

电子战：看不见的电磁对抗，怎么让对方的雷达和电台"变聋变瞎"

现代战争打响之前，第一枪往往不是枪声，而是一段谁也听不见的电磁波。雷达突然出现一片雪花，电台里全是刺耳的杂音，导弹找不到目标，指挥部和前线的联系突然中断——这些都不是设备坏了，而是遭到了电子战攻击。电子战是战场上看不见的"暗战"，它不动一刀一枪，却能让一支装备精良的军队瞬间"变聋变瞎"。

一、电磁波是信息化军队的"神经"

要理解电子战，先得明白现代军队有多依赖电磁波。

雷达靠发射和接收电磁波来探测目标；电台和卫星通信靠电磁波传递命令；卫星导航靠电磁波告诉飞机、导弹、单兵"你在哪"；精确制导武器的制导、无人机的遥控和数据链，全都跑在电磁波上。一支现代化军队从指挥到侦察、从通信到打击，整条链条都架在电磁频谱这个"神经系统"上。

好处是效率极高，坏处是太依赖：一旦电磁波被切断、被欺骗、被压制，整支军队就会像被掐住神经一样，反应迟钝、判断失误、协同失灵。电子战要打的，正是这条神经。

二、电子战三大件：侦察、干扰、防护

电子战的全部内容，基本可以归成三类。

第一类是电子侦察。也就是"偷听"和"分析"。用侦察接收机截获对方的雷达信号、通信信号，分析出对方用什么设备、什么频率、什么工作方式、部署在什么位置。它不开火、不干扰，只是静静地听——但听过之后，对方的部署意图、武器型号、甚至兵力调动规律，都可能被推算出来。今天很多情报不是靠人冒死潜入得来的，而是坐在屏幕前"听"出来的。

第二类是电子干扰。这是最"主动"的一环，目标是让对方的电子设备失灵或被骗。干扰又分两种思路：

- 压制性干扰：往对方的频段里灌入强大的噪声，让对方的接收机里全是杂音，有用的信号被"埋"掉。效果就是雷达屏幕一片雪花、电台里只剩噪音。它不讲道理，就是"盖过去"。
- 欺骗性干扰：更阴险。不搞大噪声，而是制造假信号——在对方的雷达上"造"出一群不存在的飞机，或者让真实目标的位置发生偏移。对方雷达明明在工作，屏幕上也有图像，但看到的是假的。这比"一片雪花"危险得多，因为它不容易被发现。

干扰的实施方式也分两种：一种是噪声/杂波干扰机，装在飞机、舰艇或地面车辆上，靠近对方就开机压制；另一种是箔条、红外诱饵这类“物理干扰”——飞机被打中前撒出一片金属箔条，在雷达上制造出比真机身还醒目的假目标，把导弹引开。

第三类是电子防护。就是自己别被对方打聋。办法很多：通信采用跳频，频率每秒钟变几十上百次，让对方刚摸清你的频道，你已经跳走了；雷达采用低截获概率设计，让自己的信号尽量弱、尽量短，让对方不容易侦测到；采用抗干扰算法和定向天线，把干扰信号过滤掉；甚至用猝发通信，本来要几秒钟发完的电文压缩到几毫秒发完，让对方来不及干扰。

这三类构成一个循环：侦察获取信息，干扰破坏对方，防护保护自己，然后再侦察效果如何。电子战从来不是一次性动作，而是一个高速运转的博弈。

三、顺着雷达波打过去：反辐射导弹

电子战里还有一种“硬杀伤”手段——反辐射导弹。它的原理很直接：被动接收对方的雷达辐射波，顺着这个信号直接飞过去，把雷达连人带车一起摧毁。

这解决了一个问题：光干扰还不够彻底，只要雷达关机，干扰就无从下手；而反辐射导弹让“开雷达”本身变成一件危险的事——你一开机，就可能招来一枚导弹。海湾战争中，多国部队的电子战飞机和反辐射导弹配合，把伊拉克的防空雷达打得不敢开机，整个防空网就此瘫痪。

四、几个改变了战局的例子

电子战的历史比很多人想的更久。

二战期间，盟军和德军都搞过大规模电子欺骗。最经典的是对德军无线电导航系统的干扰：德军轰炸机夜间靠无线电波束导航飞向英国目标，英国人想出一个办法——布置干扰台，把德军的导航波束“扭”向错误方向，让轰炸机飞偏甚至把炸弹扔到无人区。这是早期电子战的代表作，靠几台机器就搅乱了对方的空袭。

赎罪日战争中，电子战的作用更加明显。以色列军队依靠有效的电子对抗和反干扰措施，让阿拉伯国家装备的苏制制导武器和通信系统大受影响；而对手的雷达和通信被压制后，战场态势感知能力明显下降。

海湾战争则把电子战推上了新高度。空袭前数小时，多国部队先对伊拉克的雷达、通信、指挥系统实施大规模电子压制，使对方雷达致盲、通信中断。等真正开始轰炸时，伊拉克的防空部队基本处于“看不见、叫不通、打不着”的状态。这场战争让全世界第一次直观看到：制电磁权，可能和制空权一样决定胜负。

五、它和网络战不是一回事

有人会把电子战和网络战混为一谈，其实两者有重叠也有区别。网络战主要针对数据和信息系统——入侵、植入、破坏软件和网络；电子战针对的是电磁频谱——压制、欺骗、截获在空中传播的电磁信号。电子战甚至可以不接触对方任何计算机，纯粹在物理层上让对方的设备失灵。

现代趋势是两者越来越融合：电子战手段可以为网络攻击创造条件，网络攻击也可以反过来瘫痪对方的电子战体系。所以业界常把"网络空间"和"电磁空间"并列，看作信息化战争的两片新战场。

六、未来：更安静，也更复杂

电子战的技术还在往前走。人工智能被用来自动识别和分类信号，几秒钟内从海量电磁信号里挑出高价值的；认知电子战能根据对方的变化实时调整干扰策略，不再是预设几套方案；宽频谱、一体化、软件定义的电子战系统，让同一套设备既能侦察又能干扰，还能量身定制干扰波形。

但有一点不会变：电子战的核心从来不是"谁的功率大"，而是"谁更懂对方"。你要让对方的雷达失灵，就得先弄清它是什么体制、什么频率、什么工作习惯；你要骗过对方的操作员，就得知道他们会怎么判断。技术决定下限，对对方的理解才决定上限。

冷知识 - 现代战争的第一枪常常是电磁压制，而不是枪声——让对方的雷达、通信、导航先失灵。 - 欺骗性干扰比压制性干扰更危险：对方雷达上明明有目标图像，但那些飞机根本不存在。 - 跳频通信能每秒钟变几十上百次频率，让对方刚摸清频道，你已经跳走了。 - 反辐射导弹顺着雷达波飞过去直接摧毁雷达，让"开机"本身变成危险动作。 - 二战中盟军曾用干扰台把德军夜间轰炸机的导航波束"扭"偏，让它们把炸弹扔到无人区。