用蓝绿光进行通信，这些问题都可迎刃而解。

科学家们在试验中发现，蓝绿波段的激光具有极强的穿透力，能穿透海水直至海洋深处。海水对它的吸收损耗很小，甚至可以说是“ 透明 ”的。尤其当蓝绿光的波长选用适当时，在 2 公里多深的海域里，透光程度可达 95%，似光线可顺利透过玻璃商户那样，这种现象称作海水的“ 蓝绿窗口 ”，加上激光束能量集中，方向性极强，相干性好，让它充当深海通信的传输媒介是最理想不过的了。

图 8-2　蓝绿光通信示意

用蓝绿光传输信息，与一般大气激光通信的原理相似。以打电话为例，在发话端，先将声能变成电能，通过光调制器将话音调制到蓝绿光激光束上，然后经一种特制的光学发射无线发射出去。到了接收端，通过光解调器，将光信号变回电信号，再把电信号还原成话音。

为了摸索蓝绿光的穿透威力，和用蓝绿光进行通信的可能性，本世纪 80 年代初，美国通用电话电子公司在加利福尼亚的圣迭戈附近海域，进行了一次“ 空——海 ”一体化的蓝绿光通信试验，并取得了成功。通信系统的一端设于在 4 万多英尺高空飞行的飞机上，另一端设于在近似“ 实战 ”深度中巡航的潜水艇上。波长为 0.532 微米的激光束，输出功率峰值为 1 瓦的光脉冲从飞机上发出，穿过厚厚的大气层和海水，作用到潜艇上，顺利地完成了人类历史上首次用蓝绿光传输数据的实践。蓝绿光通信试验成功，为实现深海

通信打开了方便的大门，今后，导弹核潜艇可游戈海底、就可与地面、高空进行通信联络。不怕敌方侦察、干扰和摧毁，在电子对抗领域中，前景十分诱人。

3.流星余迹通信

发展瞬间通信(又称碎发通信)，尽量缩短无线电波在空间的暴露时间，这是提高无线电通信抗侦察、抗干扰和抗摧毁能力的重要手段，在这方面，“流星余迹通信”大有可为。

通俗他说，流星余迹通信就是利用流星“尾巴”通信。据天文观测，天体中每天大约有近100亿个流星划破长空坠落于大气层中。由于它们与大气层的相对速度很大(可高达每秒钟12～72公里)，当闯入大气层时，与空气产生剧烈摩擦，绝大部分燃烧而发出耀眼的光芒并瞬间消失。当流星掠过空气时，流星体中飞出的原子与空气中的分子、原子相碰撞，分离成带正电和负电的微粒，于是在流星飞驰的轨迹上留下了一条长长的电离气体柱。大约经过250毫秒以后，电离气体柱中的带电微粒逐渐扩散，成为一条柱状电离云，形似流星的“尾巴”，称作“流星余迹”(图8-3)。

流星余迹宽达15～40英里，距离地面约80～120公里，存留的时间大约为十分之几秒至几分钟。

科学研究表明，凡是具有波动性的物质都可反射无线电信号，用来传递信息。流星余迹也是一种波动物质，当将无线电波对准流星余迹发射时，会产生两类反射：“前向”反射(向前的反射)

图8-3　流星余迹形成示意

图8-4　流星余迹通信示意

和“后向”反射(返回的反射)。后向反射用于对流星的雷达观测，前向反射则用于流星余迹通信。流星余迹好比是一颗“天然的通信卫星”，为地面用户实现通信构筑起了一座高空彩桥。图8-4为流星余迹通信的示意。和往常的无线电波通信比较，流星余迹通信具有许多突出的优点。主要是保密性好，抗干扰能力强。这是由于流星余迹稍纵即逝，而且对无线电波反射具有明显的方向性，不容易遭敌侦察、窃获，也不容易受到干扰。

虽然，宇宙空间每小时有几亿颗流星坠入地球像雨一样的掠过大气，但何时出现，毕竟是随机的，不能做到“星随人愿”。因此，要想实现流星余迹通信，在通信系统中必须设置一名“侦察兵”，随时探测流星的出现，并优选一条合适的佩星余迹。当捕捉到合适的流星余迹时，就以最快的速度打开发射机的“发射闸门”，此时发射机将事先存贮好的信息，一古脑儿地以最快的速度朝流星余迹发射出去。与此同时，平时始终处于“待收”状态的接收机自动将断续收到的信息，先送到信息存贮器保存起来，然后再把它变成连续的信息打印出来。流星余迹一消失，通信系统恢复到等待状态，准备进行下一轮的信息传递。由于流星通信是随机的，也增加了通信的保密性能和抗干扰能力。

此外，沉星余迹通信的传输距离远，通信稳定性好。试验表明，利用普通的八木天线，当发射机输出功率为千把瓦时，通信距离可达2000余公里。

流星余迹通信因为是用高空流星余迹反射无线电波，通信距离远，也不像普通无线电波用天波通信那样，容易因时辰、气候变化受到高空电离层的骚扰而影响通信质量。

流星余迹通信虽早在本世纪中叶，加拿大、美国等国家就先后进行了试验,并于 1965 年由北约组织在法国与荷兰之间建立了用于军事目的的流星余迹通信系统。但由于通信设备比较庞杂，技术要求高，当人造地球卫星问世，出现卫星通信时，它曾一度受到冷落，停滞不前。

“ 山重水复疑无路，柳暗花明又一村 ”。流星余迹通信的魅力。和通信卫星易受反卫星武器击毁的现实(军事专家们分析，在未来战争中，卫星会成为敌方第一次打击的目标)，一直在激发着科学家们努力探索积极研究。可以预言，随着高新科技的发展，流星余迹通信必将焕发出青春活力，成为通信领域中电子对抗的能手。

(二)发展新一代间谍侦察飞机

间谍侦察卫星在太空，无论是沿同步轨道还尾非同步轨道遨游，其运行轨迹总会是有规可循，因此容易遭受敌方太空武器的袭击。此外，间谍侦察卫星上天以后，一旦出了故障，检修起来非常不便。为此，世界有些发达国家的军队除继续研制与发放侦察卫星外，还大力研制间谍侦察飞机。据英国《简氏防务周刊》报道，新一代秘密间谍侦察飞机已在美国空军服役。

这种名为“ 瞩光女神 ”号的飞机，其飞行时速可以达到 8440 公里，可以在 3 小时以内飞到全世界的任何角落。侦察手段比拍摄高分辨率照片的卫星更胜一筹，是“ 搜集全球各种情报 ”的能手。美国空军还正在研制一种取名为“ 极光 ”的新一代秘密侦察飞机，以取代己于 90 年代初退役的“ 黑鸟式 ”间谍飞机。这种飞机的航速是音速的 8 倍，绕地球一周大约只需 5 小时，它所拍摄的照片比来自侦察卫星的高分辨率图象更有价值。这种飞机呈三角形，机头呈 75 度倾斜，可在空中加油。

图 8-5 所示的是俄罗斯武装部队，最近装备的新型侦察系统中起主干作用的“ 蜜蜂-1 ”型无人驾驶机。这种新型的侦察飞机可用于昼夜侦察，并能通过电视传播侦察情报。

图 8-5　新型的无人侦察飞机

(三)发展高强度全频谱干扰源

现代战场上的各种武器制导系统和指挥、控制、通信、情报“四位一体”的 C3I，莫不是一套庞大复杂的电子及电磁波系统。要打赢一场不见刀光剑影的电子战，“软硬毁伤、综合制敌”不失为是一条取胜之道。从某种意义上说，旨在造成敌方通信瘫痪、指挥中断、探测武器失控的电子“软杀伤”更为有效。这是因为随着科学技术的发展，当今战场上各种高强度的防护设施大量涌现，其抗毁性日益增强。因此，利用“硬打击”并不能完全达到瘫痪、摧毁敌方各种作战系统的目的。海湾战争期间，以美国为首的多国部队对伊拉克进行了 40 余天的“地毯式”轰炸，但并没有完全摧毁其战略 C3I 系统。海湾战争中，伊拉克的 4000 多门高射炮、700 余部防空导弹发射装置、140 多枚“霍克”式防空导弹和 700 余架作战飞机之所以没有充分发挥作用，也并非全部受到多国部队的火力杀伤。究其原因，是由于伊军的预警系统、导弹雷达系统、通信系统和指挥控制系统，被多国部队的电子战系统压制和干扰得无法工作。“就连巴格达市的无线广播都听不清楚”。因此，要夺取高技术条件下的战场主动权，必须在一定时空内夺取和控制电磁权。为此，必须大力发展高强度、全频谱的电磁攻击力量。

高强度。指增强干扰功率，发展强功丰干扰设备。据报载，目前美国海军装备的 ALQ-99F 电子干扰系统，是当今世界上功率最强大的干扰源。可成功地实施大功卒杂波干扰和跟踪遮断欺骗性干扰。

全频谱。指拓宽干扰源的干扰频带。形成“一机多用，干扰一片”。目前，国外正在研制、开发的全频谱电子干扰系统，频谱能覆盖毫米波、红外光，适于在陆地、舰载、机载使用，能对雷达、无线电导航、红外光制寻、无线电通信和激光制导等实施干扰。

有了高强度、全频谱干扰源，就能形成一只陆、海、空、大一体化的干扰网，这对限制敌方指挥、通信等系统发挥效能将起重要作用。

(四)发展定向能武器

“定向能武器”是定向束能武器的简称，通常是指利用激光束、粒子束或微波束的能量，产生高热、电离、辐射等综合效应，来摧毁目标(包括电子设备)的新奇武器。它与传统的武器——炸弹、炮弹、导弹乃至原子弹等截然不同，具有异乎寻常的特性与“能耐”。

定向能武器具有“聚能”功能。能将能量聚集成细束(密集束流)，这种束流具有极强的能量，当击中目标时，可在瞬息之间将目标内部的电子器件击穿，以致使目标表面迅速气化。

定向能武器具有惊人的射速。它利用大功率加速器，将电子、质子或离子等微观粒子加速到接近光波的速度，射击 3 公里处的目标，仅需十万分之一秒。加上它是利用电磁能代替爆炸能，目标几乎在“子弹”出“枪口”的同时，就会无声无息地比为缕缕青烟。由于定向能武器射速极快，不易遭受敌方电子干扰，瞄哪打哪，非常准确。

由于定向能武器具有“强、快、准”三大优点，一经问世，就获得军事大国的青睐。目前，它虽尚处于“襁褓”之中，但有着巨大的军事潜力和诱人的发展前景。军事专家们预测，定向能武器有望在 21 世纪初投入实战使用，成为未来电子战场上义一把“利箭”。

(五)发展反隐身技术

事物的发展，总是有矛必有盾。军事科技更是如此。随着隐身技术的出现和发展，反隐身侦察技术便应运而生。

隐身术是研究如何降低兵器被雷达、红外、可见光等探测，反隐身侦察技术是针对隐身技术的一种对抗。它旨在使隐身措施失效或效能降低。

反隐身侦察技术通常从以下两个方面着手。一是从空间域上考虑。例如，设法使雷达从多个方向去捕捉目标。采用相拄阵雷达可实现此要求。二是从频卒域上去考虑，即避开隐身频段，如可采用工作在高频波段的长波雷达。因为不管飞机外形如伺设计，都会在一定条件下产生某些谐振而引起较强的反射。

随着科学技术的发展，反隐身侦察的法术愈来愈高，利用“天基雷达”将是一种尝试。就是在太空中设置一部向地面发射电磁波的雷达，当电磁彼照射到地面时，在地物上产生的反射回波，就会使在雷达荧光屏上出现片状光点。此时，如有一架隐形飞机闯入电磁波覆盖范围之内，由于它要吸收电磁波(不反射电磁波)，那么，雷达荧光屏上就会出现一个独特的、活动着的“黑点”，使隐身飞机“露馅”。而且其隐身法术越高，“黑点”越黑，越会自我暴露。

(六)发展智能化电子对抗

高技术广泛用于军事，使战争进程空前加快。面对战机稍纵即逝、战情瞬息万变的战争舞台，要求电子对抗必须很快建立并持久维系。其中，尤其要对电子侦察系统注入“智能”，迅速提高其自动化水平。只有侦察快而准，才能迅速实施对敌方通信、雷达设施的电子打击。

广泛使用由电子计算机控制的电子侦察系统，是发展自动化电子对抗的必然趋势。利用这套系统(图 8-6)，能自动快速地测定电磁辐射源的位置和分析其信号特性。

在电子计算机的控制下，该系统能自动快速完成下列功能：对

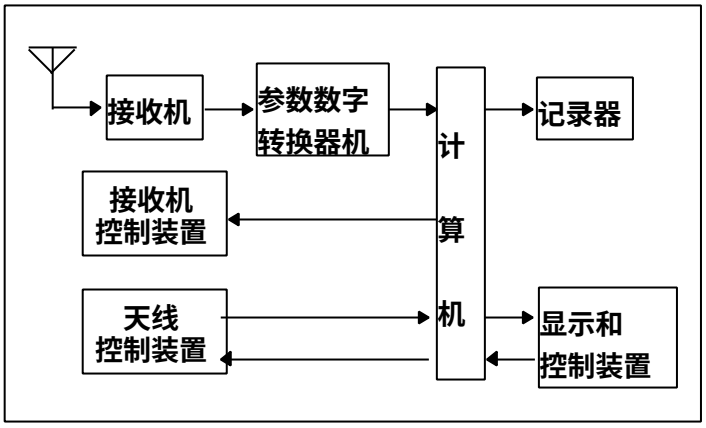


图 8-6　计算机控制的侦察 系统原理方框图

接收机进行自动调谐；截获信号；测量信号参数；进行信号处理；记录侦察结果；采取相应对抗措施等。图 8-7 示也了电子计算机控制的自动化侦察系统的基本组成。

图 8-7　电子计算机控制的自动侦察系统

(七)发展自动化指挥系统对抗

本世纪 50 年代以后，随着电子技术，航天技术、导弹技术的发展，和几次局部战争的刺激，电子对抗的范围已从原来的无线电通信对抗和雷达对抗，迅速扩大到对整个自动化指挥系统(C3I 系统)的对抗。

C^3I 系统是美国于本世纪 60 年代末、70 年代初，为提高电子战条件下的指挥效率，率先建立的。C^3I 系统的建立，不仅使分散的电子对抗和部队行动在以 C^3I 系统为中心的指挥、控制下，发挥出更大的效能，而且出现了以 C^3I 系统为中心的指挥自动化对抗。一个国家要想有效地发挥电子作战和武器系统的威力，不仅要拥有先进的 C^3I 系统，而且还要有强有力的 C^3I 系统的“保护神”。在海湾战争中，伊拉克的 C^3I 系统，因无防卫能力，在“沙漠风暴”初期，遭美空袭破坏后，一直处于瘫痪状态，在这种状况下，只能以失败而告终。

为了把握未来战争的主动权，现在出现了各式各样的自动化指挥系统对抗方式，伴之以出现了许许多多新词汇：C^4I 系统、C^5I 系统、C^3CM 等，C^4I 系统又叫”反 C^3I 系统”，是专门用来破坏、欺骗、引诱和干扰对方的 C^3I 系统的；C^5I 系统又叫“抗反 C^3I 系统”，是专门截获对方 C^4I 系统的电磁信号并给以削弱、破坏，使其无法正常工作，并保护己方的 C^3I 系统免遭干扰和破坏。

C^3CM(叫 C^3 对抗)的产生是基于对敌方的 C^3I 系统的削弱与摧毁。美国国防部给 C^3CM 下过这样的定义：“在情报工作的支援下，综合运用保密、欺骗、干扰及实体摧毁等手段，来防止敌方获取信息，影响、降低或摧毁敌方的 C^3 能力，并保护己方的 C^3 系统免遭敌方的干扰和破坏。”这说明，C^3CM 必须起既“能软杀伤”又“能硬摧毁”的作用，是一种有效的综合战法，成为一把锋利的双刃钢刀。从中也使我们看到，C^3CM 与一般所说的电子对抗的含义不同。一般意义上的电子对抗是指电子侦察、电子干扰和电子摧毁的总称，而 C^3CM 除了上述三种形态外，还包括其他手段的侦察，以及对于 C^3I 系统的实体摧毁。换言之，”自动化指挥系统对抗”的范围要比一般电子对抗宽得多。或者说，在自动化指挥系统对抗中含有电子对抗要享。

在海湾战争中，美军按照该国国防部关于对 C^3CM“一个支援，四种手段”的要求(图 8-8)，充分发挥了 C^3CM 系统的作用。

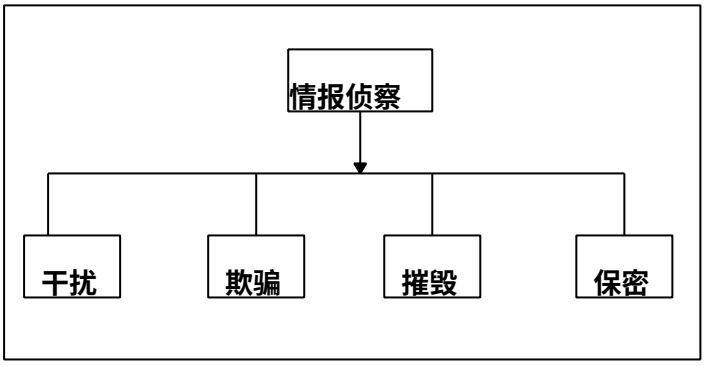


图 8-8　C3CM 组成

美军动用了各种侦察工具(包括侦察卫星、侦察飞机、地面及海上侦察站

等)，实现各种侦察功能(包括照相、监视、监听、光学成像、红外成像、雷达成像等)，获取了各种情报资料(包括通信情报、图象情报、电子情报、电磁辐射情报等)，把电子打击的矛头，直接指向伊军 C3I 的神经中枢——通信。

C3I 系统十分重要，但又十分脆弱。特别是通信网的配置，因地幅大，易遭破坏，往往成为系统的“瓶颈”。美军在战术运用上采取远距离支援干扰，近距离干扰，随队干扰、自卫干扰等方式。很快使伊军通信中断。与此同时，美军采用了种种电磁欺骗方法俺盖其战略意图。军事保密是战胜对方的重要措施，美军非常重视作战意图保密、通信保密和 C^3CM 保密，这比在海湾地面战斗阶段，伊拉克用广播指挥部队撤军，导致被多国部队围追堵截险遭全歼的状况不知要强多少倍。

为了从根本上摧毁伊军的战争实力，以美国为首的多国部队，运用“哈姆”导弹等精确制导反辐射兵器，摧毁伊军 C^3I 系统的“视、听”系统；运用隐形飞机摧毁伊军深远、纵深及腹地的 C^3I 系统，一举摧毁了伊 10 大防空中心的通信枢纽，很快使伊最高统帅部与各集团军司令部间的通信联络陷于瘫痪，从根本上切断了伊军 C^3I 系统的“神经”，导致伊军 C^3I 系统全面受损，成了现代“植物人”。

C^3I 系统与 C3CM 是一对彼此促进发展的矛盾。现在，世界上各发达国家军队，一方面大力加强 C^3I 系统建设，拟在 21 世纪给散兵坑里的单个士兵，配装超小型电子计算机、头前显示器和高效能无线电台(你“电子士兵”)，建立起从总统到前线士兵、从战略指挥级到散兵坑的“天衣无缝”的 C^3I 网络，实现在全球范围内实时地传输话音、数据、视频和图象信息。另一方面，大力发展 C^3CM。

在未来战争中，为了一次性的全面干扰、摧毁敌方的战略、战役和战术 C^3I 系统，现在，有的发达国家，正加紧研制和发展“远程隐形导弹”。这种号称“战场魔弹”的新型导弹，兼具隐形、高速、超远程和智能化的特点，可直接攻击敌方的 C^3I 系统。据称，这种导弹的隐形效果比目前隐形战斗机还好。攻击目标的效果也强于用隐形飞机搭载的精确制导武器。当它一旦问世后，处于敌战役、战术纵深的 C^3I 系统，乃至配置在敌深远、纵深和腹地的战略 C^3I 系统，均将受到毁灭性的打击。专家们预测，不用多久，具有全自动信号处理、分析和识别能力的智能化指挥自动化对抗系统，可望广泛步入战争舞台，成为现代战场上电磁角逐的主角。

有道是“道高一尺，魔高一丈”。正像普通电子对抗一样，C^3I 和 C^3CM，C^3CM 和“反 C^3CM”这一对对矛盾，必将在相互对抗中不断发展，并对未来战争产生着深远的影响。

(八)发展自卫电子战系统

纵观人类战争的历史，战争的规模、样式和结局与武器装备的质量有着极密切的关系。如果说，以往的战争还属于低科学技术水平状态下进行的‘低技术战”，那么，20 世纪 80 年代之后，随着科学技术的突飞猛进，高技术已用于战争，开始出现了“高技术战争”，或者更确切他说，是体现了高技术战争的一些特点。反映高技术战争特征的标志之一，是精确制导兵器的问世。

80 年代以来发生的几场局部战争表明，精确制导兵器在战争中使用的比重越来越大，功能越来越强。马岛战争期间英阿双方使用的精确制导兵器只有数十种，而海湾战争期间已多达数百种；80 年代初，精确制导兵器只用来打击一些公开目标(如飞机、坦克、军舰)，后来发展到能对“藏于九地之下”的隐蔽目标实施打击；一开始，精确制导的对象是带“弹”字号的武器，像导弹、炸弹、炮弹等，现在地雷也实现了精确制导；制导的精度更是昔不如今，过去误差可达数十米，而现在的偏差度仅为十分之一米以内。军事专家们认为“未来的武器库将是制导兵器的天下”。

然而，尺有所短，”打人者必遭人打”。精确制导兵器之所以能实现“既导又准”，全有赖于电子系统的功劳。当它去攻击目标时，与它相关联的电子系统就悄悄地被受攻击一方的电子设备“记录在案”，也就是说，它不由自主地为对方提供了有效的攻击数据。中东战争期间，以色列摧毁贝卡谷地的“萨姆”防空导弹阵地；海湾战争中，“爱国者”袭击“飞毛腿”导弹，都有一个共同的重要原因，就是事先掌握了对方雷达、导弹的技术参数。因而可有的放矢，导弹中的。因此，如何提高精确制导兵器的自卫电子战能力，将是未来发展精确制导兵器中，一个极为重要的问题。

为了提高空中和海上电子防护能力，飞机、直升讥以及各种舰艇均应建有自卫电子战系统，并着力提高其电子战水平。几次局部战争的经验，都非常鲜明地表明，作战兵器有没有自卫电子战系统，以及系统的作战威力如何，有着“天壤之别”的防卫炒能。据国外军界的概率统计，轰炸机若没有自卫电子战系统，实战生存能力不列 25%，有了自卫电子战系统，实战生存能力可升至 95%，上升了 70 个百分点。军舰在无自卫电子战系统时，仿真生存率只有 3%左右，有了自卫电子战系统后，仿真生存卒骤升至 95%，上升的百分点高达 92 个。军事专家们普遍认为，饥载和舰载电子战设备是空战、海战兵器突防时的一种“关键性的自卫武器”。

1982 年，英阿马岛战争中，英方价值 2 亿美元的“谢菲尔德”号战舰，由于在电子对抗装备上存有弱点，无强有力的自卫电子战系统，被造价仅数十万美元的阿方一枚“飞鱼”导弹击中，葬身海底。而“鹞”式飞机上由于装有性能先进的电子对抗系统，创造了空战中击落阿方 36 架飞机、自己全无损失的战绩。1986 年，美国在对利比亚的空袭中，使用了 EF—IIIA 和 EA-6B 电子干扰飞机多架，配合攻击机的自卫电子对抗系统，有效地干扰了利比亚的防空雷达，并发射反辐射导弹摧毁利多部“萨姆-5”导弹制导雷达，保证了空战的成功。

海湾战争中，以美国为首的多国部队派往海湾参战的作战飞机和作战舰艇，几乎都装有先进的自卫电子战设备；因而迅速夺取了制空权和制海权，并大大提高了这些兵器的自身生存能力。据称，美国战斗机上一般都装有电

子对抗的报警和防卫设备，当对方飞机或导弹接近它时，便会向飞行员发出警报，并自动采取电子战防卫措施。美军一名飞行员这样形容飞机上这些措施的使用效果。他说，“他们(指伊拉克)向我发射萨姆式导弹，飞机上电子干扰设备一工作，导弹便发懵，掉转方向离开了。如果没有自卫电子战系统，我们飞机也许有一半回不了家”。在 42 大的海湾战争中，美国共出动了飞机约 10 万多架次，仅损失飞机 30 多架，飞机的损失率不到万分之四。

自卫电子战系统是一种综合性的电子对抗系统，其中包括设置假目标、散发金属箔条、投放闪光弹等，进行欺骗和实施各种无源干扰；此外，还有有源干扰。干扰的对象包括导弹、飞机、战车、火炮等兵器。图 8-9 是战略轰炸机自卫式电子对抗的示意图。

在日益扩大的电磁环境中，大力发展作战兵器的自卫电子战系统，将成为未来电子对抗领域中大力发展的重要课题。

图 8-9 自卫式电子对抗示意

放眼未来看世界，电子对抗对国家安危所起的作用将越来越大。军事专家们普遍认为，如果说，18 世纪是陆战，19 世纪是海战，20 世纪是空战，那么，21 世纪将是电子战。

“如果一旦发生第三次世界大战，必将是一场电子战争”。获胜者将属于“最善于控制和运用电磁频谱”，“拥有最新式电子战兵器的军队一方。”