



少年国防教育丛书

# 寂静的战场 ——电子战

主 编：方 敏  
副主编：张长东 张 云  
夏欣欣 许涑华 编 著

少年儿童出版社

少年国防教育丛书

# 寂静战场 ——电子战

主 编：方 敏

副主编：张长东 张 云

夏欣欣 许涑华 编 著

少年儿童出版社

## “少年国防教育丛书”编委会名录

编委会主任：巴忠倓(中将)

编委会副主任：糜振玉(中将)

编委：方敏 张长东 张云 朱宗葆  
顾伟强 孙洪锁 李名慈 徐九生

策划：李名慈

主编：方敏

副主编：张长东 张云

## 少年强则国强(代序)

青少年是祖国的未来，民族的希望。

不关心青少年未来的民族是没有希望的民族。

不重视青少年爱国主义国防教育的国家也是没有前途的国家。

在青少年中，唱响主旋律、弘扬爱国主义，崇尚卫国习武精神，这是一个国家、一个民族之希望所在！

梁启超说得好：

少年智则国智，

少年富则国富，

少年强则国强，

少年独立则国独立，

少年自由则国自由，

少年进步则国进步，

少年胜于欧洲，则国胜于欧洲，

少年雄于地球，则国雄于地球。

爱家、爱民族、爱国家、爱国防，忧患意识至关重要。忧患兴邦，忧患足以兴国防，国防强才能保民安邦，国家才能长治久安。

青年朋友对近代中国的历史并不陌生，触目惊心的现实危机，受人宰割的衰败惨状，丧权辱国的血腥纪录，“俄北瞰，英西眈，法南瞬，日东耽，处四强邻之中而为中国，岌岌哉！”“吾中国四万万人民，无贵无贱，当今日覆屋之下，漏舟之中，薪火之上，如笼中之鸟，釜底之鱼，牢中之囚，为奴隶，为牛马，为犬羊，听人驱使，听人宰割。此四千年二十朝未有之奇变”（康有为）。每一个了解中国近代史的中华儿女，每当回忆起这段悲惨历史，每当看到圆明园在秋叶飘摇孤独屹立的断垣残柱之时，无不对这段屈辱史刻骨铭心！

这段时光虽然已经过去，但历史不能忘却，警钟必须长鸣！

今日，人类居住的地球，比之过去天翻地覆。但既有阳光与鲜花，更有血与火，仍然充满着危机和灾难。战争的硝烟没有一天从我们的视线里消失。人们不会忘记，我驻南斯拉夫使馆被炸，台海上空的阴云，霸权主义横行，强权政治肆虐，宗教冲突，领土纠纷，资源掠夺与反掠夺、灾害、疾病、事故……现实反复告诉我们一个真理：和平不等于太平，发展绝

非安宁。和平不是靠幻想，化剑为犁的时代离我们还很远很远。

我们能轻信“天下太平”的故事么？

最可怕的是一个民族在危机中失却了忧患意识。

丧失戒备的民族，势必会受到历史的奚落！

“位卑未敢忘忧国”。

“天行健，君子以自强不息”。

中华民族代代相传，生生不息。正因为有这样一种精神！

关注国家的兴衰，捍卫国家的尊严，维护国家的主权。国家利益高于一切！

今天的青少年，明日国家的主人。世界归根结底是属于青少年一代。作为跨世纪的一代青少年，历史已将你们推上了历史的舞台。

青少年朋友们，努力吧！

方 敏

二 年八月一日

## 导言

这是一个寂静的战场。当你还没有看到弥漫的硝烟，它已迷盲了敌人的“眼睛”；当你还没有听到犀利的爆炸，它已振聋了敌人的“耳朵”；当你还没有感受搏杀的激烈，它已摧毁了敌人的“大脑”。一切似乎还没有开始，但胜负已见分晓。这就是电子战。

电子战的历史并不久远。若从无线电使用于军事行动之日算起，也只不过百年的光景。但是，自从电子战登上人类战争的历史舞台，就以其神奇而又诡秘的“表演”，引起了人们极大的兴趣，成为军事家们关注的焦点。在科学技术的推动下，电子战以不可阻挡之势，迅猛地从地面燎原到海上、空中和外层空间，渗透到每一个角落，并贯穿于现代战争的始终，左右着战局的成败。

本书将追踪电子战无形的足迹，勾画各国在侦察与反侦察、干扰与反干扰、欺骗与反欺骗、摧毁与反摧毁的较量中的一系列重大和典型的历史事件。笔者试图通过对这些历史事件的简要分析，找出电子战的



一般原则和方法，以把握其中的规律，让人们特别是让青少年了解电子战的来龙去脉，认清电子战在高技术战场上举足轻重的作用，关注电子战在未来战场上的强劲走势。美国前参谋长联席会议主席、海军上将托马斯·H·穆勒告诫人们：“不仅应当让军队和关心国防的人及时了解电子战的存在和它的一般用途，而且应让普通公众也有所了解。如果发生第三次世界大战，获胜者将是最善于控制和运用电磁频谱的一方。”

和平与发展是人类永恒的主题，而当今的世界却并不太平。我们的国家面临的来自地面、海洋、空间和高技术领域的威胁一天也不曾消失。伟大的战略家、军事家毛泽东曾指出：“主动地位不是空想的，而是具体的、物质的，这里最重要的，是保存并集结最大而有活力的军队。”这里的“大”，无疑是强大的“大”；这里的“活力”无疑是对军事科技“制高点”的攀登和占据。爱好和平的人们必须牢记“忘战必危”的古训。历史无数次验证了这样的事实——一个怀有危机感、勇于自我批判的民族，才有可能兴盛与发展；而一个兴盛民族的背后，必定有一支强大的

军队。有亿万民众特别是亿万青少年关注、关心、支持的军队，才能是一支充满希望的、强大的军队！

图书在版编目(C I P ) 数据

寂静战场: 电子战/ 夏欣欣, 许涑华编著. - 上海: 少年儿童出版社, 2000. 12

(少年国防教育丛书/ 方敏主编)

ISBN 7-5324-4314-0

. 寂... . 夏... 许... . 电子战- 少年读物  
. E869-49

中国版本图书馆 CIP 数据核字(2000) 第 80656 号

寂静战场  
——电子战

夏欣欣 许涑华 编著

俞跃庭 插图

赵晓音 王 峥 装帧

责任编辑 刘 蔚 美术编辑 赵晓音

少年儿童出版社出版发行 开本 787 × 1092 1/32

上海延安西路 1538 号 印张 6 . 5 插页 2

邮政编码 200052 字数 111, 000

全国新华书店经销 2000 年 12 月第 1 版

商务联西印刷厂排版 2000 年 12 月第 1 次印刷

辽苏扬中印刷厂印刷 印数 1-5, 100

ISBN7-5324-4314-0/N · 522(儿) 定价: 8.00 元

# 目录

导言 .....	8
一、探根求源——走近电子战 .....	15
穿越大西洋的第一束电波 .....	15
电报， 侦察和泄密的双刃剑 .....	19
“炸弹”炸开的“谜”底 .....	25
“电子干扰”建功勋 .....	27
电波“巧设”迷魂阵 .....	30
电台坐唱“空城计” .....	33
穿云破雾，雷达闪亮登场 .....	35
雷达预警，“海狮”受挫 .....	37
“千里眼”失明，德舰逃亡 .....	41
“无源干扰”出“窗”，汉堡被炸 .....	43
改进雷达，希特勒苟延残喘 .....	46
抓住机遇，盟军空军柳暗花明 .....	48
所向披靡，导弹横空出世 .....	51
高空追杀“黑色女侦探” .....	53
“软”“硬”兼施，美空军重整旗鼓 .....	57
假雷达，请君入瓮 .....	60
电子干扰下的“布拉格之春” .....	63

一代天骄， 卫星拓展电子战空间 .....	67
计算机—电子战的“倍增器” .....	70
“人—机”一体的 C <sup>3</sup> I 系统 .....	73
“沙漠风暴”中的无形“杀手” .....	77
电子计算机的“克星” .....	81
神秘的“黑客” .....	83
“第一代网络战士” .....	86
网络催生的“第四领土” .....	89
二、 战场搏杀——回眸电子战 .....	94
电子战“擒获”的第一位舰队司令 .....	94
诺曼底登陆中的电子战 .....	100
古巴导弹危机 .....	105
在战鹰展开翅膀以前 .....	111
跨越“巴列夫”防线 .....	116
南大西洋上的电子战 .....	123
“死亡线”上的较量 .....	128
“黄金峡谷”行动 .....	134
海湾战争中的“白雪”行动 .....	139
电子战中的“非对称作战” .....	145
在“非对称作战”的另一端 .....	150

---

车臣上空，一“足”遮天 .....	155
三、纵横驰骋——分析电子战 .....	161
独特的风景线 .....	161
风雨历程电子战 .....	162
形形色色的电子对抗技术 .....	176
C <sup>3</sup> I：电子对抗的明星 .....	178
电子对抗：战争的重要支柱 .....	181
电磁优势：战争的制高点 .....	185
无所不在的影响 .....	193
鲜明的战争特征 .....	199
攻防兼备的战争手段 .....	205
四、遥看千河——展望电子战 .....	209
电子战理论在突破 .....	209
电子战技术在发展 .....	213
新概念武器在研制 .....	229
计算机的卫士 .....	240
军队建设的双翼 .....	248
联合作战中的电子战 .....	251
信息战中的电子战 .....	253

# 一、探根求源——走近电子战

## 穿越大西洋的第一束电波

提到电子战，不能不介绍一下无线电之父马可尼。1874年，古列尔莫·马可尼出生于意大利一个富裕的家庭。那个年代，科学技术发展的速度是前所未有的。1820年，丹麦哥本哈根大学教授奥斯特，在一次物理教学实验课上意外地发现了电流磁效应。在对电磁的深入研究过程中，出生于美国的发明大王爱迪生于1863年发明了自动发报机；英国人贝尔于1876年实现了人类第一次有线电话传输……这一切，对从小就喜爱读书和做各种电学实验的马可尼产生了重要的影响。他看到有线电报架设线路非常费力，就想：“能不能用电磁波来传送电报呢？”1895年，20岁的马可尼在自己家的花园里成功地进行了无线电波传递实验，妈妈十分高兴，给了他1,000美元，鼓励他继续实验。

由于实验规模的不断扩大，为了寻找实验经费的来源，22岁的马可尼来到了科技水平处于世界领先地位的英国，在英国政府的支持下，继续进行实验。1897年，他和助手在英国西海岸进行了跨海通讯实验。他们把发射机装在海岸上的一个小屋子里，屋外竖起一根根高高的杆子，上面架设了用金属圆筒制成的天线。开始时把接收机放在距海岸4.8千米的一个小岛上，通讯效果良好。然后又把距离扩大到14.5千米，同样获得成功。这是人类第一次不用导线将信号传过了海湾。





20 世纪到来了，马可尼决心去中美洲的英属牙买加和北美洲的加拿大，在那里架设无线电台，以便实现穿越大西洋的无线电通信。有不少人来劝说他。先是父亲担心：大西洋有 3，000 千米宽，再强的电波也会在空气中消衰的。接着老师也提醒他：无线电先驱赫兹说过，要实现跨大西洋的通信，必须在空中高悬一面面积比欧洲大陆还要大的天线才行，哪里去找这么大的天线啊！

马可尼决心已下，他说：“无线电到底能不能飞越大西洋，必须亲自试一下。即使失败了，也要为后人留下一些实验数据。”勇于探索的精神使他义无反顾地到了牙买加，在那里他架起了一座 100 多米高的天线塔。

接着他又来到加拿大的纽芬兰岛，在大西洋旁边的一座高山上放起一只大风筝。这一切安排好后，他让助手在牙买加发射电波，而他则在纽芬兰准备接收电波。他用手捂着紧贴耳朵的话筒，等待着远方的呼唤……

1901 年 12 月 12 日，这是一个不平凡的日子，马可尼终于等到了“滴-滴-滴”三声。这正是莫尔斯电码中的“S”字母！这就是人类穿越大西洋的第一束电波，这一天标志着无线电已成为全球性事业。由于他为无线电作为通讯工具方面和无线电技术的发展作出了巨大贡献，1909 年，他获得了诺贝尔物理学奖。1937 年 8 月 30 日，为了悼念无线电之父——马可尼的逝世，英国所有邮局的无线电报和无线电话都沉默两分钟。

先进的技术，总是被嗅觉灵敏度极高的军事家们所觉察。因为在战场上，谁抢占了科技的“制高点”，谁就可以使自己在血与火的搏杀中增大获胜的机率。和众多的科技发明一样，无线电报刚发明两年零两个月，它就被用于战场上的角逐。起初，无线电报主要用于军舰之间或军舰与陆地之间的远距离通信。日本人在他们的所有军舰上都安上了按马可尼发明仿制的无线电装置，但性能很差，只能用一个频率工作，通信距离勉强达到 60 英里。同样，俄国人在他们的远东地区的战舰上和靠近海军基地的大量地面站中也配置了无线电装置。实战的运用，使这一技术得到了进一步的完善和发展。

### 电报，侦察和泄密的双刃剑

知己知彼，百战不殆。在无线电发明以前，为了收集敌方的情报，主要采用由侦察员深入敌后、或用间谍打入敌人内部等方法。这些方法虽然行之有效，但费钱、费时而又危险。电报的使用，除了为通信联络带来了便利之外，也同时打开了侦察敌方情报、

泄露自己秘密的一扇窗口。因为发出的无线电信号己方可以接收，敌方同样也可以接收。通过窃听敌人的无线电通讯，从破译敌方电文中获取有关战略、军队调动和部队作战的情报，做到知己知彼，有针对性地采取措施，这就是最初的电子侦察，是电子战活动的一个重要方面。电报，是一把双刃剑。如何运用，关键在于扬长避短。

第一次世界大战期间，对外交无线电通信的侦听已达到了不可思议的程度。英国谍报机构破译了最秘密的德国密码，他们侦听破译所有德国外交部发给国外大使的电报达 3 年之久。

“俾斯麦”号战列舰，是用 19 世纪德国“铁血宰相”俾斯麦的名字命名的，是当时世界上最先进的一艘特大战列舰。1941 年 5 月 21 日，英国获知“俾斯麦”号将驶入大西洋这一情报，深知这是对英国的极大威胁，决定想方设法，一定要把它击沉。

威力强大的“俾斯麦”战列舰由万吨级巡洋舰“欧根王子”号护航，于 1941 年 5 月 22 日晚离开挪威的卑尔根开往大西洋。在那里和停泊在布列斯

特的战斗巡洋舰“夏恩霍斯特”号及“格鲁塞瑙”号会合，组成一支舰队去袭击英国商船。

5月23日傍晚，“俾斯麦”号和“欧根王子”号进入丹麦海峡。5月24日，英国巡洋舰“胡德”号和“威尔斯王子”发现并率先与德舰交战，与此同时，英国整个本土舰队，战舰、巡洋舰、驱逐舰、航空母舰开始从各个方向朝这里集结。交战中，“胡德”号被德舰的第三次齐射击中，这艘英国皇家海军引为骄傲的巨大巡洋舰背部被炸得粉碎，舰首和舰尾翘向空中，然后消失在波涛之下，只有三名水兵幸存。“威尔斯王子”号也遭重创退了下去。然而，“俾斯麦”号也遭“威尔斯王子”号的炮击，正在漏油。

当英舰队的大队人马赶到时，“俾斯麦”号已不知去向。“俾斯麦”号此时完全可以逃避英国舰队的追杀，糟糕的是，它发给柏林的电报被英国截获，英军得知了它的位置后，就杀奔而去。不料，英军却扑了一个空。原来旗舰把“俾斯麦”位置标错了。这一次又给了“俾斯麦”一个逃生的机会，当时它距英舰320千米，完全可以从容不迫地离去。可就在这时，德国司令部给“俾斯麦”发出的一长串电报，令它

全速驶向布列斯特。这封电报，再次被英国截获。于是，英军在前往布列斯特的航线上布下了围歼“俾斯麦”的天罗地网，使它置于持续的炮击之下，5月27日10时40分，“俾斯麦”号沉没了，舰上近2000名水兵也同归于尽。可以说，是那一份电报成了“俾斯麦”号的“掘墓人”。

山本五十六是组建日本海军的鼻祖，又是日本空军的先驱。他曾一手策划指挥了日军偷袭珍珠港事件，重创了美国的太平洋舰队。这个有名的日本战犯，也是因为一份电报泄露了秘密，使自己毙命空中。

珍珠港事件后，日本决定乘胜对已濒于瘫痪的美国太平洋舰队给予毁灭性的打击。日本首先选中了距离珍珠港1000千米的美海军基地——中途岛作为目标。为此，日军出动战舰达200艘、作战飞机1000架、兵力10余万，由三本五十六大将亲自指挥。战前数星期的1942年5月20日，山本五十六把这一计划用密电发给了他的海军指挥部。

美国自珍珠港事件后，吸取教训，建立起当时世界上独一无二的电子侦察网。山本五十六所发的电文

当即被美国人截获破译。由此，美国太平洋舰队司令、海军上将尼米兹得知：山本五十六已决定在 6 月 3 日攻击“AF”地点。尽管美方推测“AF”就是中途岛，但为了证实这一推测，美军有意让驻中途岛的海军司令部发一份能被日本人破译出来的简易电文，佯称岛上的“淡水设备装置有故障。”果然，日本截获这份“密报”后，报告说：“AF”可能缺少淡水。这份报告又被美军截获并破译，于是肯定了“AF”就是指中途岛。此后，美军又通过截获和破译，查明了日军参战部队的数量、番号、航线和进攻时间，设伏歼灭日本 4 艘航空母舰、一艘巡洋舰、332 架飞机和数千名官兵。



1943年4月，山本五十六决定亲自率幕僚去前线视察，并布署对美军的进攻行动。通讯官用无线电发出了日程安排，包括山本巡视的航线、起飞和到达的时间。密报一发出，便被美国日夜执勤的无线电台所截获、破译。电文以最快的速度摆到了美国总统罗斯福的办公桌上。美国人永远也不会忘记山本五十六制造的珍珠港事件！美国高级领导层做出决定：“不论付出任何代价，务须于4月18日截住日机，使山本及其幕僚葬身海底。”有如此细致可靠的



情报在手，美军经过周密计划，完成了他们的“复仇”行动，终于将山本五十六的座机击落。

### “炸弹”炸开的“谜”底

第一次世界大战爆发后，沙皇俄国没有接受过去与日本在海上交战中惨败的教训，在两个集团军向德国大举进攻时，竟然用明码拍发了有关俄军布署和作战计划的电报，这份电报被抵抗俄国的德军第 8 集团军截获。德军从电报中了解到俄两个集团军之间有宽达 100 千米的空隙，于是集中兵力攻击俄第 2 集团军。俄第 2 集团军司令萨松诺夫向第 1 集团军求援，而第 1 集团军则认为萨松诺夫是怯战而不予理睬。这些来往的明码电报又被德军截获。德军只用一个师来对付俄第 1 集团军可能会有的象征性支援，而以主力猛攻第 2 集团军并一举将其消灭。然后又回过头来对付第 1 集团军，并取得了巨大胜利。这一战役俄军被歼近 30 万，德军只付出了伤亡 1 万人的代价。这就是有名的坦仑堡战役。由此可见，保密对取得战争的胜利具有非常重要的作用。

为了保密，战争中使用了密码电报。这样，对方截获的电报要经过破译密码才能知晓电报的内容。这就增加了电子斗争的新手段，即密码与破译的斗争。

为了保密，德国人发明了“谜”密码机，它能产生 220 亿种不同的组合。在当时，假如一个人昼夜连续工作，每分钟破译一种密码组合法，需要 4,200 年才能将所有的密码译完。因此，“谜”不怕被敌方截获，因为没有时间破译，希特勒完全信赖它。后来英国之所以能破译“谜”，还是验证了中国的那句老话：“解铃还需系铃人”。

“系铃人”是一个化名理查德·勒文斯基的犹太人，他曾在柏林制造“谜”型密码机的工厂当工程师，参与了“谜”的制造和改进。因为他是犹太人，遭到纳粹的歧视而被清除，他以 10 万英磅和他与妻子在英国居住为条件，向英国谍报机关提供了复制的“谜”型机，为英国破译它创造了条件。而“解铃人”则是一位名叫艾仑·图林的人。他当时 34 岁，在数学逻辑方面有很深的造诣，1936 年发表了这方面的研究成果，进行了设计通用计算机的研究。他接受了破译“谜”的任务，在“系铃人”理查德·勒文

斯基的帮助下，终于研制出一台名叫“炸弹”的机器，这台机器只需几分钟或十几分钟就可以“炸”开“谜”底，再也不用等待4000多年了。当1940年8月13日，戈林向德军下达轰炸伦敦命令时，“炸弹”就破译了这个命令，从而为最终粉碎德军的进攻提供了重要的条件。

第二次世界大战中，日本海军使用的很难破译的“紫色密码”，在偷袭珍珠港得手，以后日本海军仍使用它。但美国经过反复研究，终于破译了“紫色密码”。在中途岛海战中，因为美军破译了日军的密码，结果取得了海战的胜利。也正是由于美国成功破译日军的密码，成功地击落了日本海军司令山本五十六的座机，使其机毁人亡，重创了日本军队的士气。

### “电子干扰”建功勋

大家都知道，当今，不同的广播电台都要采用不同的频率，以防止互相干扰，影响收听的效果。而在无线电报刚诞生不久，人们对此并没有一个清楚的认

识。有人只是在有意无意之间，尝试性地做了一些举动，而正是这些潜意识的动作，逐步发展成为电子战的一种重要方式——电子干扰。

1904年3月8日，日军试图袭击停泊在旅顺港内的俄国军舰，这些军舰位于内航道，在开阔的海面上无法看到。如果闯入航道，必定受到众多俄国舰船和岸上炮火的围攻，等于自取灭亡。因此，日军开出两艘装甲巡洋舰“春日”和“日慎”号，以间接射击的方式炮轰航道，由一艘悄悄潜伏在近海岸的小型驱逐舰观察炮弹的落点，及时对射击的方向进行修正。然而，一个俄国基地的无线电报员听到了日舰之间正在交换信息，他本能地按下发射机的信号键，希望能对敌舰通信起到一些干扰的作用。这一举动使日军的无线电通信受到严重干扰，信息无法传递，不得不提前中止炮击并撤退。而这一下意识的动作使得俄舰在当天的战斗中无一损伤。

人们逐渐发现：无线电报不仅可以用来传送自己的信号，而且可以用来干扰敌方的信号。从此，电子干扰就被人们有意识地、大量的使用，并发挥着越来越大的作用。

1914年，英国刚刚对德宣战不久，地中海发生了一起引人注目的事件。德国巡洋舰“格贝德”号和“布雷斯劳”号准备开往当时的中立国意大利。途中被英国巡洋舰“格洛斯特”号紧紧盯梢，“格洛斯特”号的任务是把德舰的所有活动用无线电通知伦敦的海军总部，然后由海军总部下令给地中海舰队，将这两艘德国舰只消灭。这时德舰侦听到“格洛斯特”号和英国海军部之间的无线电通信联系，在这关键时刻，他们果断地发出一种与英国人频率相同的混乱噪声。英国人几次改变他们的频率，但德国人总是咬住不放，噪声挥之不去。德舰趁机改变航线，全速开往与其友好的土耳其达达尼尔水域。在急切而又无效的呼叫声中，“格洛斯特”号只能眼睁睁地看着到了嘴边的美餐又溜之大吉。

好运总是光顾善于运用先进技术的一方。

第二次世界大战苏军反攻加里宁格勒格时，利用杂波干扰了被包围的德集团军的无线电通信，该集团军曾先后250次企图与希特勒大本营取得联系，使用了各种不同的波长，发出了各种不同的呼号，但都无济于事。德军不得不举起了投降的白旗。后来从被

俘虏的德军司令官的供词得知，德军投降的原因之一，就是同希特勒大本营的通信受阻，精神上和兵力上都得不到支援。

### 电波“巧设”迷魂阵

1943年5月，德军情报机关截获并破译了英美联军发给美某空军基地的一份电报：“进攻西西里岛之作战方案已定，命你部务必于5月8日23时前，完成向该地空运地面部队的任务”。

德军如获至宝，为了破坏这次空运行动，他们精心制定了一个用无线电通信手段进行欺骗的作战计划。

5月8日，德军派出轰炸机轮番轰炸停泊在美军基地附近海域上面的英、美军舰。同以前轰炸一样，所有轰炸机始终保持在1,500米的高度上。“德机，高度1,500米，狠狠地打！高度1,500米，狠狠地打！”这样就使英、美军舰产生一种误解：以为1,500米高度的机群都是德国人的。接着，德军便利用美英联军的这种错觉，并且利用当

时无线电通信“只听声音不见面”的缺陷，开始了他们的欺骗活动。

执行任务的时间到了，美空运飞机一架架呼啸着飞上蓝天。刚离开基地不久，德军突然实施了强烈的电子干扰，使其与地面失去联络。当美飞行员在空中像瞎子一样兜圈子、并急切地呼叫：“请指示高度和方位，请指示高度和方位……”突然收到地面的指挥：“请保持1，500米高度！请保持1，500米高度！航向3，500密位！航向，3，500密位！”



这是德国人冒充美军向空中发出的。美军飞行员听到“命令”后欣喜万分，不加思索地按指定的高度和方向、朝德军设置的圈套钻了进去。

刚刚遭到轰炸的英、美军舰上的官兵，一看到飞行高度在 1，5 0 0 米的飞机，怒发冲冠，所有舰上的对空火炮一齐开火，许多美国飞行员还没有弄清是怎么回事，就连人带机坠入大海。这是第二次世界大战中最大的一次盟军误伤事件。



科技和军事的互相作用，演变出了特定历史条件下的电子欺骗。

### 电台坐唱“空城计”

1965年3月的一个清晨，一架美侦察飞机，在越南南方N山谷上空执行侦察任务。突然，丛林中飘出的缕缕清烟吸引了飞行员的目光。为了看个真切，飞行员还在该上空盘旋了几圈。傍晚，正当美军的指挥官们研究侦察情报时，一个情报参谋报告：“在N山谷发现无线电波，从功能上看，极可能是我们上月丢失的电台。”

根据侦察的报告和近日掌握的一系列情况，美军指挥官们断定：“在这里安营的、肯定就是上月袭击我们指挥所的那支越南游击队。”

真是冤家路窄。“立即消灭他们！”美指挥官发出了命令。

20分钟后，美军出动了6架F-105战斗机，对N山谷进行了近30分钟的狂轰滥炸，倾泻了近千枚炸弹。顿时，山谷里树倒石飞，火光冲天。美

军这时判断，游击队此时即便还有几个活下来的，也不会有多少还手的力量了。“乘胜追击，一定要将游击队一网打尽！”

紧接着，美军又出动了两个营的兵力，空降到 N 山谷，对“残余”游击队进行最后的围剿。出乎美军意料的是，他们连一个人影也没见到，只发现了两部自己上次丢失的电台，其中一部已经被炸坏，另一部还在不断地发射着无线电波。上面还压着一张纸条：“对不起，让你们受累了。谢谢合作。”……

原来，越南某游击队队长在早晨看到在山谷上空盘旋的美国飞机后，估计敌人已经发现了自己队伍的行踪，便利用夜色的掩护向山谷外转移。当他看到小通信员身上背着两部沉重的电台时，想起上次战斗一下子从敌人那里缴获四部电台，眉头一皱，计上心来。他笑着对小通信员说：“有‘借’有还，再‘借’不难。我们就还给他们两部。”于是，队长把两部电台分别藏在不同的石缝中，然后让通信员使电台处于发射状态。就这样，两部缴获的电台，把美国佬痛痛快快地捉弄了一通。这是越南人民武装以无线电波欺骗美军的一次成功的战例。

## 穿云破雾，雷达闪亮登场

雷达，是英文缩写词 *r a d a r* 的音译。原意为“无线电探测和定位”。素有“千里眼”之称的雷达，是一种利用电磁波发现目标并测定其位置的电子设备。主要组成部分有天线、发射机、接收系统和终端显示设备等。按工作状态，可分为脉冲雷达和连续波雷达。

脉冲雷达由发射机产生高频脉冲，经天线集成电磁波束，按一定方向间歇地发射。采用转动天线或电子控制波束的方法，使波束在空中扫掠。电磁波碰到物体时，其中一小部分反射回来，被原天线所接收，经接收系统检波、放大，进行信息处理后在显示器上显示出来，或直接输出信息数据。根据电磁波由发射出去到反射回来所经历的时间来测定距离；根据收到反射波与天线所指的方位来测定方向；根据距离和波束所处的仰角来测定高度。

连续波雷达分调制与非调制两类。非调制连续波雷达利用多普勒效应测量目标速度。调制连续波雷达

一般采用调频无线电波，根据发射波和反射波之间的频率差来测定距离和速度。雷达具有探测距离远、测量目标参数速度快、可全天候使用等特点，广泛应用于侦察、警戒、导航、瞄准、制导、地形测绘和气象探测等方面。

雷达的发明走过了坎坷的里程。1888年，德国物理学家海因里希·赫兹证明了电磁波的作用跟光射线相似，它能集中成单个的波，并能被金属不约而同反射回来，形成可以检测到的回波。1904年，一个名叫克里斯蒂安·许尔斯迈尔的德国工程师发明了一种用于航海的“无线电测量设备”。该设备包括并排安装的一台发射机和一台接收机，其工作方式是发射机发射的电波如果被金属物体反射回来就会被接收机接收。他把这个设备称做遥测望远镜。当时在意大利、法国、美国、英国等都有了对雷达的研究。1935年，英国物理学家罗伯特·沃森·瓦特接受当局委托制造“死光”的任务。所谓“死光”就是指发射波长很短但能致人于死地的电磁波。当时，正处于第二次世界大战前夕，如果能用“死光”来消灭远距离的敌人，肯定可以在未来战争中发挥重要作用。瓦

特经过反复试验后，发现制造“死光”的设想不能实现，但他却意外发现用电磁波来探测远距离的飞机是完全可能的。他根据这种设想制成了当时性能先进的雷达，在第二次世界大战中发挥了巨大的作用。雷达使英国最早形成了全国范围的预警系统，从而能够在德国空军的每一次空袭前发出警报，并引导英国空军起飞拦截。

### 雷达预警，“海狮”受挫

两国交战，处于防御的一方，总是想能够提早知道进攻者何时“光顾”，以做好充分的准备。尤其是空战，时间显得更加重要。第一次世界大战中，轰炸机的速度每小时只有130千米左右，那时，防御的一方往往是派几名听觉灵敏的人，用大喇叭口的听音器来掌握敌机的动态。到了第二次世界大战，轰炸机的速度达到了每小时400千米，已接近音速的一半，继续用土办法就不行了。

科技推动了军事的发展，军事发展又呼唤着新科技的支持。

1940年，希特勒曾制定了一个臭名昭著的“海狮计划”——在一个月内摧毁英国空军，进而从海上入侵，吞并英伦三岛。为此，德国空军司令戈林集中了2,669架飞机，对英国实施铺天盖地的轮番轰炸。当时，英国的飞机还不到700架。然而，令德国人惊讶的是，英国空军的歼击机就好像知道德国飞行的时间表一样，总是能抢占有利的攻击位置，拦截并将其击落。只经过两周的战斗，德国空军就损失了600架轰炸机。

后来德国人才发现，并不是什么人泄露了秘密，而是英国的雷达预警网提前向战斗机发出了通报。英国人的“千里眼”，也正是德国人的“眼中刺”。显而易见，要实现“海狮计划”，只有先撕毁英军的雷达网。德国人发怒了！开始了直接攻击雷达网的行动，这就是现代电子战中“硬杀伤”的初始。

德国人对五个沿海雷达站的采取突然行动，是英国人始料不及的，德国轰炸机携带两枚500千克的大型炸弹对天线进行了闪电式袭击，五个站都被击中并受到了严重的破坏。尽管只有一部天线真正倒塌，实际上五个雷达站都不能工作了。

为了迷惑敌方，聪明的英国人很快想到了一个好办法：用一种只能发射不能回收的、根本不能发现目标的普通发射机暂且替代雷达，并开始向外发射。这一举动，使刚刚绽开的笑容又马上从德国人的脸上消失了。因为“事实”证明，袭击天线的作用不大，它只“沉默”了两三个小时，又开始“唱歌”了。德国人只好放弃了对雷达的攻击，使这些雷达站得以保留。英国的雷达预警网在整个不列颠战役中，提供了重要的情报保障。

后来，英国把雷达装到了飞机上，这就出现了机载雷达。雷达“更上一层楼”，也就能提供更多的预警时间。

二战时，在大西洋海面，德国海军头目邓尼茨策划了一个所谓的“狼群战术”。每当潜艇中有一艘发现所要攻击的目标，立即报告岸上基地指挥部，并通知其他潜艇。之后，由一艘有经验的潜艇担任“头狼”，指挥作战，另一艘引诱对方护航舰，其它潜艇乘虚而入，发动水中夜袭。天亮脱离，次日夜里再进入攻击位置。仅半年时间，德军就击沉了英、美等国的舰船 668 艘。英国空军装备了机载雷达后，可

以在很远的地方看到浮出水面的德国潜艇。而德军还没有装备雷达，所以看不到远方的英国的飞机。只要德军的潜艇一露出水面，就被英国空军的眼睛——机载雷达发现，随之而来的就是英军飞机的轰击。德军潜艇毫无办法，最后不得不把剩余的 2 2 0 艘潜艇自沉大海。

此外，在电子战方面，英国还专门启用了世界著名的数理逻辑学家——图灵，研制成功一台被称为“极端者”的密码自动破译机。靠着“极端者”和英国设在全世界各地的侦察网，英国人能准确地知道德国陆、海、空三军司令部给各自部队的指示、命令及相互间的通信，甚至希特勒本人发出的作战命令也被截获、破译。因此，德军每次在什么时间、什么地点，有多少批、多少架飞机，沿哪条航线行动，经常被英军掌握得十分清楚，英军事家能在重要方向上集中兵力，伺机出击。在防空作战中英军取得击落德军飞机 1，7 3 3 架，击毙和俘虏德飞行员 6，0 0 0 多名的辉煌战绩，使德军的“海狮计划”变成“死狮计划”，希特勒的图谋化为泡影。



## “千里眼”失明，德舰逃亡

雷达是侦察和瞄准的有效工具，它能穿透迷雾和黑暗发现目标，但也容易受到干扰和欺骗。雷达接收机必须制造得十分灵敏，才能接收那些微弱的目标回波。一旦对方知道了雷达的接收频率，用较强的波束对准雷达发射，就可以把雷达真正想要的目标回波淹没，让雷达“失明”。

在实施“海狮计划”的过程中，德国人发现：英国的侦察比火炮更厉害。基于这一认识，从1939年8月开始，德国空军通信兵的头目、马梯尼将军就已经亲自对敌人的雷达进行了研究，那时他试图侦收英国上空的磁辐射，但没有成功。1940年法国沦陷后，他又沿着法国北海岸设置若干接收站，侦收英国的雷达发射信号。用这种方法，德国人已经发现很多英国雷达的主要性能，如频率、脉冲宽度等等，并找到了它们的位置。这一成果，为不久后德舰的一次海上突围，起到了重要的作用。

1941年3月22日拂晓，德国战斗巡洋舰“夏恩霍斯特”号和“格鲁塞瑙”号驶入被占领的法国

布列斯特海军基地，长期的战斗使这两艘德舰疲惫不堪，伤痕不少，需要进行修理。两个月后，另一艘德国重型巡洋舰“欧根王子”号也来到港口避难。几天之前，它曾与“俾斯麦”号一同对英作战，“俾斯麦”被击沉，“欧根王子”则逃脱了。

在修理期间，尽管这三艘军舰巧妙伪装，但还是被英国皇家空军发现了，皇家空军立即对这个港口日夜轮番轰炸。这些舰只不止一次地被损坏。

希特勒亲自权衡这个犹如“垂死的癌症病人”情况。不“动手术”（不转移），就意味着死亡；而动手术（转移），虽然冒风险，却有一线生存的机会。于是决定，转移到德国一个比较安全的港口。马梯尼受命负责为“海峡突围”施放雷达干扰。

德国工厂立即设计制造了特殊的干扰机，它们能使英国雷达接收饱和、阴极显像管呈现一片空白。马梯尼在这些舰只离开前两个月，就开始有步骤地施放干扰，并一点点有步骤地增加，让英国错以为是气象原因造成的。

德国军舰 1942 年 2 月 11 日开始撤离。干扰机全部调到对准英国雷达工作的频率上，施放强大

的干扰，迫使一些雷达关机，一些雷达试图改变频率避开干扰，但没有成功。就连一个从未使用过的雷达，也立即被德国的干扰机所“迷瞎”。尽管德国军舰被一架英国飞机在无意中发现，并在海上发生了战斗，但德国军舰还是在 2 月 13 日中午回到了德国。成功地实现了海上突围。

### “无源干扰”出“窗”，汉堡被炸

希特勒的“海狮计划”破灭后，英军开始转守为攻。

1943 年 7 月 24 日深夜，盟军 791 架轰炸机组成的巨大的编队，满载着炸弹和成千上万个特制的盒子，浩浩荡荡，闯入德国的领空。当德国的雷达发现有敌机临近，还没有弄清有多少架的时候，突然，雷达荧光屏上出现了无数白色尖头信号，宛如几千架飞机奔袭而来，所有雷达操纵员惊惶失措。这样大的“机群”使他们无法确定飞机的数量和位置，不得不报告：“雷达不能工作！”德军措手不及，无

法指挥地面火力还击，也无法有效地引导飞机拦截，地面指挥一片混乱。

袭击汉堡所造成的破坏是巨大的。仅仅两个半小时，2,300吨炸弹倾泻在汉堡港口和市中心，猛烈的大火顿时形成了一个火球，因吸收巨量空气，在城市引起可怕的大风，树木被连根拔起，人和物被刮入海中。盟军仅以12架飞机的损失，换取了历史上这次大空袭的胜利。

发生了什么事情使德国雷达不能正常工作呢？原来是英国研制了一种消极干扰器材——金属箔条，并且首次投入实战。英国飞机快要驶入德军火力范围时，他们将250万盒装有箔条的干扰物抛向空中，千百万根箔条在空中散开，由于箔条对无线电波有较强的反射作用，能产生大量的回波，可以使雷达达到饱和状态，无法发挥作用。

此前，英军虽然已经发现了箔条的作用，但担心这一“绝招”落入敌人手中，反过来对付自己，一直犹豫不用。最后，是丘吉尔首相亲自下令，皇家空军飞机在空袭汉堡时终于使用了这种干扰措施。这个命令的代号叫“打开窗子”。此后，箔条就被称为“干

扰窗”。这是战争史上最早出现的“无源干扰”的方法和手段，至今仍被大量使用。

具有讽刺意味的是，德国人掌握用箔条进行干扰这一方法比英国人更早。当希特勒知道这种方法后，他像英国人一样，害怕新的电子对抗措施落到敌人手中和被模仿，再用来对付自己。结果，当对手抢先使用这一办法空袭汉堡时，当地的防空系统感到十分意外。在那可怕的夜里，汉堡数万人被炸死，没有几个人甚至德国防空司令部的高级官员也丝毫没有意识到发生了什么情况。据说当时还下令：“不要碰，它们可能有毒”。

两昼夜之后，盟军第二次袭击汉堡，然后进一步空袭德国其他大城市时，都使用了这种新的电子对抗措施。在头六次空袭中，盟军出动4,000架次飞机，仅损失124架轰炸机，占总数的3%，比以往每次空袭都低得多。几个月后，德国空军通信部队的头目马梯尼将军承认，敌人在战术上获得了空前的成功。

然而，像电子战中经常发生的那样，英国人好景不长。遭到初次打击后，德国很快找到了一种解决

这个新问题的方法。此后，许多有经验的雷达操纵员学会了把轰炸机和“干扰窗”回波加以区别的方法。飞机是以有规律的速度、固定的方向移动的，而箔条在雷达显示器上几乎是不动的。英国人则采用投放巨量的箔条进行反击，使敌方雷达荧光屏完全失效。

有矛就有盾。一种新的作战方法出现后，敌方必然会寻求更新的方法来应对，此消彼长，循环往复，螺旋上升。及时地掌握新技术、运用新技术，并不断地加以改进和创新，才能在激烈无情的战争对抗中，使自己处于有利的地位。

### 改进雷达，希特勒苟延残喘

为了避开盟军的无源干扰(如箔条)和有源干扰(如干扰机)，增进其防空系统的效能，德国大大加快了新雷达的研究，因为每过一个白天和夜晚，就可能意味着另一个德国城市的毁灭。

1944年初，几乎所有的德国夜间战斗机都装上了一个称为“列支敦士登 SN<sub>2</sub>”的新雷达。它覆盖面大、功率大、探测距离远，使德军的防空战术得

到了全面的修改和更新。没过多久，德军飞机上又加装了雷达告警接收机。它有三个胜于雷达的优点：第一，它是完全被动的设备，不发射电磁能量，所以不会暴露自己；第二，它功率大，比雷达具有更大的作用距离；因为是直接接收敌方的信号，可率先发现敌机，迎得主动；第三，由于它是被动接收，不受箔条的干扰。

1944年初，针对英国领航飞机上安装的H<sub>2</sub>S雷达和轰炸机上安装的“墨尼卡”雷达，德国专门设计了能分别接收它们电波的“纳克奥斯”雷达和“弗兰斯堡”雷达，并安装在战斗机上。两种性能先进、针对性很强的新雷达一装上飞机就发挥了巨大的作用。这一年，柏林之所以能免遭全面破坏，很大程度上依赖于德国电子领域的新进展。在此期间，盟军空军的损失大幅度上升，士气相应地下降，许多英国最好的飞行员已经疲劳到了极点，经常因为有最轻微的危险和困难的预兆，盟军轰炸机就把他们的炸弹投在海里或旷野上，一听到战斗机不可抗拒的接近的噪音，轰炸机惊惶失措的炮手就开始向他看到的或想象中的任何东西射击。有时把自己人的飞机误认为是敌机，

将其击落。这种混乱状态，到 1944 年 3 月 30 日至 31 日夜达到了顶点。德国战斗机凭借他们的雷达告警接收机引导，对布鲁塞尔上空的一个英国皇家空军轰炸机编队进行了一场结局悬殊的大空战，一直到把对手打了回去。盟军为了执行这一任务，派出 795 架轰炸机，损失 95 架，另外 71 架遭受严重损伤后回到基地，还有 12 架在着陆时坠毁。最终，盟军共损失 115 架轰炸机和 800 名训练有素的飞行员。德军这一胜利，主要归功于他们在战争的这一阶段中，电子战技术又处于了领先地位。

### 抓住机遇，盟军空军柳暗花明

1944 年 7 月 13 日拂晓，一架最先进的德国夜间战斗机“容克”Ju 88G-1 由于导航错误，在英国的领土上着陆。它装有最新的电子设备 SN<sub>2</sub> 雷达、“弗兰斯堡”雷达警告机和一些最新式的高效无线电设备。这对英国、对盟军可以说是天赐良机。因为德国军队技术上的暂时领先，使盟军的空军处于十分危险的境地。



英国专家立即开始对所有的设备进行检查，当他们了解到“弗兰斯堡”雷达警告机的作用时，感到非常惊愕。英军在飞机上安装的雷达不但不起保护作用，恰恰相反，暴露了自己，吸引了敌机——像苍蝇逐肉一样。为了证实 S N<sub>2</sub> 雷达和“弗兰斯堡”雷达警告机的作用，英方专门组织了一次飞行试验，有 71 架“兰开斯特”轰炸机，其尾部都装有护尾雷达设备，接到“命令”飞向德国，起飞后，英军轰炸机奉命打开了他们的电子设备。



这架“容克”J u<sub>88</sub> G - 1 飞机由英国飞行员驾驶起飞。“弗兰斯堡”雷达警告机约在 50 千米的距离处就接收到了英轰炸机上雷达发出的信号，而且不

用打开自己的雷达。“容克”Ju 88 G - 1 飞机在神不知、鬼不觉的情况下，跟上了轰炸机群，并轻易地占领了最好的攻击位置。这时，英国皇家空军的指挥员们如梦方醒，前段时间空战屡屡受挫的谜团也被解开。他们命令：立即把安装在轰炸机尾部的所有雷达统统卸了下来。同时，按照“列支敦士登 SN 2”雷达的波长准确切割的大量箔条被生产出来。到 1944 年 7 月底，这种新的“干扰窗”投入使用。由于新的“干扰窗”的使用和机尾雷达的拆除，英国夜间袭击德国的飞机损失明显减少。

随后，德国改进了他们的雷达天线，以减少由于“干扰窗”引起的电子扰乱。当英国得知这一情况后，他们开始使用很长的金属条（有的达 400 英尺），系在一个小降落伞上，它能模拟一架大型的飞机回波。德国被迫进一步改进雷达，以抵消英国新的对抗措施的功效……

盟国空军终于走出了低谷，变得越来越自信。这有力地推动战争向有利于盟军的方向发展，加速了希特勒的灭亡。

雷达、电子对抗措施之间斗争一直在持续进行着。谁取得了技术上的优势，谁就能处于有利的地位。

## 所向披靡，导弹横空出世

导弹是依靠自身动力装置推进，由制导系统控制飞行线路，并自动引导弹头飞向目标的武器。它由弹头、弹体、推进系统、制导系统和电源等组成。最初用于战争的导弹是第二次世界大战末期德国的 V - 1 飞航式导弹和 V - 2 弹道式导弹。

与其他武器相比，导弹具有自身明显的特点。一是射程远。世界上目前还没有任何武器在射程方面能与导弹相提并论。洲际导弹的射程都在 8 , 0 0 0 千米以上。一旦射程达到 2 0 , 0 0 0 千米时，就可以攻击地球上的任何目标。二是速度快。从发射到击中上万千米以外的目标只需半个小时左右。在高空和外层空间进行弹道平飞，因为几乎没有阻力，飞行速度可达到音速的 1 3 - 2 0 倍。三是精度高。导弹的命中精度通常用圆概率误差表示，误差越小，命中精度就越高。海湾战争中投入使用的“战斧”式巡航导

弹飞行 1 , 0 0 0 多千米, 圆概率误差只有 1 0 米左右。四是威力大。导弹战斗部可以装高能炸药、核炸药或其它战剂; 还可以采用多弹头, 威力更大。目前, 导弹核武器的威力已经达到几千万吨梯恩梯当量, 比 1 9 4 5 年美军投放在日本广岛的那颗“小男孩”原子弹的威力(2 万吨) 要大几千倍。

导弹的种类很多。根据任务的不同, 可分为战略导弹和战术导弹。战略导弹是指用来袭击对方战略目标, 射程在 1 0 , 0 0 0 千米以上, 通常携带核战斗部的导弹。它的使命是削弱或摧毁对方的军事和经济实力, 使对方在战争中处于被动状态。战术导弹是用于攻击战术目标, 射程在 1 , 0 0 0 千米以内, 携带常规战斗部或小型核战斗部的各种导弹。

反雷达导弹是战术导弹中的一种, 又叫反辐射导弹。它是一种以火控、制导、预警以及其他雷达为主要攻击目标, 利用电磁辐射信号进行被动制导, 从而直接摧毁辐射源的导弹。反雷达导弹的工作原理是: 在导弹上装有雷达信号接收装置, 当载弹平台(飞机或舰艇等) 被雷达跟踪时, 导弹即从平台上发射, 并沿雷达波束飞向目标, 直到命中为止。

在现代战场上，雷达布置的密度越来越大。在电子对抗中要做到既能有效地干扰破坏对方的电子设备，同时又不至于影响己方的电子设备的正常工作，将变得越来越困难。如作战飞机和导弹，仅仅靠一般的电子干扰措施来迷惑对方的“耳目”，实施突防是很不容易的。最好的办法就是采用识别性很强的“硬杀伤”手段——直接摧毁对方关键部位的雷达，以消除“软杀伤”的不彻底性和自己同时会被干扰的副作用。电子“硬杀伤”除使用传统的火力手段外，主要是发展反辐射导弹。

反辐射导弹使电子装备由单一的“软杀伤”发展为“软”“硬”结合的统一体。它极大地提高了电子对抗的能力，为夺取战场的电磁优势，发挥武器装备的效能提供了有效的保证。世界近期的几场局部战争，使用反辐射导弹摧毁对方雷达已成为现代战争的主要手段之一。

### 高空追杀“黑色女侦探”

1960年5月1日，一架绰号为“黑色女侦探”的美国高空侦察机U-2，和从前一样，在前苏联20,000米以上的高空潇洒地进行着侦察活动。在飞行员弗朗西斯·加里·鲍尔的眼中，天依然是那么蓝，丝丝白云宛若轻松的心情，随风飘荡；广袤的土地、玉带般的河流在云缝里时隐时现。突然，一条长了眼睛似的火龙穿云而出，直扑过来，飞行员还没有反应过来是怎么回事，“女侦探”便被无数的弹片击中，鲍尔眼前一黑，坠毁在异国他乡。

这就是“萨姆-2”导弹击落第一架U-2精彩的一幕。它标志着反电子侦察的突破性进展，也预示着防空作战能力的飞跃性提高。

早期的电子对抗是在地面与海面之间进行的。第二次世界大战后，随着飞机和防空武器的发展，电子对抗设备和反雷达设备被带上了天。50年代末至60年代初，美国使用了当时世界上最先进的、用于远距离侦察监视核武器试验和导弹发射的“空中间谍”——高空侦察机U-2。它飞得快，飞得高，当时的高炮打不到它，飞机不但没它快，也飞不到它的高度；它全身涂满了黑色，用光学手段和雷达很难

发现。所以它总是举止傲慢地从你的领空飞过，你也只能“雾里看花”，望机兴叹。它装有8台巨型全自动摄像机和电子侦察设备，对地面景物和电子设施进行侦察，不受白天黑夜、天气好坏的限制。那时，只要哪国一进行核试验，这家伙就会“不请自到”，光顾巡视。各国对它都感觉神秘莫测，称之为“黑色女侦探。”为此，前苏联加紧了导弹的开发研制工作，针对高空侦察机U-2，生产出了新一代导弹“萨姆-2”，并投入了实战运用。

1950年10月，我国成立了中国人民解放军防空军司令部。1957年7月17日，空军和防空军合并，空军除航空兵、空降兵外，增加了高射炮兵、雷达兵、探照灯兵、通信兵，后来又增加了地空导弹兵等兵种，实行统一指挥，进一步增强了防空力量。国民党空军从1957年起，使用经过改装的B-17电子侦察机，利用暗夜、复杂气象，低空窜扰大陆纵深地区。1957年11月20日夜，敌一架B-17飞机低空进入大陆长达9小时，飞越9个省，甚至到达了石家庄上空。空军指挥沿途航空兵起飞18架次进行拦截，均无战果。当晚，国务院总

理周恩来指示：“告诉刘亚楼同志(当时的空军司令)，我们应用一切办法将蒋机击落。”12月18日，毛泽东主席指示：“全力以赴，务歼入侵之敌。”

1961年11月6日夜，当一架P-2V敌机从辽东半岛低空窜入东北地区上空时，先后有6个雷达站发现敌情，并连续测报，及时掌握敌机动向。我军引导高炮、探照灯部队，及时准确地一举将敌机击落。国民党空军不甘心失败，从1962年1月起改用美制U-2高空侦察机继续窜犯大陆。6月，人民解放军利用为数不多的导弹营，实施机动设伏，终于在9月9日8时32分，地空导弹2营在南昌附近，用我国的红旗-2号导弹，成功地击落1架入侵大陆的国民党空军的U-2高空侦察机，在国内外都引起强烈的反响。

越南战争初期，越南人民军防空体系中只有20多部雷达和700多门高炮，而美国依仗为数众多的现代飞机，在越南北方上空为所欲为。1965年7月24日，“萨姆-2”导弹在越南战场上首次让美国人尝到了苦头。那天，4架入侵河内的美制F-4“鬼怪”式飞机被苏制“萨姆-2”导弹击落一架



，击伤 3 架。第二天，美军使用 F - 1 0 5 战斗机，又去突袭防卫越南首都河内的越军两个导弹阵地，结果被导弹击落 3 架。从此，美国的飞机飞到高空，有“萨姆- 2 ”拦截，到了低空又有高炮和高射击机枪打击。到 1 9 6 5 年底，美国损失包括 B - 5 2 、F - 1 0 5 在内的飞机大约 1 6 0 架，其中大部分是被导弹击落的。

### “软”“硬”兼施，美空军重整旗鼓

对抗引发了竞争，竞争激化了对抗。

由前苏联制造的萨姆导弹已对美空军构成了致命的威胁，美国当局立即举行绝密会议专门研究这一问题。与会者一致认为，对付这一新的威胁的唯一途径是要研制机载电子战系统，以干扰制导地对空导弹的雷达。这一任务被作为最优先的任务交给了美国在该领域居于领先地位的某些公司。与此同时，美军努力收集有关萨姆- 2 导弹系统的战术技术情报，以寻找破敌对策。美国人发现，萨姆- 2 导弹也有弱点。就是该导弹系统在地面配备的“扇歌”制导雷达，靠超

高频无线电发出制导指令，“扇歌”雷达通常与目标指示雷达以及测高雷达配合工作。一旦这些雷达受到干扰，导弹也就失去了战斗力。

于是，美国不惜花费 25 亿美元，研制了以“野鼬鼠”电子战飞机和反雷达导弹为代表的一系列电子对抗设备，以迷惑越南的“千里眼”或直接摧毁它们，达到使越南导弹部队减弱和丧失战斗力的目的。其中“野鼬鼠”电子战飞机由 F - 105 “雷公”飞机改装而成，既能施放电子干扰，又能发射反雷达导弹，可以说是“软”“硬”兼备。这就是所谓的“软硬一体化”电子战飞机。

“百舌鸟”导弹，具有自动寻找目标功能，也就是具有“自寻的”系统。它可以沿着敌方雷达发射的无线电波束“顺藤摸瓜”，冲向雷达所在地，将雷达摧毁。在战斗中，越军要么不开雷达，只要一开动，它就能找到。这可谓是用敌方开的“路”，寻敌方的“门”，炸敌方的人，即以导弹反导弹。“扇歌”雷达一旦被摧毁，就像弓箭手被挖去了“眼睛”，萨姆导弹也就成了盲人手中的箭。

在“野鼬鼠”和“百舌鸟”投入使用之前，美军在突袭时，是使用四架由 F - 1 0 5 组成的“铁手”小队，专门进行压制干扰。突击时，“铁手”小队先行，搜索萨姆导弹的电磁信号，测得萨姆导弹的位置，然后突击机群以超出越军高射炮有效射程的高度轰炸。这就是美军在越南战场上创造的电子对抗“硬压制”战术。面对困境，在新的技术装备未到来之前，不是坐以待毙，而是创造性地研究新战法，充分发挥手中现有武器的效能，这种精神应该说是难能可贵的。

美国运来“百舌鸟”反辐射导弹，吊挂在改装的 F - 1 0 5 上，使“铁手”小队如虎添翼。每次空袭时，有的干扰机专门投放金属箔条，在轰炸机群通过的航路上形成一条“干扰走廊”；护航战斗机专门在越军可能出现的方向上空盘旋；远处有 E C - 1 2 1 预警机不时向机群发出敌情通报。F - 1 0 5 “野鼬鼠”组成的“铁手”机群，专门使用电子设备，携带“百舌鸟”导弹专门对付萨姆导弹。这就是越南战场上首创的电子战中“软”“硬”杀伤有机结合的战术。

。

在不到两个月的时间，美空军使用这种新战术，炸毁了越南北方的 106 座桥梁，而飞机的损失却大为减少。据美国人统计，1965 年越军每发射 10 枚地对空导弹就能击落 1 架美国飞机，而到 1966 年底，已下降到发射 70 枚地对空导弹才能击落 1 架美国飞机。

在越南战争后的几场局部战争中，拥有反雷达导弹的空袭一方，几乎无一例外地使用这些电子战武器和这一电子战战术，取得了有效的战果。

### 假雷达，请君入瓮

1965 年 5 月的一个早晨，1 架美国高空侦察飞机在越南义安省某山地掠过。突然，飞行员眼睛一亮，发现一部正在不停旋转的“雷达”，他吹了一声口哨，便消失在茫茫的天空。

20 分钟后，4 架载有“百舌鸟”导弹的美军 F-105 战斗机，按美军指挥所的命令，气势汹汹地向该雷达阵地扑来。“怎么没有无线电电波？”飞行员暗暗寻思。“肯定是被我们炸怕了，不敢开机！”

雷达不开机，有导弹也只能是聋子的耳朵——摆设！这一来，美飞行员的胆子顿时壮了不少。“干掉雷达！”带队长机一声令下，美机急速下降，2架一个小组，每组间隔40秒，直扑越军“雷达”。

第一架飞机刚进火力网，美机飞行员还没来得及投弹，就被一连串的炮火击中，美机拖着浓浓的黑烟，一个跟头栽了下去。同时，另一架飞机将密集的火箭和炸弹倾泻在雷达阵地上后，慌忙将副油箱扔掉，企图逃出高炮编织的火力网。这时另一处高炮阵地又吐出了火舌，“轰”的一声，美机被打得空中开花。

随后，第二波次的美机又扑向“雷达”，因为“雷达”仍未开机，“百舌鸟”导弹无法使用，只能用火箭弹攻击，于是，一架飞机在高空盘旋掩护，另一架呼啸着扑了下来。在美军密集的炮火中，“雷达”被炸得粉身碎骨，但这架飞机也被越军预先设置好的火网罩住，飞行员只感到机身剧烈的一震，拖着长长的黑烟撞在不远的山头上。另一架在高空的飞机见势不妙，慌里慌张投下了一大堆炸弹，逃窜而去。

为什么会出现这种情况呢？原来，美军自从装备了“百舌鸟”反雷达导弹后，不断使用F-105战

斗，多次成功地袭击了越南军队的雷达阵地，在一定程度上限制了“萨姆”导弹作用的发挥。越军这个雷达阵地也刚受到袭击，几部雷达被摧毁。这一天，该营营长望着一部雷达发愣。因为这部雷达损坏严重，基本无法修复。他突然灵机一动：“对，就用它作诱饵……”

在他的指挥下，一个班的战士立即砍来了几十根木头，经过设计，用了一上午的时间，树起了一部假雷达。然后，他们又找来涂料，按照真雷达抹上了色彩。一部假雷达就这样制成了。为了使雷达“活”起来，他们把天线系上了绳子，用以拉动天线旋转。同时，他们用一部可以发射电波的机器，安置在“雷达”身边，使这部雷达更加逼真。

随后，营长将“雷达”设置在靠南的山坡上。根据地形和敌机前几次来袭击的情况，他们在“雷达”两侧1，000米左右的位置，各部属了一个高炮连，形成了交叉火力；在山顶，部属了一个连，准备给敌人以迎头痛击。

越军以一部假雷达，采用高炮设伏的方法，击落了3架敌机，取得了骄人的战绩。

同样的武器装备，用得与用得不好，其结果是大不一样的。

## 电子干扰下的“布拉格之春”

1968年8月23日，一则爆炸性的消息让全世界人为之震惊：前苏联纠集了华约国家3个集团军，23个师，25万人，800架飞机，7,000辆坦克的兵力，从空中和地面对捷克斯洛伐克进行了突然袭击。6小时控制了布拉格，22小时占领了捷克全境。捷共领导人被押送到了莫斯科！这就是前苏联为对付“布拉格之春”运动而采取的侵略行径。

在入侵之前，为了隐蔽沿捷克边界布置的装甲车，苏联人对捷克和在欧洲中部的北约监视雷达使用的所有频率施放了广泛的积极干扰。许多诸如北约称之为“墩砖”、“浴盆砖”和“酪砖”型的干扰机投入了使用。这些干扰机装在车上，使用的频段覆盖了捷克及北约搜索雷达使用的所有频率。R-118通讯干扰机也被装在卡车上，以阻止或干扰北约及捷克的通信。

除了使用广泛的积极干扰设备之外，入侵那天深夜，苏联人还使用了消极干扰，使北约和捷克的雷达无法正常工作。结果，没有人察觉到苏联坦克正向布拉格开进；不知道在布拉格机场和捷克其他城市的机场已有大型运输机把前苏联的人员和武器运下来。由于苏联人没有让捷克及附近地区所有的雷达发现运载入侵力量的大型运输机，从而最大限度地保证了入侵的突然性及作战行动各阶段的安全性。捷克人简直不知道正在发生什么事情，在很短的时间里，电子干扰就使捷克人完全丧失了组织抵抗的能力。





人们不禁要问：美国和北约拥有大量雷达站、电子侦察设备，拥有世界上最先进的军事技术，对苏联的这次大规模的军事行动怎么会一无所知？

其实，北约对苏联的行动也曾发现过一些蛛丝马迹，只是未曾引起足够的警觉。

在“布拉格之春”的前一天夜晚，北约方面的雷达信号监视员曾发现了奇怪的电子信号：荧光屏上呈现出一点白斑，雷达不能正常工作。是巧合？还是有人干扰？北约无法断定。

但是，这件事情被莫名其妙地搁下，人们也开始淡忘。直到1969年初夏的一天，此事才慢慢地真相大白。

当时，濒临波罗的海的一个北约雷达站，雷达手们像往常一样正在进行例行的对空搜索。“快看！”一名雷达手忽然手指荧光屏发出了惊叫。原来，荧光屏左上方出现了一个可疑的亮点。雷达手急忙报告：“发现情况，在我雷达前方出现一架飞机，从其航线上看，是从莫斯科方向上飞来的。”指挥员命令：“加紧监视！”话音未落，情况又发生了变化，只见雷达荧光屏上的信号越变越大，最后竟使整个荧

光屏成了一块亮斑。目标正在施放干扰——训练有素的雷达员一下子明白过来，他不慌不忙地报告道：“目标施放干扰，雷达受到干扰。”

基地指挥员当机立断，命令一架北约侦察飞机起飞侦察情况，不多一会，该侦察机飞行员传回情况：“我已发现这片干扰云，但我的眼睛却无法看见什么。”“接近干扰云，尽可能摸清情况！”指挥员命令。

很快，侦察机飞行员再次报告：“我已飞临目标，但凭肉眼我仍然什么也看不见。”指挥员无可奈何，只得下令飞行员返航。

此事迅速报到了北约首脑机构，他们迅速调集了大批电子专家来破解这一费解之迷。

最后，专家们得出一致结论：苏联军队在军事上又有了新的突破，他们利用飞机发动机或火箭喷气发动机将金属粉末喷出，结果便像烟幕似的在空中布放了一道反射雷达波的“屏幕”。雷达波探测到这片“屏幕”后，就会在荧光屏上显示出一大片亮斑，从而完全掩盖空中飞行的飞机的踪迹。

前苏联独具匠心的金属微粒气状云，在空中形成了数千米甚至数十千米的干扰屏幕，成功地骗过了北约高性能的预警系统和侦察卫星，使其大规模的军事行动让北约一点也未觉察。这也说明，在高技术条件下的现代战争中，运用并发展传统的电子对抗技术，仍可以有所作为。

## 一代天骄，卫星拓展电子战空间

1957年10月4日，前苏联发射了第一颗人造卫星，吹响了人类向宇宙进军的号角。时隔3个多月，1958年1月31日，美国的人造卫星“探险者1号”也飞入了外层空间。此后30年，世界各国大约发射了4,000多颗卫星。在这众多的卫星中，有一个数字是惊人的：也就是其中有40%是侦察卫星。无论在战时还是在和平时期，它们警惕的目光，日夜注视着人类生存的这颗星球。

20世纪60年代，美国的照相侦察卫星查实了前苏联当时部署的洲际导弹为14枚，而不是原先估计的400枚，美国掌握了前苏联核力量的确实

情报，因而在苏联向古巴运送导弹期间，美国采取了强硬措施，迫使前苏联撤回导弹。

1973年10月第四次中东战争中，美国利用侦察卫星窃听到埃及空军飞行员与地面指挥员的谈话，了解到埃及飞行员的人数、住址及某些电话号码。美国的侦察卫星还发现了埃及军队部署的薄弱部位。美国将这些情报及时向以色列提供，促成了以色列军队成功地偷渡大苦湖，袭击埃及军队的后方，一举扭转了战局，使胜利的砝码从埃及一方迅速移向了以色列一方。

1976年12月，美国发射了“KH-11”照相侦察卫星，对前苏联的重要军事设施进行了密集摄影，并将其数据转变为电子信号，经由卫星传送回来。结果美国对前苏联的洲际导弹、新武器研制和试验情况都了如指掌。

1977年9月，华盛顿五角大楼的放映室里放映了侦察卫星拍摄的关于前苏联和中国军事情报的成套照片。其中有：前苏联的洲际导弹基地、导弹控制中心、导弹发射井井盖、正在建造的核潜艇船坞以

及中国的空军基地、导弹发射基地及在导弹旁边站岗的士兵等。

1982年的马岛战争中，前苏联为获取战争情报发射了10颗侦察卫星。如6月16日发射升空的“宇宙-1377”侦察卫星，将高度下降到距离地面170千米，将战场情况都拍摄下来。在此以前，英军谢菲尔德号驱逐舰的位置情报，就是由前苏联侦察卫星得知后向阿根廷军方提供的，阿军才有了“飞鱼”导弹击沉“谢菲尔德”的辉煌一幕。

只有查明情况，才能有针对性地作出决策。侦察卫星站得高、看得远、跑得快、效果好。一颗在5000千米高的侦察卫星，可以观察200千米方圆的地域。卫星速度快，一天绕地球几圈、十几圈甚至几十圈，只要轨道合适，几乎可以看遍全球。卫星侦察安全可靠，合理合法。国际公认，在距离地球表面100千米以上的空间不属于地面国家的领空范围。宇宙空间不受国界限制，卫星可以任意出入。因此侦察卫星比任何高空侦察机有更大的安全性。除了侦察卫星之外，还有通信卫星、导航卫星、气象卫星、测地卫星等。这些卫星名为民用卫星，实际上也是“

合法”的军中“间谍”。如果发射数颗卫星，构成卫星侦察网，可以对某一地区实施不间断的监视。美国发明的GPS全球卫星定位系统，它包括24颗距地球20,000千米轨道上的地球同步卫星。这些卫星连续发射特殊的信号，传送给装备有特殊接收机的军舰、飞机和地面作战部队，使他们能以非常高的精确度来确定自己的位置。导航卫星具有全球定位功能，可以提高洲际导弹、巡航导弹以及其他系统的武器的命中率，给航天、航空、航海提供全天候的、连续的导航信号。

军用卫星在现代战争中的运用，贯穿于空、天、地的每一个角落，大大拓展了电子战的空间。

### 计算机—电子战的“倍增器”

电子计算机是当代最卓越的科学技术成就之一。它以人们难以想象的高速度向前发展。计算机的运用，对工业、农业、军事、科技的发展，对人们的思想观念、思维方式都产生了巨大的、革命性影响。电子计算机使人类快步跨入信息时代的大门。

电子计算机在军事领域得到广泛的运用，从战略分析、战略规划、战役战术研究、军事演习、军事训练、作战指挥、后勤保障到武器的研制和生产，均离不开电子计算机。

在尖端武器的研制上，巨型电子计算机是研制原子弹、氢弹等核武器的有力工具。过去靠大量的核试验来摸索核武器的规律，花费大量的人力、物力和时间，有了计算机，可以摆脱过去那种理论指导实验，实验验证理论的方法，而是用科学计算的结果来验证理论，指导实践。其实质是对所研究的问题进行数学仿真，即利用数学模型在计算机上模拟事物的变化过程，探索事物发展变化的规律。20世纪90年代，有一些发达国家宣布停止核试验，并要求其他国家也给予响应。其实这一举动并不是这些发达国家要放弃自己的核优势，而恰恰相反，他们是想保持自己的核优势。因为他们已经可以利用计算机模拟核试验。

现代战争战场广阔，情况瞬息万变，堆积如山的情报需要在短时间内处理完毕，这对战争的胜败有着至关重要的作用。手工处理情报，不仅速度慢，而且准确性差。用电子计算机处理，既快又准，可以协助

指挥员在短时间内作出正确决策，实施科学指挥。有资料统计：按现有手工为主的信息处理方式，野战集团军司令部在作战过程中，只能处理收集到情报的 30 % 以下；而指挥员因时间不足，要下决心时只能使用司令部已加工情报的 10 %，显然，这势必使指挥员的决策产生很大的盲目性和危险性。

在数据处理方面，电子计算机可以自动判读卫星和飞机从高空拍摄的照片。可以利用可见光、红外辐射或地球磁场的微弱变化来拍摄照片并记录在磁带上，输入计算机。计算机对这些图像信息进行处理，并与原来贮存的图像进行比较，发现差异，就能提醒判读人员注意。因此，敌方修建军事设施或部属调整都能随时随地被察觉。

自动控制在军事领域的应用也极其广泛，小到武器的火控系统，大到全球军事指挥控制系统，都是以电子计算机作为系统中枢。导弹上的电子计算机可用于对导弹飞行政序进行自动控制，迅速修正因干扰产生的误差，使导弹准确地命中目标。飞机上的电子计算机可以用于飞行降落、领航、投弹和空中射击等系统。美国 F - 5 战斗机装有 45 个“黑盒子”（内装



有计算机)，能以 2.5 倍音速机动灵活地飞行，盯住远在 160 千米以外的目标，保证了在目标接近时能及时给予打击。

人工智能是 20 世纪 50 年代兴起的一门综合性边缘学科，是计算机科学的一个分支，主要研究用机器来实现人的某些智能活动的有关理论技术和方法。其研究结果将突破计算机只能完成逻辑运算和逻辑推理的框框，使之与信息理解系统、知识信息处理系统、专家系统、知识库等结合起来，组成一个包含人的经验因素和知识的体系，这种系统就是计算机智能系统。人工智能技术在军事领域的运用，引发了军事专家系统、智能机器人、智能武器等不断涌现。

电子计算机的出现和使用，使电子战渗透和辐射到战场的每一段时间和每一个空间，使电子战对现代战争的进程和结局作用更大。

### “人—机”一体的 C<sup>3</sup>I 系统

第二次世界大战后，随着科学技术的飞速发展，军队武器装备、编制体制、机动能力、作战范围等都

发生了巨大变化，作战指挥再延续手工作业的方式已无法适应瞬息万变的战场形势，军队指挥方式的重大变革已不可避免。1953年美国提出了军队自动化指挥新概念并迅速付诸实施前，苏联、西欧、加拿大、西德、日本等一些国家和地区也相继研制和装备该系统。

军队自动化指挥系统是在军队指挥体系中，采用以电子计算机为核心的技术装备与指挥人员相结合，对部队和武器实施指挥与控制的“人-机”系统。它综合运用现代科学技术和设备，把指挥、控制、通信和情报紧密地联系在一起形成一个多功能的统一体系。军队自动化指挥系统简称 C<sup>3</sup>I 系统，即指挥、控制、通信、情报(C o m - m a n d , C o n t r o l , C o m m u n i c a t i o n , I n t e l l i g e n c e ) 系统。现代战争中，地面、机载、舰载、星载等探测器遍布全球，不分昼夜，时刻收集陆、海、空、天的各种军事情报，这些情报不但信息量大，而且瞬息万变。军队自动化指挥系统能大量、精确、迅速地搜集、处理、传输情报。在防空技术方面，现在三维坐标雷达和相控阵雷达不但探测距离远、

精度高、抗干扰能力强，而且具有自动录取情报的能力，目标一旦进入荧光屏规定的某一区域，录取设备即自动跟踪目标，将目标的方位、距离、高度、速度、航向等数据传输到指挥中心，使指挥人员实时掌握情况，确定应战对策。海湾战争中每天的信息量至少上千万字，手工作业是无能为力的，主要由  $C^3I$  系统处理。

$C^3I$  系统能“记住”大量的数据，也就是把来自不同信息源的原始数据经过处理，存于计算机中。如美军大西洋总部舰船航行中心的计算机存有 15,000 艘舰船的各种数据。在反导弹武器系统中，计算机是整个系统协同动作的枢纽。现代战略导弹具有多弹头，能携带成百上千个诱饵，大量使用真假弹头；而目前反导系统的远程雷达的预警时间只有 10 分钟左右。只有计算机才能在这短暂的时间里，处理大量的数据，从多个真假弹头混杂在一起的目标中识别来袭的真弹头，还要计算出其飞行轨道，分配并控制导弹去摧毁敌方来袭的导弹。海湾战争中，伊拉克军队用的“飞毛腿”从发射、升空、离开大气层到击中目标，飞行 7 分钟，而美军的“爱国者”导弹是

从“飞毛腿”导弹再入大气层时的尾焰中捕捉到“飞毛腿”的信息，此时“飞毛腿”离弹着点的飞行时间仅有40秒，“爱国者”要在这40秒内对“飞毛腿”进行真假识别，计算导弹的航路、速度、弹着点等，尔后发射导弹拦截，以上过程实际上只用了20秒左右，可见“爱国者”导弹系统的功能之强大、高效。

C<sup>3</sup>I系统的核心技术设备是电子计算机，它具有逻辑判断能力，可以协助指挥人员拟定各种方案，模拟战斗过程，评价其效果，优选方案。既可以把作战的有关规则编成程序，预先存入计算机，当情况输入时，就按规则处理并显示处理结果，供指挥人员参考选用；也可以由指挥人员根据作战任务和已知情况，拟定几个作战方案，同时拟定几个敌人可能采用的反击方案，输入计算机进行“推演”，以便分析各种方案的优劣，最后选定最佳方案。

C<sup>3</sup>I系统的出现和运用，使军队指挥具有了现代意义上的自动化。也极大地丰富了电子战的内涵。

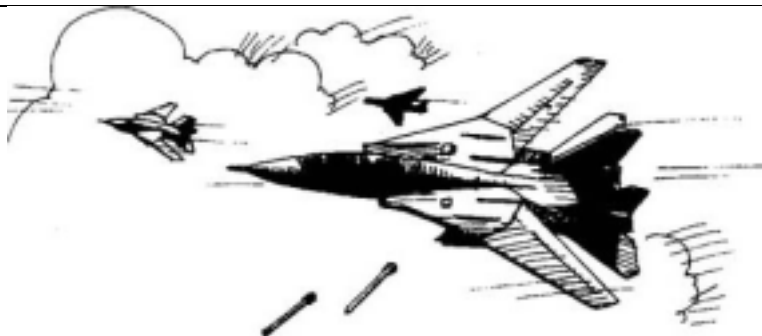
## “沙漠风暴”中的无形“杀手”

1991年1月17日当地时间凌晨2点37分，夜色苍茫中的伊拉克首都巴格达万籁俱寂，以为美国人不敢轻易发动战争的居民睡梦正浓。也就在这时，2架美国F-117隐形战斗机已经瞄准并分别发射出两枚导弹，这两枚名为GBU-15的激光制导炸弹，准确地击中巴格达通信中心大楼和防空司令部大楼，在屋内爆炸。随后，萨达姆私人住宅、总统府、地面防空雷达站、指挥控制中心和机场设施等要害目标都遭到轰炸，整个巴格达被淹没在火光与硝烟之中。“沙漠风暴”开始席卷伊拉克。

在此之前几个月，以美国为首的多国部队对伊拉克的电子战已经展开。美军从地面和空间收集了有关伊拉克指挥、控制、通信系统各电台的使用频率，多国部队通过电子侦察卫星、地面监听站、各种电子侦察飞机，对伊拉克的电磁威胁了如指掌。在通过外交谈判解决海湾冲突的一个星期前，美军就开始对伊拉克军队的电子战系统实施先期侦察和干扰。在美国的授意下，沙特战斗机曾多次闯入伊拉克领空骚扰，引

诱伊军防空的 C<sup>3</sup>I 系统开机，以便实施临时的电子情报印证。与此同时，以美国为首的多国部队，就一直断断续续多次实施迷惑性压制干扰，以麻痹伊军。

在作战时，以美国为首的多国部队坚持采用积极电子干扰、消极干扰和火力摧毁等多种方式，互相结合，压制伊拉克军队的通信系统。首先是使用地面干扰机或舰载干扰机，发射与伊拉克频率相同，但功率更大的高频、特高频噪声信号，最大限度地压制和削弱伊拉克军队的 C<sup>3</sup>I 系统，甚至使之瘫痪。在“沙漠风暴”前半小时，E F - 1 1 1 A 电子战飞机率先起飞，深入伊拉克纵深 3 2 千米，掩护突防机群起飞编队；有 4 架随突防机群一道，在接近目标的 4 8 千米的空域，爬到 1 万米左右的高空执行随队支援干扰任务。各参战飞机也采用了投放箔条这种消极干扰的办法。



美军还使用 F - 4 、 F - 1 6 等战斗机携带反辐射导弹，如伊拉克雷达一开机，就立即给予摧毁，不开机飞机就安全通过。

实施大空袭的第一天，美军共 6 0 余架次电子战飞机，用各种干扰手段，使伊拉克部队雷达迷盲、C<sup>3</sup>I 系统瘫痪，伊拉克数千枚导弹基本未能发挥作用。如此大规模的电子战，如此神奇的功效，成为二战后局部战争的一个夺目的亮点。

在这次海湾战争中，伊拉克之所以没有有效地使用防空武器，就是其防空部队在强大的电磁干扰之下，失去了与上级指挥机关的联系，因而无法接受上级的作战命令。同时，由于强烈的电磁干扰，严重削弱了伊拉克防空作战能力。在战争的第一天，伊拉克向沙特和巴林共发射 8 枚地对地战术导弹，都因受到强

烈的电子干扰而未击中目标。在战争的头两天，美军共损失4架飞机，只有一架是被防空导弹击中的。

针对美国的高技术武器装备，伊拉克也做了一定的准备，对重要的军事设施和武器装备进行了电子伪装，成功地欺骗了多国部队的侦察系统和轰炸。自1990年9月起，伊拉克关闭了大部分防空雷达系统，使美军侦察不到雷达参数和确切方位，难以制定电子干扰和反辐射摧毁的战术，这在一定的程度上削弱了美国电子战的能力，也减轻了自己的损失。

无论是从政治上、军事上、外交上等哪一方面讲，伊拉克的失败是必然的。抛开其他因素不说，光从电子战装备上看，伊拉克一方也处于明显的劣势。电子战装备差、能力低，因而难以抵挡美国的强电子干扰。

海湾战争给人们的教训十分深刻：只强调武器的威力，否定和低估人的作用是不对的；而过分夸大人的作用，忽视武器装备的更新和运用，是一定要吃大亏的。



## 电子计算机的“克星”

电子计算机是 C<sup>3</sup>I 系统的核心，它高效而又精确。但却像“一个容易受伤的女人”，非常脆弱。从 20 世纪 80 年代中期起，计算机病毒如同瘟疫一样在世界各地迅速蔓延。其速度之快、范围之广令人防不胜防。正因如此，有些国家以此为武器，目的在于把计算机病毒注入敌方武器及军事装备的计算机系统或计算机网络中，使计算机系统或网络紊乱、瘫痪。

计算机病毒实际上是一种依附在各种计算机程序中的一段具有伤害性、并能自我繁衍的计算机程序，它能不按操作者的意愿自行复制、传播。病毒并不是利用计算机操作系统的缺陷进行感染和扩散的，而是通过正常的操作，执行正常的应用程序后对计算机系统软件进行修改或破坏。

病毒程序依附一定载体而存在，侵入系统后有一定的潜伏期，只有满足一定条件后，才会触发生效。在发作前已被感染的计算机一直有传染性，所以潜伏期的染毒计算机会大量传播病毒。有的病毒的触发条

件是固定的，总是在特定的时间发生。病毒程序具有再生能力，利用自己再生机制，可将自身复制到其他尚未感染的对象中。当触发条件满足后，病毒被触发，系统资源遭到破坏。其破坏程度取决于设计者。轻者使计算机运行速度变慢，占用CPU（计算机中央处理器）资源，显示一些与程序无关的信息；重者则删除可执行文件，破坏数据，甚至摧毁系统，或使计算机死机等。

由于计算机广泛运用于军事技术装备的研制、生产、训练、作战和维护的全过程，病毒随时可能侵入。不同阶段有不同的侵入方法。主要方法有：一是战略潜伏。计算机离不开集成电路，有些西方国家投入巨额经费研究将病毒固化在出口的集成电路中的方法，在必要时激活病毒，从而达到使敌方的电子信息系统失效的目的。这种摧毁计算机的方法被有些人称之为“逻辑炸弹”。二是中间介入。在充分研究对方的科研体制、管理方法、军事技术装备设计研制方案及使用过程后，有针对性地设计病毒程序，通过特定渠道传播给对方的计算机，达到破坏军事技术装备系统的目的。三是电子传输。在作战过程中病毒武器在远

距离穿透电子信息系统或通过无线电通信和有线网络，把病毒传染给计算机，使计算机系统无法工作。四是因自我管理不善而造成的无意识入侵。病毒程序不是针对特定的军事装备，而是针对计算机领域的。由于管理不严，在军事技术装备研制、生产、维护过程中使病毒程序交叉感染，传播进来。

计算机病毒的危害很大，在海湾战争中，美军运用计算机病毒攻击伊拉克指挥中心，取得了良好的效果。在以后的战争中，计算机病毒将成为更加重要的武器被普遍使用。

除了病毒以外，美国的阿拉莫斯国家试验室还研制出了一种手提箱大小、能产生高能量电磁脉冲的设备。把它放在一栋大楼附近，其产生的脉冲可以摧毁大楼中所有的电子器件。五角大楼还在培养一种电子生物作为武器，它能吞噬计算机器件，使电子线路绝缘，从而破坏整个计算机系统。

## 神秘的“黑客”

最初，“黑客”(hacker)是一个褒义词，指的是那些努力挖掘计算机程序最大潜力的电脑精英。然而，随着黑客“功能”的拓展，黑客已渐渐地没有了褒贬之分。

1987年，美国联邦司法部门指控17岁的高辍学生赫尔伯特·齐恩闯入美国电话电报公司的内部网络和中心交换系统，成为根据美国1986年生效的“计算机欺诈与滥用法”被判有罪的第一人。康奈尔大学的研究生罗伯特·莫里斯(22岁)向互联网上传了一个“蠕虫”程序，上网后迅速扩散感染了6,000多个系统——占当时互联网的二十分之一，使网络陷于瘫痪。同年，在发现有黑客侵入军事网(Milnet)的一部联网电脑后，美国国防部切断了非保密的军事网络与阿帕网(早期的互联网)之间的物理联接。

1998年，美国国防部宣布黑客向五角大楼网站发动了“有史以来最大规模、最系统性的攻击行动”，打入了许多政府非保密性的敏感电脑网络，查询并修改了工资报表和人员数据。声称属于黑客组织“下载大师”的黑客攻入五角大楼网站，窃取了机

密软件。五角大楼随后否认这大套软件是机密的，只是承认一个保密级别较低的网络被黑客成功打入。1999年5—6月，美国参议院、白宫和美国陆军网络以及数十个政府网站都被黑客攻陷。

2000年2月在3天的时间里，黑客使美国数家顶级互联网站——雅虎、亚马逊、电子港湾、CNN陷入瘫痪。黑客使用了一种称作“拒绝服务式”攻击手段，使大量无用信息阻塞网站的服务器，使其不能提供正常服务。

据有关电子专家介绍，目前黑客作案使用的手法已知的达数千种之多，最常见的有以下几种：一是电子邮件炸弹，这是最广泛运用的攻击方式。简单地说，就是在发往对方的电子邮件中附载一个很大的文件，将对方的电子信箱“撑破”。二是使用“PING”炸弹，它是一种用来测试网络速度的小程序，这个程序会向服务器发送数据包。如果很多人同时用这个程序不断地向服务器发送数据包，服务器就会像拥挤的公路一样发生阻塞，最终瘫痪。三是套取密码。攻击者通过远程监视对方计算机等获得对方的密码，然后利用密码修改网页、破坏服务器等。四是突破防

火墙。一些攻击者利用某些防火墙的漏洞，巧妙地将自己的网址请求设置成指向防火墙的路径，接近防火墙。这种办法往往是最凶狠的，攻击的目的大多是为了修改、破坏、盗取对方需要保护的资料，甚至控制对方的整个网络系统。被公认为“世界头号黑客”的美国天才少年凯文就曾用过这种方法多次攻入美国空军、联邦调查局的计算机，夺取有关资料。

随着计算机网络在军事领域的广泛运用，黑客在电子战领域的角逐已愈演愈烈。黑客为本已神秘的电子战又遮上了一道“面纱”。

### “第一代网络战士”

1995年，美军“第一代网络战士”从美国国防大学信息资源学院毕业。美国国防部把掌握高技巧的黑客和具有广博计算机知识的人组织起来，成立了所谓信息战“红色小组”。这类组织既可以在演习中扮演假想敌，通过攻击自身的网络系统发现结构隐患和操作弱点，以便及时纠正；又可以入侵他国网络

，窃取、利用或破坏信息和数据，散布假消息，占用服务时间。

1997年6月间，美国国家安全局举行了一次代号为“合格接收者”的秘密演习，参加者是“红色小组”，另外还雇佣了35名黑客，任务是设法闯入美国本土及统率10万大军的美军驻太平洋司令部使用的计算机网络。演习的结果使美国国防部高级官员深感震惊，几个黑客小组4天之内就成功地闯入了美军驻太平洋司令部以及华盛顿、芝加哥、圣路易斯和科罗拉多州部分地区的军用计算机网络系统。美国联邦调查局和国防部都试图找到黑客，但只发现了其中的一个小组。通过计算机、调制解调器和电话线，使一些在因特网上唾手可得的软件，就能轻易对计算机网络进行大规模的破坏活动。因此，美军认为，在未来计算机网络进攻战中，“黑客战”将是基本的战法之一。

军用计算机网络作为计算机网络发展最早也是最快的部分，很早就被应用于网络攻击问题的研究。时至今日，军用计算机网络攻击手段已是花样繁多，功能各异，构成令人生畏的网攻击库。计算机病毒就是

这一武器库中庞大的组成部分。美国现在正开展用无线电方式、卫星辐射注入方式、网络方式把病毒植入敌方计算机主机或服务传感器、网桥中的研究，伺机破坏敌方的武器系统、指挥控制系统、通信系统等高敏感的网络系统。为了达到目的，对出售给潜在敌手计算机芯片进行暗中修改，使之可遥控使用，也是主要的网络进攻手段，现在被称为“芯片武器”或“芯片陷阱”。据报道，美国国家安全局、中央情报局早已开始研制芯片武器，并在出售给别国的武器系统中使用经改装的芯片，以起到“定时炸弹”的作用。据称，美国正在进行的 C P U “陷阱”设计，可使美国通过因特网发布指令让敌方电脑的 C P U 停止工作。

从网络防御的角度讲，计算机黑客是一个挥之不去的梦魇，但从网络进攻的角度来讲却恰恰相反。借助黑客工具软件，黑客可以有针对性地频频对敌方网络发动攻击让其瘫痪，多名黑客甚至可以借助同样的软件在不同的地点“集中火力”对一个或多个网站发起攻击。而且黑客们还可以把这些软件神不知鬼不觉地通过互联网安到别人的电脑上，然后在电脑主人根本不知道的情况下为我所用——以别人的电脑为平台



，对敌方网站发起攻击。雅虎等网站被袭击事件中，黑客就是利用斯坦福大学、洛杉矶加州大学和加州大学圣塔巴巴分校的计算机作为发起破坏行动的平台。

战场上，时间就是生命。雅虎等如此众多的大型网站连续遭到黑客攻击，被迫中断服务长达数小时之久，从军事角度来讲具有极其严重的后果。众所周知，美国国家战略预警系统现有预警能力只能提供 3 — 4 5 分钟左右的预警时间，假如该系统遭到攻击，后果不堪设想。因此，如果一国的网络防御问题没有加以妥善解决，则敌对国家或恐怖组织可以以黑客战的形式控制其军事信息系统，在电子战中占得先手，由此大大降低该国武装力量的部署与作战能力。与此同时，建立起有效的计算机网络防御体系又是一个动态的过程，不存在一种能够一劳永逸地对付计算机网络攻击的防御措施，因此，计算机网络安全问题已显得日益紧迫和重要。

## 网络催生的“第四领土”

在人类社会的发展过程上，人们对“领土”的认识是从土地开始的。土地是人类赖以生存的基础，对土地的拓展和守卫，使土地——构成了“第一领土”的概念。然后，由于技术的发展，人类开始从土地走向海洋；通过对海洋的开发和利用，人们开始认识到海洋有土地不可替代的作用，“第二领土”——“领海”孕育而生。当科技之“风”把人类送上天空后，1900年法国的法学家首次提出要制定国际空间法，并提出了领空的问题；随着飞机的发明，无线电技术的发展，各国更加意识到“领空”——第三“领土”的重要性，并把20世纪誉为经典空间技术的世纪。

美国率先建起“网络信息高速公路”，它们无声无息地穿越了国界，很快裹起了“地球村”。等到他国醒来时，发现美国人的那条“公路”已经成了美国的新“领土”，凡进入这片“空间”的人必须向美国“申请护照”了。站在这片“领土”面前，人们突然发现，原子弹虽然能摧毁地球上的一切，却只能成为争夺霸权或捍卫主权的工具，而不能成为“领土”和“主权”的本身。

在互联网所营造的没有疆界的电子空间中，国家主权的概念正经受着前所未有的冲击。在某些方面互联网已突破了主权的范围，使主权受到新的威胁和考验。由于网络以无形的方式深入到各个主权国家之中，这就使国家安全的概念发生了巨大的变化，维护国家主权的斗争由有形的现实世界，扩展到无形的虚拟电子空间。在网络的世界里，一个国家的经济主权、政治主权、文化主权、军事安全等都越来越依赖于“第四领土”的有效管辖。在这里虽然没有高楼大厦，没有界碑，但它流动的信息甚至比蕴藏的石油资源更为重要，它与捍卫领土、领海、领空权有同等重要的战略意义。今天，一个国家在维护其陆地、海洋、天空主权的同时，只有充分挖掘“第四领土”的潜力，并实施有效的管辖，这个国家的主权才是真正意义上的完整。

1995年，美国提出了“战略信息战”的概念，意在通过袭击和操纵计算机网络的办法，对敌国防防和基础设施实施破坏，从而达到其战略目的。他们把这种“不费一枪一弹的战争”与核战、生化武器战并列为对国家安全最具威胁的三大挑战。在《全球信

息基础设施》中，美国人直言不讳地提出，要通过发展全球基础设施，“促进民主的原则，限制集权主义政权形式的蔓延”，并“使世界具有更大意义上的共同性”，这显然是要在全球推行自己那一套政治和文化准则。1998年，美国总统克林顿发表了引人注目的“网络新政”演说，其核心要点之一，就是继续保持美国在高科技上的绝对领先地位，为其政治霸权服务。据透露，克林顿曾批准中央情报局出动电脑黑客，实施颠覆南斯拉夫联盟政府的绝密计划。还有消息说，微软的“Windows”操作软件留有可供美国国家安全局随意出入的“后门”，英特尔“奔腾”三代处理器上的序列号亦被认为是网上信息安全的隐患。因此，后发展电子信息技术的国家如何适应新形势，维护自身主权和安全不受侵犯，将是网络时代需要解决的重要课题。

现在，包括欧洲国家在内的许多国家都已识别了美国的网络霸权，都在努力探索发展新路。我国很多院士提出，要用“两弹一星精神”（原子弹、氢弹、卫星）来研制自己的CPU、操作系统、网络方案、密码芯片和大型数据库等，特别是新千年伊始，我们研

制自己的 C P U 技术方案已获通过，海外华人科学家闻此消息兴奋不已，称“中国赢得信息时代自由解放的日子不远了”。

电子战作为信息战的核心，任重道远。

## 二、战场搏杀——回眸电子战

### 电子战“擒获”的第一位舰队司令

在朝鲜和日本之间的海峡中，有一座对马岛，它亲眼目睹了发生在 1905 年 5 月 27 日的对马海战。这一天，俄国海军上将罗泽斯特文斯基率领的庞大舰队，在对马海域遭日本海军舰队的猛烈袭击，整个俄舰队只有 3 艘设法逃脱，其它所有军舰不是被击沉，就是升起了白旗，刚愎自用的舰队司令官罗泽斯特文斯基也成了日本人的阶下囚。

日本人在马岛海域的成功，应归功于对电子信息控制的成功。

在 20 世纪初，对电子信息的控制主要体现在对通讯的侦察与反侦察上。在日俄战争这一大背景下，日本人利用了无线电的潜力，而俄国人却未能有意识地加以利用。从 1904 年开始，形势越来越对俄方不利，在和日本舰队的多次战斗中，他们损失了远东的大部分军舰。于是，圣彼得堡的统治者决定把波

罗的海舰队遣往远东以替换那些损伤的舰只，并为他们的失败报仇雪恨。沙皇统治者，把这一事关国家威望和海军舰队存亡的重大责任系于罗泽斯特文斯基的身上。

这个罗泽斯特文斯基原来只是一个小小的舰长，在一次为迎接德国皇帝威廉二世而举行的盛大欢迎仪式中，一跃成为舰队司令的。

1904年10月14日，波罗的海舰队的59艘军舰，在舰队司令罗泽斯特文斯基的指挥下，从芬兰湾的利耶帕亚起锚驶向遥远的、位于西伯利亚东岸的海参崴港。他们来到大西洋，绕过非洲大陆，耗时200天，航程18,000海里，历尽艰险，终于1905年5月中旬进入中国东海。

如何从中国东海到达海参崴港？摆在罗泽斯特文斯基的面前有三条通道：一是中间有一座对马岛的朝鲜海峡；二是在两个日本岛屿本州、北海道之间的津轻海峡；三是更北一些的位于库页岛和日本群岛最北端之间的宗谷海峡。在三条可选的路径中，首先要考虑的问题是如何在到达港口之前不与日本舰队相遇。舰队所有的官兵都清楚地知道：他们经过了长期航行

，疲惫不堪，如果真的和日本人交了火，在没有得到补给和休息的情况下，实力肯定大打折扣。很多人深信他们应经过北部的津轻或宗谷海峡，因为它们都离开设在朝鲜的日本海军基地较远，而且都离海参崴较近。但奇怪的是，舰队司令罗泽斯特文斯基却宣布：走直线，通过朝鲜海峡！

此时，日本舰队司令东乡平八郎指挥的大部分日本军舰都集结在朝鲜海峡南端的马山海湾，并已作好立即开赴开阔海面拦截敌舰的一切准备。而且，东乡已建立起严密的监视系统，由定点布置的舰只进行连续巡逻、跟踪。东乡作战计划的成败，取决于他最大限度地提前发现俄舰的能力和快速的无线电预警。就是说：整个计划基于他的无线电通信网的效率和速度，否则，俄国舰队就会逃脱。

1905年5月25日，俄国舰队分为两长列，以每小时9海里的速度向朝鲜海峡航行。海面上波涛汹涌，能见度很差。早晨，俄国舰队就从无线电接收机中开始侦听到微弱的信号。当他们越来越接近对马海峡时，侦听到的无线电信号幅度也越来越大。这表明，俄国人离日本舰队不远了！



然而，罗泽斯特文斯基根本就不把日本人放在眼里，甚至也不听参谋们的建议，连派鱼雷艇侦察也嫌麻烦，下令舰队继续沿着他选定的航线前进。

5月27日晚上，浓雾密布，天上只有朦胧的残月，能见度下降到只有1海里。这时日本巡洋舰“信乃丸”正在按计划巡逻。一开始并没有发现任何可疑目标，到了2时45分，突然透过浓雾看见一艘亮着航灯的船开来。日本巡洋舰不能分辨这艘船的种类、国籍，也不清楚它是单独的一艘船，还是编队中的一员。于是，日舰决定保持无线电寂静，尾随其后继续侦察。

清晨，约4时30分，“信乃丸”向不明船靠近并看出这是一艘俄国医疗船。这时，后者也注意到日本的巡洋舰，但误认为是自己的同伴而用信号灯进行联络。俄国船犯的这个错误，使“信乃丸”上的指挥官推断出它一定是编队中的一艘。果然不出所料，到了4时45分，在大雾渐散时，“信乃丸”终于非常吃惊地看到了一长列俄国战列舰和巡洋舰，日本人被惊出了一身冷汗。

“信乃丸”立即用无线电向舰队司令东乡报告，但是由于两者之间的距离太远和当时的气象条件，船上简单的无线电设备无法发出这个重要消息。这时，罗泽斯特文斯基的舰队也看到了日舰，它正在俄国舰队平行的航线上行驶，在晨雾中时隐时现。俄舰队大部分官兵都急不可待，希望司令官派最快的巡洋舰去摧毁日本巡逻舰。在这个极为关键的时刻，俄国战舰的命运和整个战争的结局都取决于这个决定。终于，罗泽斯特文斯基下令：舰队所有的大炮对准日舰，但神使鬼差的俄国司令官此时并不下令开火，犯下了一个不可思议又无法挽救的大错。

同时，在俄国舰队的“乌拉尔”号上，舰长对司令未采取任何有力措施深为不满，决定和无线电报务员商量如何采取措施阻止日舰的无线电发射。他们认为：只要发射与日舰所用频率相同的连续信号就足以干扰日舰的发射。于是，舰长及时用信号向旗舰请示：“用无线电进行干扰。”几分钟后，舰队司令作了简短回答：“不要阻止日舰的发射”！日舰在没有受到任何干扰的情况下，把“发现敌舰队”的重要信息传给了东乡司令。接着又连续不断地把俄舰的航

线、位置、速度等等情报——上报日本舰队。没有充分认识到电子干扰价值的罗泽斯特文斯基又铸成了一次大错。

拂晓之前，浓雾再次密布海面，给俄国人提供了一个迅速改变航线，直逼津轻或宗谷海峡以避免日本舰队袭击的机会。罗泽斯特文斯基没有听从参谋人员的正确意见，仍然一意孤行。在形势非常紧迫和危急时刻，俄国舰队许多高级军官被罗的顽固态度所激怒，他们共同命令无线电操作员立即向日本巡逻舰发出强有力的电子干扰。可惜，为时已晚，俄国人无法改变一步一步地走向死亡的悲惨命运。所有的机会都失去了！

当晨雾散尽时，日本人已经在那里恭候多时了。

两支舰队一遭遇，罗泽斯特文斯基拿出了表演射击时的自信和果敢，立即命令舰队开火射击。两分钟后，当他的军舰刚进入射击位置时，日舰队司令东乡马上用大炮进行回击。炮弹像雪崩似地落到俄国旗舰上，俄军参谋人员集中的舰桥受到反复炮击，罗泽斯特文斯基自己受重伤而不省人事，他的指挥班子也或死或伤。俄舰队一看旗舰惨败，司令官已成俘虏了，

纷纷举起白旗宣布投降。这个不可一世的罗泽斯特夫斯基，这个庞大的俄国舰队随着浓浓的烈火和硝烟，带走了俄国人的全部希望而覆灭了。

一场并不是严格意义上的电子战就这样给俄国人狠狠地上了一课。不学习新技术、不懂得新技术、不运用新技术，必然成为新技术的囚徒。

### 诺曼底登陆中的电子战

诺曼底登陆战役，是以英美军队为主的盟军与希特勒军队之间的一场殊死的搏杀，被军史专家们称为第二次世界大战中最困难、最危险的战役。当时，双方都非常清楚，如果登陆成功，由 1 0 0 万德军据守的“大西洋堡垒”便会顷刻倒塌，2 0 0 多万盟军将从这里开始直捣德国本土；如若进攻失败，美国将元气大伤，英国不得不谈判求和，因为英国在这次进攻中用尽了其军械库中的一切东西。

由于这次行动关系着双方的生命，纳粹头目希特勒曾一度惊恐万分；英国首相丘吉尔曾做过登陆时会发生什么情况的恶梦；美国总统罗斯福也拖着病体为

此东奔西忙。这次战役的盟军最高统帅艾森豪威尔将军在给华盛顿的一位朋友的信中写到：“重大的日子临近了，紧张情绪在增长，所有的人愈来愈变得焦躁不安。因为关系重大，这一次的气氛大概比以往任何时候都要显得惊心动魄。在这一特殊的、充满惊险的行动中，我们不是在冒一次战术失败的危险，而是生死存亡在此一举。”

盟军之所以实施诺曼底登陆战役，就是要在西欧开辟第二战场，迫使德军多面作战。要登陆，就要选择合适的登陆地域。当时，法国比较适宜的登陆地点有 3 处：即康坦丁半岛、加莱海滨和诺曼底。盟军对这 3 个登陆地区作了认真分析，认为：从康坦丁登陆容易成功，但该半岛地形狭窄，登陆后不易展开兵力和向纵深方向发展；加莱地区虽然离英国海岸最近，但距离英国主要港口较远，又是德国军队重点设防的地区，并且海滩偏窄、岩石险峻、缺少内陆通道；而诺曼底地区敌人防御松懈，能建立起同时容纳 26 个至 30 个师的登陆场，距离英国主要港口朴茨茅斯又比较近等优越条件，因此最后决定，从诺曼底地区突击登陆。

那个年代，登陆行动的决定性阶段是用登陆艇把兵员从军舰上运到海滩，这一行动要持续几小时，如果敌方掌握了准确情报，集中了足够的兵力，并占据有利的地形，登陆部队就会被击溃。因此，这一战役能否成功，从盟军一方来说，就是要采取一切有效手段迷惑德军，使他们弄不清、甚至弄错登陆的地点，等到真正打起来以后，他们再调动军队就为时已晚。于是，战争史上一个庞大的伪装行动开始了。这就是名为“坚忍”的欺骗计划。电子战则充当了这一计划中的主要角色。

盟军首先在加莱对面的英国东部设立了一个虚构的“第一集团军”，让大名鼎鼎的巴顿中将担任司令官，让他在肯特惹人注目地抛头露面。盟军经常从这里拍发各种假作战电报，散布盟军即将渡过海路最短的多佛尔海峡的谎言，有时还故意制造些并不存在的“秘密”，并巧妙地让这些“秘密”泄露出去，造成盟军就要对加莱地区实施大规模登陆作战的假象。这些“泄密”现象与模拟准备登陆行动密切配合，因而惟妙惟肖，达到了以假乱真的程度。



盟军在奥维尔、多佛尔、福克斯通等港口和泰晤士河口，精心设计、构筑了规模宏大的假码头；设置的大量舰艇模型，引人注目地分布在东南沿海一线，并故意让一些从高炮群“漏网”的德国侦察飞机拍下这一组组“重要”的镜头。同时，连篇累牍的新闻、电讯渲染着巴顿部队的行动；大功率、多频道、频繁

的无线电联络，给人们这样的印象，很多部队正在这里集结，准备在加莱地区登陆。

1944年6月5日夜晩，等待已久的时刻终于到来，登陆行动开始了。在佯动的加莱、康坦丁半岛方向上，成千只装着角反射器的模拟舰艇，拖着涂铝的气球迅速驶近，这些气球所产生的回波和大军舰一样。几十架飞机在模拟舰艇上空，投放了大量的箔片。这一切使德军雷达的荧光屏上，出现了大量的飞机和庞大的舰队，铺天盖地压向加莱一带海岸。此外，盟军空降兵登陆的同时，还派出大批运输队到加莱地区实施战役佯动，致使盟军登陆后德军仍误认为诺曼底登陆只是一种牵制行动，仍以很大兵力用于防御加莱地区，严重地削弱了诺曼底地区的防御力量。

在盟军主攻的诺曼底方向，20架装有大功率干扰机的飞机，沿着英国南部沿海，对德军的雷达实施强烈干扰。盟军的1,200多架运输机从英国的20多个机场同时起飞，满载着3个空降师飞越英吉利海峡，在预先选定的诺曼底海岸的空降场迅速着陆。在波浪滔天的大海上，2,700艘各种型号的舰只载着数十万大军，向诺曼底方向驶去。当临近登陆时



，所有舰载电子战设备同时开机，产生了足够强的干扰，使德国布置在海岸的火控雷达失效。

对盟军来讲，一切按计划进行，诺曼底登陆取得了巨大成功。电子战使德军产生了混乱，直到盟军成功登陆后的第二天，还使德军的头目，包括希特勒产生一连串的判断错误并作出错误的决定。

丘吉尔关于诺曼底登陆有这样的一段话：“我们的欺骗措施在总攻开始之前和总攻开始之后，有计划地引起敌方的思想混乱。其成功令人赞美，而其重要性将在战争中长期经受考验。”无疑，电子战为诺曼底登陆战役的辉煌胜利添上了浓重而又独特的一笔。

诺曼底登陆战役突破了希特勒吹嘘数年的“大西洋堡垒”，使德军陷入苏军与盟军的東西夹击之中，并开始节节败退，也使世界人民看到了二战胜利的曙光。

## 古巴导弹危机

1963年11月22日，美国总统肯尼迪遇刺身亡。行刺者很快被捉拿，他年仅24岁，名叫奥

斯瓦尔德。次日，行刺总统的人，又被一个“愤怒者”当众击毙……对刺杀肯尼迪的动机，人们有种种猜测，因为奥斯瓦尔德亲近前苏联、同情古巴，因此，人们难免会把此事与前不久发生的“古巴导弹危机”联想到一起。

1962年夏末的一天，当时美国海军正在加勒比海巡逻，电子侦察船“玛拉”号侦收到来自古巴岛附近不寻常的电子信号。这些雷达信号被记录在磁带上立即送回华盛顿分析，以识别出这种新型雷达。当美国人获悉它是苏联带核弹头的弹道导弹制导雷达时，不由大为震惊。

为了证实这一发现，美国海上巡逻飞机被派往加勒比海执行电子侦察任务。几天之内，沿佛罗里达海南部海滨架设起高灵敏度的侦听接收机，其天线全部指向古巴。古巴岛上与外界所有的无线电通讯联络全被侦收。

紧接着，在10月14日，一架U-2飞机被派往古巴进行空中侦察。在大约30,000米高空，U-2拍摄下来的照片，很快就被冲洗出来，并送中央情报局专家检查。这些照片与两年前即1960

年 1 月在古巴上空另一架装有红外摄像系统的 U - 2 飞机拍摄的照片进行了比较。那时已把古巴每一寸土地都拍摄下来，并且未让古巴的防空系统察觉出来。

经过对照片详细分析后，次日晚上美国人得出了中程弹道导弹基地位于圣克里斯托瓦乐附近的结论。在古巴上空进一步的飞行侦察证实了苏联人实际上已架设了若干枚这样的导弹，而且正在架设远程导弹发射台。这些远程导弹的射程大约是 1，6 0 0 千米。因为古巴位于美国的南部的“家门口”，一旦在古巴布置了苏联的这种远程弹道导弹，它能击中和摧毁美国的许多目标，包括华盛顿、巴拿马运河和一些战略空军司令部的基地。

美国总统约翰·肯尼迪在 1 0 月 1 6 日早晨得知这一情况后，立即与其最密切的顾问商议，要求他们深入研究这些导弹的存在给美国带来的危害和美国应采取的行动。

一个工作小组审查了各种建议，并在 U - 2 加紧飞行侦察的同时，接连讨论了五天。几天之后，前苏联外交部向肯尼迪总统保证，前苏联只向菲德尔·卡斯特罗提供过防御性武器。



10月27日，一架在古巴上空进行侦察飞行的U-2飞机被前苏联的萨姆-2导弹击落，飞行员身亡。U-2飞机立即停止执行侦察任务并由驻扎在佛罗里达的战术空军司令部的麦克唐纳RF-101巫术师型飞机接替侦察任务。这些飞机的时速是两倍音速，高度范围高可达15,000米，低可接近树梢。它们装有电子系统控制的摄像机和供夜间拍摄用的曳光弹投放器。

RF-101经过短期而又紧张的昼夜低空飞行，不仅从照片上，连飞行员肉眼都能看到，42套中程弹道导弹发射架和12套远程弹道导弹发射架与制

导雷达都已经部署完毕。它还证实了古巴拥有 4 2 架伊尔- 2 8 喷气式轰炸机、1 4 4 枚萨姆- 2 导弹、4 2 架米格- 2 1 战斗机和几艘前苏联造的导弹快艇，以及大约 2 , 0 0 0 名苏联军事顾问和技术人员。地面侦听站也提供情报证实了先前侦察船和飞机侦收到的辐射信号范围，但没有存在核弹头的依据，它们可能是和导弹一起由许多正从前苏联驶向加勒比海的商船运来的。

根据大量的证据，肯尼迪总统向美国及盟国通报了已经发生和将要发生的情况。此事立即在美国引起一片哗然，也绷紧了盟国的战争这根敏感的神经。如何处理这一棘手的问题，对年仅 4 5 岁的肯尼迪无疑是一个巨大的考验，对他争取连任总统也是机遇和挑战并存的一份试卷。以强硬而著称的肯尼迪决定采取行动。

在可供肯尼迪选择的方案中，他决定采用对古巴进行海上封锁的办法，所有装载武器的船只无论其是什么国籍都不准进入古巴水域。但是，前苏联当时毕竟是世界上两个超级大国之一，美国人还必须顾及苏联人的脸面，所以这一行动被称为“海上检疫”。

一天，18艘载有导弹和附件的前苏联商船正朝古巴驶来。美苏在大西洋上的一番争斗似乎不可避免，这意味着第三次世界大战的可能爆发。当时，美国总统肯尼迪和苏联部长会议主席赫鲁晓夫都难以预料将会发生什么，事态的发展成为全世界关注的焦点。

由潜艇护航的前联商船，一直处于美国人的监视之下，并越来越近。当第一艘船被拦住，受到检查、盘问并要其马上改变航线的时候，赫鲁晓夫终于退怯了，在美国允诺不攻打古巴的前提下，他下令船队返航。

自从1945年以来，世界还从未像1962年10月那样如此接近核战争悲剧的边缘。假如美国海军没有如此迅速地收集和评估有关前苏联雷达的电子情报，让苏联有时间在古巴安设更多导弹的话，世界的局势可能趋向严峻，因为一旦安装完毕，再要拆除就很困难了。

第二次世界大战以来，出现了多起国际危机，电子战在这些危机中扮演了重要的角色。在古巴导弹事件之后，苏联人感到丢了面子，便开始大规模地制造大型舰船，每年都有许多新型的军舰下水，壮大了海

军力量，使前苏联成为世界上第二大海军强国。他们特别注意在新舰上安装各种各样的电子设备，提高了电子对抗能力。苏联人还努力发展其商船和辅助船只，以适应电子侦察任务，其中不少直接由海军控制，它们也成为苏联海上力量的一个重要组成部分。

### 在战鹰展开翅膀以前

1967年6月5日，以色列开始实施了一个“将敌机全歼于地面”的计划。也就是让敌对方埃及的飞机还没有升空、不具备作战能力的时候，就将其击毁。要实现这一计划，就必须使敌方出乎意料并使其通信和监视系统瘫痪。

为了不让阿拉伯人察觉迫在眉睫的进攻，以色列精心拟制了欺骗敌人的计划。早晨的飞行训练照常进行，而进攻的时间则定在7点45分，因为从拂晓到7点30分这一段时间里，大家都认为是爆发战争的时间，埃及飞行员处于戒备状态，而在7点30分后，飞行员都去机场餐厅吃早饭，参谋人员也都要回办公室去。

以色列事先的区域性侦察飞行已经掌握了阿拉伯空军中队和雷达站的布署、雷达的覆盖空域及其盲区，以色列飞行员还绘制了详细的超低空飞行航线图，以保证飞行时不被敌方雷达发现，以造成攻击的突然性。在开罗西部的机场，埃及空军不仅停有用于首都防空的美格-21，还停放有重型轰炸机图-16。通过对照片的仔细分析，以色列飞行员已经可以识别摆放在机场上的真飞机和假飞机。

精明的以色列人还精心策划，让自己的战斗机并不直接飞向目标，恰恰相反，以空军的第一梯队先是飞向埃及的沿海一带，然后贴着水面从西进入，正好同埃及人判断的方向相反。

进攻计划7点45分次准时开始。一切似乎都是在按照以色列人的预想进行，此时除一架飞机外，埃及所有的飞机都“趴”在地面。那架在空中的双引擎伊尔飞机载着3名埃及武装力量的高级指挥官正飞向与以色列接壤的边境。他们之中，有一位是国防参谋总长艾默少将。当时，收音机上的通信装置都打开着，他们没有发现什么异常情况，可过了一会，突然



收到埃及空军一个基地管制塔台的报告：机场遭到轰炸！

接此报告后，伊尔飞机马上返航，此时将军们很想了解一下地面的情况，就与地面司令部联系，可是，无线电中传来的只有一片嘈杂声。他们想在一个机场降落，但从能听到的少数几个字中得知，该机场正遭到袭击。他们甚至连续几次想在苏伊士运河附近的空军基地降落，都因机场受到攻击而未能如愿。最后该机设法在开罗机场降落。当他们回到最高司令部后才得知——整个埃及空军实际上已经被消灭。

本来，以色列飞机架数非常有限，但他们充分利用了路程短这一特点，注重提高飞机的使用效率，许多飞行员每天要飞 8—10 个架次，使数量有限的飞机，完成了近 1,100 个架次的飞行。在第一次攻击后，埃及的雷达、无线电通信就已瘫痪，这使埃及人大为震惊。以色列的飞机执行完第一次任务回到基地后，重新加油装弹，然后换上新的飞行员再次出击。在歼灭了埃及 320 架飞机中的 300 架之后，以色列又成功地摧毁了约旦、伊拉克、叙利亚的空军。

在夺得空中绝对优势之后，以色列空军投入了对地面部队的战术支援。10万埃及人组成的西奈远征军被以色列的装甲部队击溃，混乱不堪，抛弃了许多崭新的武器装备，包括刚刚从苏联人手中得到的坦克和电子装备。

6月5日清晨，在以色列发起首次大机群密集空袭的同时，他们不仅破坏了开罗、大马士革、安曼之间的通信联络，全面干扰了埃及的通信系统，并派出电子干扰船，干扰埃及的地面防空雷达。对航空兵飞行地带内的防空部队雷达进行了重点压制，对远距搜索雷达、航空兵和防空兵指挥控制雷达也实施了干扰。以色列还破坏了西奈半岛上埃军的有线通信线路，在战争的第一天就摧毁了西奈半岛上埃军的前线通信枢纽。以色列利用己方通信设备，使用获得的埃及和叙利亚通信频率和破译的通信密码，混入对方无线电网络，由一名操一口流利埃及语的播音员冒充敌方电台，下达假命令、假指示，调动埃及与叙利亚部队按自己的意图行事。

在西奈战线上，埃及在调动第4坦克师对以军进行反突击时，部队在途中突然接到以色列冒充埃军发

出的假命令，致使该坦克师向苏伊士运河方向撤回，结果，埃及的反突击计划落空。以色列还“指挥”埃及的重炮部队向自己的部队开炮轰击了2个多小时，并诱骗埃及运送弹药和油料的车队进入布雷区，使其遭受巨大损失。

9时30分，一个负责保护运河区的埃及米格-21歼击机中队从古尔代盖机场起飞，并冲进了以色列的由16架飞机组成的机群。尽管埃及的飞行员十分勇敢，但由于机载雷达受到干扰等原因，没有取得大的战果，在几分钟内反而被对手击落4架；有的飞机在返航时，由于机场被炸，坠毁在跑道上，还有的飞行员在油料燃尽后只好弃机跳伞。

在另一场战斗中，也由于以色列强烈的电子干扰，埃及的8架米格-21刚刚升空就遭到以色列一个“幻影”战斗机飞行中队的拦截，最后以全部8架的代价换取了对方的两架幻影飞机。

10时50分，约旦4架猎人式战斗机从马夫拉克起飞，扫射了以色列的凯法·锡尔金机场跑道，并打掉了2架超级熊式飞机和几部车辆。然而，当约旦皇家空军的英雄们返回自己基地上空时，基地雷

达和机场跑道正遭受以色列幻影式战斗机的攻击。约旦皇家空军无法与地面取得联系，加之通信和相互间的联系被干扰破坏，当即被击落 2 架，另外 2 架试图在被破坏的跑道上强行着陆时也爆炸了。

整个上午，一场一边倒的战斗按照以色列人的意愿顺利进行着，阿拉伯人的抵抗效果甚微。而以色列在摧毁了约旦空军之后，又由“幻影”和神秘式战斗机对哈巴尼亚实施攻击，进而摧毁了伊拉克空军 9 架米格-21 式、5 架猎人式和 4 架伊尔-14 式飞机。

对于埃及来说，6 月 5 日是一个灾难性的日子。以色列的突然袭击，使埃及的绝大多数飞机还未升空就被炸成了碎片。夜晚，约旦、叙利亚和伊拉克的空军也全部被摧毁。

显而易见，在空中作战时，没有电子对抗能力的一方与熟练掌握电子对抗手段的一方是不可同日而语的。

## 跨越“巴列夫”防线

1973年10月6日，按照犹太教的教义，这一天是犹太人的赎罪日。按传统习惯，在赎罪日，以色列军政机关大多放假，电台停止播音，居民参加宗教活动或者留在家中……

时针指向开罗时间14时，叙利亚和埃及为了收复被以色列夺取的西奈半岛及格兰高地，突然发兵，以迅雷不及掩耳之势向以军的防守阵地展开了大规模的进攻。

几千门大炮、迫击炮和坦克炮万炮齐鸣，几百架米格-21、苏-7和“猎人”飞机腾空而起，对着苏伊士运河东岸以色列的前线机场、部队指挥所、通信和电子对抗中心，对着以色列的炮兵阵地、导弹阵地、弹药库以及其它重要军事目标狂轰滥炸。接着埃、叙两军使用电子战部队干扰以色列的通信指挥系统，压制了无线电导航系统和地空导弹武器系统的引导站，以及大部分远程通信设备。另外，以色列沿运河的一些无线电台和雷达站还遭到了埃军特别小分队的破坏。

紧接着，第一波次约8千名埃军士兵或乘橡皮舟，或乘水陆两用战车，奋力向对岸冲去。几分钟

后，埃及的 8 0 0 多辆坦克通过浮桥跨越“巴列夫”防线。

此前，本来在接近西奈前线的地方，美国为以色列提供的尖端电子设备，日夜监视着埃及的军事动态，美国电子情报机构国家安全的电子计算机专家，也为以色列分析、整理、通报了侦察的结果。美国设在伊朗南部的一个基地，也一直监听中东的无线电通讯，在地中海还派有间谍船。过去两三年里，埃及集中在运河地区频繁进行的演习；近一年来，埃及赶造新堤岸和碉堡工事；9月21日以来，埃及军队准备开始的演习发生的不同以往的变化，比如：第一次以整个师的兵力进行演习、开罗军事司令部的无线电通讯联络突然从监听网中消失，埃及组建大大超过了单纯演习需要的通讯网，埃及和叙利亚的军队都在集结等，以色列的监察网听得见，为以色列提供情报的美国卫星也都看得见。但以色列却没有把它看成是阿拉伯人准备发动进攻的迹象。他们满不在乎的认为，这无所谓！埃及人“只不过是让他们的部队忙着有点事干罢了”。

原来，埃军采取了“瞒天过海”之计，巧妙地骗过了美国和以色列的空中电子情报网。



事情还得从1973年7月说起。埃及要发起对以色列的进攻，必须进行周密的准备。埃及情报机关知道，为以色列提供情报的美国卫星，能够极其准确地拍摄到军事装备离开原地进行移动的照片。用什么办法瞒过间谍卫星的眼睛呢？这是一个必须解决的难题。为此，埃及成立了一个专门研究对付卫星侦察的小组。这个小组仔细分析了通向战场的道路及其特点

，并研究了美国卫星的轨道及发射时间，然后编制了几个复杂的时间表。在这个表上，标有部队的行动时间、停留地点，以及停留的详细时间。另外，发布了必须严格遵照时间表行动的强制命令。根据规定，开往前线的队伍化整为零，分批行动，所走的路线全都是精心挑选的，其中有一些是羊肠小道。而当运兵的空车返回时，则有意结成一些大型车队，并且选择一个适当的时间行动，以便使收寻情报的间谍卫星正好能飞过他们的头顶。这样，敌人虽然会收到很多空中照片，但是，这些照片只会导致他们得出相反的结论。

在战争爆发的前一个星期内，美国就以自己所掌握的情报，曾在不同的场合向以色列发出过多次警告：这是不是阿拉伯人为发动进攻而做的准备？在战争开始的前一天，也就是星期五的中午，以色列总理召开的紧急内阁会议上，包括副总理、财政部长在内的要人都未出席，因为他们都已安然地回到了乡下，准备第二天过节了。结果讨论来讨论去，与会者还是认为爆发战争的可能性极小，过早地进行战争动员没有必要。



以色列被打了个措手不及。“巴列夫防线”失守，东大门被打开。尽管以色列空军作出了较快的反应，但由于埃及和叙利亚引进了前苏联最新式的“萨姆-6”和“萨姆-7”导弹，战争的头几天，以色列空军飞机就损失了一半。

“萨姆-6”是一种灵活的防空武器。它是利用红外线传感器，寻找到飞机喷气发动机所排出气体的热量，把导弹引向飞机。这种导弹主要是打中空和高空的飞机；而“萨姆-7”是便携式防空导弹，专门打低空飞机，其红外检波器可以检测出喷气式发动机的热辐射，并把距离和方位信号送往控制和制导系统。士兵可以把它扛在肩膀上发射，能有效地对付低空飞行。

正当以色列危在旦夕之时，美国的间谍卫星“大鸟”给以色列带来了转机。它居高临下，清楚地拍下了有关苏伊士运河两岸埃及军队部署的照片，并从茫茫太空中送回了这条至关重要的信息——埃及第2军团和第3军团之间有一个10千米宽的空隙。这是一个理想的、反攻的突破口。

以色列军方当即命令沙龙急速带领主力部队，以装甲兵为先导，从埃军的那条空隙中偷渡苏伊士运河，向西岸发动进攻，进而把战火引向埃及军队的所在地，破除埃及国土上对以军作战威胁极大的“萨姆-6”、“萨姆-7”导弹网。

沙龙——以军第54师师长。他喜欢冒险、善用谋略，当时45岁，正处年富力强之龄。他首先集中了在第三次中东战争中缴获埃及的数十量坦克和装甲车，全部喷上埃及的标志。然后，挑选了几百名会讲阿拉伯语的军官和士兵，乔装打扮，组成了一支“埃及”车队。

10月16日，这支化装成埃及人的以色列军队，顺利地通过了埃及人在苏伊士运河上架设的浮桥，插入敌后，仅用一天的时间就破坏了埃军后方导弹阵地和高炮阵地，开辟了飞越西奈半岛的空中走廊。在以空军强有力的支持下，以色列地面部队开始实施犀利的反击。

埃及军队终于顶不住了，逐渐向后撤去……

电子战在第4次中东十月战争中作用是显而易见的。没有电子战的侦察反侦察，欺骗反欺骗，埃及和

叙利亚就不可能成功地突破以色列的“巴列夫防线”；没有电子战的侦察和摧毁，以色列也不可能反败为胜。

## 南大西洋上的电子战

马尔维纳斯群岛(英国称福克兰群岛)，位于南大西洋西侧，距阿根廷大陆最近处 510 千米，距英国本土 13,000 千米，它扼南大西洋和南太平洋交通要冲，是通往南极洲的大门，战略地位非常重要，1831 年以来一直为英国占据。英阿关于该岛的归属问题一直存在争议。

1982 年 4 月 2 日凌晨，阿根廷用武力夺回马岛，成为英阿马岛战争的前奏。1982 年 4 月 3 日，英国内阁作出派遣特混舰队重占马岛的决定。

5 月 4 日，这一天注定要写入阿根廷的历史，写进世界战争史。上午 10 点整，阿军舰载“超级军旗”式飞机腾空而起，直向正以三十节的速度向马岛北部开来的英军“谢菲尔德”号驱逐舰扑去。为了躲避英军雷达，“超级军旗”下降到 40 到 50 米的高

度贴着海面飞行，为了做到完全隐蔽，飞行员干脆关闭了机上雷达，飞机引擎发出巨大的轰鸣声，在机后掀起数米高的海浪，只要稍有闪失，飞行员便会葬身海底。

11时10分，“超级军旗”在距“谢菲尔德”号46千米时，突然爬高到150米，同时打开机上雷达，当屏幕上显现出“谢菲尔德”号的影子时，飞行员狠狠地按下了“飞鱼”导弹的发射按钮，两枚导弹直奔“谢菲尔德”号而去。尽管其中一枚导弹因受电子干扰偏离目标，另一枚却击中了“谢菲尔德”号着水线以上1.8米处的右舷，穿透舰身，炸毁了机械操作、探测和装备中心，舰员伤亡47人，随即舰体开始进水并缓缓下沉，5小时后，舰长不得不下达了弃舰的命令。

血的代价和痛苦的教训让英国人变得清醒了，自从“谢菲尔德”号驱逐舰被击沉后，英国舰队在受到敌方的空中威胁时，便大量施放无源干扰。为了保证不间断地补给偶极子反射体，英国莱普西航空空间公司不分昼夜地工作达一个月之久。

在英阿马岛战争中，电子干扰显示出巨大威力。阿航空兵在未使用电子压制设备的情况下，共出动 167 次，击沉了英军“考文垂号”导弹驱逐舰、“热心”号和“小羊”号护卫舰，损失飞机 117 架。英军使用了电子压制设备后，仅损失飞机 10 余架。此外，为保护水面舰艇免受导弹的袭击，英海军运用了电子压制的三种战术方法，使用“乌鸦座”、“海风扇”以及“坚忍”非制导火箭(其内部装填由镀金属的玻璃纤维和铝箔制作的偶极子反射体)，还有投放偶极子反射体的机械装置，来施放无源干扰。无源干扰在正常气象条件下，可在 6 分钟左右的时间内起作用。因此，英军利用电子干扰，挽救了“竞技神”号航空母舰、“格拉摩根”号导弹驱逐舰，及英国海军特混舰队(包括水面舰艇和潜水艇)的近百艘舰艇。

5 月 25 日 9 点 42 分，英国在抗击 2 架阿军“超级军旗”式战斗机对军舰编队袭击时，利用“变形虫”发射装置施放无源干扰，在不同高度和不同距离上形成 4 块偶极子反射体干扰云。阿军战斗机在 8 千米距离上发现了英军舰编队，在 45 千米处向位于编队内的英军“竞技神”号反潜航母发射了 3

枚“飞鱼”导弹，导弹被舰上雷达发现后，由编队的舰艇发射了大量的偶极子反射体，并由“山猫”直升机施放有源干扰，使导弹自导引头受到压制。这3枚导弹中，一枚偏离航母，并被警戒舰发射的“海狼”防空导弹击毁，另一枚掠过军舰编队时坠毁；但仍有一枚穿出偶极子反射体，击中“大西洋运输”号集装箱船，并将其连同船上的9架直升飞机一起击沉。



6月12日，当阿军使用地面发射架向英军舰队驱逐舰发射4枚“飞鱼”导弹时，英军“格拉摩根”号导弹驱逐舰，使用舰上的“乌鸦座”式发射装置发射干扰，又使3枚“飞鱼”导弹偏离，只有一枚击中了一军舰的尾台，但军舰仍能航行。

另外，英军还通过发射红外线假目标，模拟舰艇热辐射，这些假目标落入水中后，滞留在水表面，能将装有热能自导引头的导弹吸引过来。

在战斗中，英军还对阿军的导弹阵地实施了“硬摧毁”。“火神”轰炸机使用 A G M - 4 5 反雷达导弹，多次成功地袭击了阿军的 T P S - 4 3 F 雷达站。以后，每次攻击时，阿军雷达都被迫关闭。轰炸斯坦利港时，战略轰炸机对阿军担负防空任务的“罗兰”和“山猫”的制导雷达进行了压制和轰炸，大大扼制了其作用的发挥。

在英阿马岛冲突期间，英军还使用了宇宙侦察设备。根据美国侦察卫星提供的情况，1982年5月2日，英军舰艇用鱼雷击沉了阿根廷“贝尔格拉诺将军”号巡洋舰。舰上1042名成员只有400名得救。

在整个战争期间，英国特混舰队尽管遭到阿军海、空部队的顽强抵抗，遭受了较大损失，但正是由于英军的电子设备发挥了重要的作用，保护了许多舰船和飞机免遭打击。而阿军缺乏必要的电子设备，遭

受了严重的损失。这样战争胜负的天平逐渐向英国一方倾斜。

### “死亡线”上的较量

1969年9月1日，在利比亚王国，一位年仅21岁的中尉军官——卡扎菲发动了一场震惊世界的不流血军事政变，建立了阿拉伯利比亚共和国。第二年，执政的卡扎菲废除了前国王与美国签定的军事、经济、技术等9项合作协定，收回了美国在利比亚的空军基地。1979年岁末，为了支持伊朗的反美斗争，2,000多名愤怒的利比亚穆斯林，放火烧了美国驻利比亚办事处。

最使美国人恼怒的是卡扎菲还从前苏联购进大批武器，聘请前苏联专家给自己当顾问，并将原美国在利比亚的军事基地转手给了前苏联。卡扎菲成了美国人的眼中钉、肉中刺。

1986年1月22日，美国情报部门的一份报告送到了里根总统的办公桌上。间谍卫星拍摄的照片表明，利比亚已把从前苏联进口的“萨姆-5”导弹



部署在锡德拉湾沿岸，这些射程达 300 千米的对空导弹，显然对在地中海活动的美国飞机构成了严重威胁。于是，已于 1984 年获得连任的这位美国总统决定：“必须坚决铲除！”

1986 年 1 月 25 日，大概是受了进口的“萨姆-5”导弹的鼓舞，一向好冲动的卡扎菲公开重申，锡德拉湾是利比亚领海不可分割的一部分，距海岸 360 千米的海域是利比亚不可侵犯的领海(国际公认的领海是离海岸 22 千米以内的海域)，并夸下海口，北纬  $32^{\circ}30'$  是不可逾越的死亡线。

卡扎菲的一番话，让美国人的一条“妙计”出笼——以“维护公海航行自由”为借口，故意让美舰船越过“死亡线”，迫使利比亚先开火，再以“自卫”为名，狠狠教训一下卡扎菲。

3 月 23 日，美国一支庞大的舰队驶向锡德拉湾，开始了一场“演习”。第一天，尽管美军多次突入“死亡线”，但卡扎菲却没有什么反应。

第二天，美军采取了进一步的挑衅行动。卡扎菲终于沉不住气了，2 枚“萨姆-5”导弹腾空而起。利比亚防空部队先后向美国飞机发射了 5 枚“萨姆-

5 ”导弹和 1 枚“萨姆- 2 ”导弹，却一无所获。萨姆到底怎么了？

萨姆系列导弹是苏联最主要的防空导弹，在世界上也是比较先进的，包括“萨姆- 2 ”、“萨姆- 3 ”、“萨姆- 4 ”、“萨姆- 5 ”、“萨姆- 6 ”等多种型号。在越南战争中，越方曾用“萨姆- 2 ”导弹击落了不少美国的作战飞机。1983 年 12 月叙利亚曾用“萨姆- 5 ”击落了两架美国舰载飞机，并俘虏了飞行员。这“萨姆”到了利比亚人手里就不灵了呢？

原来，战前美国对利比亚进行了详细的电子侦察。在前几次锡德拉湾举行的海空军事演习中，美国利用侦察卫星、高空侦察机，还有不断在利比亚附近海域上空飞行的 E A - 6 B 等电子战飞机及电子侦察机，探测到了利比亚地对空导弹系统的详细技术、战术情报，掌握了利比亚军事通信设备的技术性能的使用规律。而且美国在这次行动之前，设法搞到了几枚“萨姆- 5 ”导弹，把它的性能摸得一清二楚。他们还向以色列取经，了解以色列在黎巴嫩战场上对付“萨

姆”导弹的办法。美军对症下药，研究出了对付萨姆的有效电子战技术和战术。

在整个战斗过程中，美军凭借先进的电子侦察设备，对利比亚导弹基地的动向了如指掌，甚至知道了卡扎菲向地空导弹基地发出的袭击命令的内容，再加上美国用电子干扰设备发出强有力的电子干扰，使利比亚的对空雷达、导弹制导雷达都成了睁眼瞎。

在长达 6 个小时的时间里，美军始终没有还手。暮色降临后，两架 A - 6 “入侵者”攻击机从“美国”号航空母舰上起飞，直奔一艘正在向美舰队逼进的利比亚“战士”导弹巡逻艇，并向它发射了两枚“鱼叉”导弹。导弹紧贴水面飞向目标，由于美机持续对利比亚舰艇进行了压制性电子干扰，利比亚舰艇毫无察觉，轰轰两声巨响，“战士”被炸得粉碎，艇上官兵无一生还。

当晚 2 3 点 1 5 分，两架 A - 7 “海盗”式攻击机从“美国”号航母上起飞，扑向利比亚的锡德拉地对空导弹基地。每架飞机携有 4 枚“哈姆”反辐射导弹。它代号为 A G M - 8 8 A，是美军最新研制的专门用于攻击敌防空雷达的导弹。导弹头实际上

是一部无源雷达，利用单脉冲扫描捕捉技术捕捉对方雷达波束，顺藤摸瓜，直捣雷达站。在“哈姆”反辐射导弹的打击下，顿时，锡德拉导弹基地一片火海。



25日凌晨1时54分，美军又派出两架A-7攻击机携带“哈姆”反辐射导弹攻击利比亚导弹基地。

有了上次的教训，利比亚基地指挥官接到发现美机袭来的报告后，立即命令雷达关机，但为时已晚。

“哈姆”导弹已经发出，其记忆装置已记下利比亚雷达的位置，并精确地摧毁了目标。在这场时间不长的导弹战中，美国军舰和飞机在卡扎菲规定的“死亡线”内共停留了 75 小时，利比亚向美军舰载飞机发射了 6 枚地对空导弹，但无一命中；美军则以更多的导弹和炸弹予以还击，击沉利比亚巡逻艇 2 艘、击伤 3 艘，并摧毁了利比亚 2 个“萨姆-5”导弹基地，造成利方 150 人死亡。

这场导弹战双方的伤亡结果为何差距如此之大？EA-6B“徘徊者”电子战飞机发挥了至关重要的作用。该机装备的电子作战设备有：AN/ALR-42 雷达告警接收机；AN/ALQ-99D 大功率战术杂波干扰机；AN/ALQ-126 欺骗式干扰机；AN/ALQ-29A 干扰物投放装置；AN/ALQ-92 和 AN/ALQ-142 超短波通信干扰机。这次战斗中，EA-6B 一直在锡德拉湾上空“徘徊”，执行两个任务：一方面及时发现利比亚雷达信号，判断其性质，测定其参数，告示己方飞行员，并施放干扰，发射假目标误导利比亚导弹到安全处爆炸；另一方面，快速测定利比亚导弹基地雷达站发射频率和

变化规律，并通知己方攻击机飞行员，以使用反辐射导弹摧毁该雷达站。

## “黄金峡谷”行动

1986年4月2日，美国泛美航空公司的一架波音727客机由罗马飞往雅典途中，飞机行李舱的一枚定时炸弹爆炸，飞机被炸出一个4平方米的大洞，4名旅客被甩出飞机外，粉身碎骨，9名旅客受重伤。死者都是美国人。幸亏驾驶员临危不惧，沉着地驾驶飞机紧急着陆成功，才避免了一起更大的灾难。3天后，正值周末。西柏林美国官兵经常出入的一个舞厅发生爆炸，2人被炸死，其中1个是美国人；155人被炸伤，其中44个是美国人。

尽管卡扎菲声明此事与利比亚无关，而美国人则认定他是“做贼心虚”。按美国人的说法，他们的中央情报局截获的电子情报表明，一个时期以来的恐怖活动都与利比亚有关，利比亚是恐怖分子的大本营。

面对接二连三针对美国的恐怖事件，当时美国五角大楼的主人、国防部长温伯格怒不可遏，声称“以

武力遏制恐怖活动”已经是“制止恐怖活动的唯一选择”。

4月9日，美国参谋长联席会议主席克劳上将将一份袭击利比亚的详细作战计划交给了总统里根。由于夜袭利比亚就像传说中的古代西班牙人在深山峡谷中寻找一座黄金城一样，是一桩冒险的军事行动，所以被称之为“黄金峡谷”行动。

14日19时36分，“黄金峡谷行动”开始。

24架F-111战斗轰炸机从英国的拉肯布思空军基地起飞；与此同时，5架EF-111A电子干扰机也从英国的另一基地飞上了夜空。由于法国和西班牙不愿提供军用基地，美国只好从“老朋友”英国这里出发。

在以上机群长途奔袭的同时，美军地中海第六舰队也在悄悄行动。15日0时，6架A-6攻击机和6架A-7攻击机从“美国”号航空母舰上起飞，8架A-6攻击机和6架F/A-18战斗机从“珊瑚海”号航空母舰上升空。2架E-2“鹰眼”预警机和EA-6B“徘徊者”电子战飞机早已

在空中等候。凌晨 1 时，舰载飞机与长途奔袭而来的机群会合。

15 日凌晨 2 时，随着一声令下，美军 F - 111 飞机和舰载攻击机全部低空高速冲向的黎波里和班加西的 5 个预定目标，倾泄了 150 吨激光制导炸弹，射出了 48 枚“百舌鸟”和“哈姆”反辐射导弹。

在这次行动中，美军通过电子干扰机对利比亚雷达进行干扰、用高速反雷达导弹对敌雷达进行破坏，使敌防空雷达系统完全丧失效用，米格飞机不能起飞，导弹不能发射。美军击中利比亚米格-23 飞机库，摧毁 5 到 12 架米格战斗机、3 到 5 架伊尔-79 运输机；5 个选定目标全部被摧毁。利比亚死亡 37 人，伤 93 人。死亡的人中有卡扎菲 1 岁半的养女；伤者中有他的两个儿子。尽管利比亚的导弹及高炮也对空进行了盲目的射击，但“瞎猫”只撞上了唯一的一只“老鼠”——有一架 F - 111 被击落。

这场战争，掩护 F - 111 战斗轰炸机的不是通常的战斗机，而是 EF - 111A 电子战飞机。它是当时美国空军，也是世界上最新、最先进的电子战飞机。它装有两台发动机，水平飞行时，最大速度为 2



，272 千米/小时；不需空中加油，可以连续飞行4小时；它装有地形跟踪雷达和攻击雷达，因此它能够伴随攻击机进行低空突袭。正是由于EF-111A具有非凡的本领，才一路伴随战斗机远征5,000多千米来到利比亚。

EF-111A是当时世界上唯一昼夜都能执行突防护航、近距离支援和远距支援三种干扰掩护任务的电子战飞机。远距离干扰支援，这是一种与攻击机队分开行动，而从远距离对敌方雷达或战斗机实施干扰的作战任务。EF-111A在高空，一方面进行机动跟踪，另一方面实施干扰，由于在距离前线上空大约100千米的空域飞行，因此与以前的电子战飞机相比，它是最安全的。近距离干扰支援，是在攻击机编队实施攻击任务的时候，在距前线最近的上空对敌防空导弹及雷达实施干扰，用来掩护攻击机编队的一种电子战方式。与远距离支援干扰相比，近距离干扰支援的危险性比较大，但干扰效果却要更好一些。突防护航支援干扰，是伴随攻击机编队而担任电子干扰掩护的任务，也是EF-111A作用发挥最大的时候。当进行突防护航时，它在整个编队的最前面，对

敌方的搜索雷达及防空导弹的跟踪雷达实施干扰，以支援攻击机编队。由于此时 E F - 1 1 1 A 首当其冲，直接面对敌方的导弹和飞机的攻击，此时，它是最危险的。

美军这次突袭利比亚途中，E F - 1 1 1 A 一直伴随在机群的左右，机上先进的电子干扰系统一刻不停地工作，施放出大量电子干扰波，使机群在地面雷达上看起来就像是空中的一片积雨云；美军一路无线电静默，让沿途多个国家的地面雷达都未作出任何反应，保证了战争的突然性。

机群飞临利比亚上空，在发动攻击之前，E F - 1 1 1 A 被调到最前面，对利比亚进行了压制性电磁干扰，使利比亚电子系统陷入瘫痪；雷达全部成了“睁眼瞎”，屏幕上布满了雪花点；无线电通信被切断，耳机里只有嘈杂的电流声。当炸弹已落到自己的头上时，利比亚人尚未弄清是怎么回事。

正是由于成功地运用了电子战战术，美军才创造了“黄金峡谷”的经典战役。

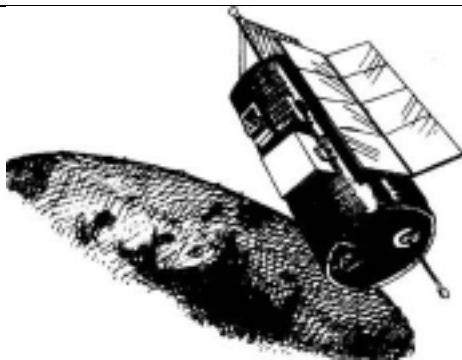
## 海湾战争中的“白雪”行动

1990年8月2日，当地时间凌晨2时，伊拉克突然向科威特发动进攻，仅12小时，伊军就基本控制了科威特全境。伊拉克的侵略行动，引发了海湾战争。

海湾战争打出了高科技战的新水平，电子战在这场战争中更是功不可没。多国部队在这场战争一开始，就夺取了电磁优势即制电磁权。

早在1990年底，以美国为首的多国部队，为了顺利打垮伊拉克，在调兵遣将的同时，就制定了一个代号“白雪”的电子战行动计划，详细拟定了实施电子突击的作战过程。

按照这一计划，多国部队在各种飞机上都装有自卫电子战系统，并采用了专用电子战飞机进行电子战支援，至少投入了107架专用电子战飞机，致使实战中伊方通信中断、雷达迷盲或被摧毁。



早在海湾战争爆发前 5 个月，美国就开始启用 70 多颗军用卫星，其中有 20 多颗部署在高、中、低轨道上的侦察卫星，形成了全方位、多途径、昼夜不停地对伊军的重要军事设施、雷达、通信、导航和导弹系统实施不间断的电子侦察，将所有获得的有威胁的电磁信号输入作战飞机的电子战数据库，为多国部队雷达告警、电子干扰和发射反雷达导弹提供了依据。

在高层，多国部队通过部署在地球同步轨道上的两颗电子情报卫星，特别是最先进的“H K —1 2”型卫星，能全天候提供地面 10 厘米大小物体的图像，并装备了红外传感器，可 24 小时日夜监视海湾地区的电磁活动。

同时，多国部队利用在赤道上空的两颗情报卫星与地面情报截获系统相配合，并在开战前又秘密发射了多种窃听装置，监听伊拉克从导弹发射指令到伊军的步话机谈话的内容，以及坦克之间的无线电通话和其它轻便型无线电通信设备的通信联络信号。

在中层，多国部队派出侦察机进行电子侦察，每天还至少出动 5 架 R C - 1 3 5 电子侦察机用于截获电子情报。在战争打响前夕，至少先派出两架以上 E - 3 A 预警机升空侦察，并与雷达和侦察卫星、战斗机部队指挥系统之间进行多角联系。

此外，多国部队的各种专用电子战飞机都可以利用机载电子设备对 1 0 0 —1 5 0 千米纵深处进行战术电子侦察。

在底层，利用设在阿曼、塞浦路斯和意大利圣维托的地面站进行监听和侦察。通过这些电子侦察手段，把侦察到的电磁信号及时输入美国情报中心，经电子计算机处理后，为开战后的美国隐形轰炸机、巡航导弹和激光制导炸弹预选捕捉和打击目标提供了重要情报信息，致使伊军一开始就处于被动挨打的地位。

1 月 17 日，大规模空袭前 5 小时，多国部队按“白雪”计划，用地面电磁干扰设备对伊军的指挥、控制和通信系统进行了强烈的电磁干扰。

在空中预警机和空中加油机出动后，又出动大批 E A - 6 B、E F - 1 1 A 和 E C - 1 3 0 H 电子战飞机，分别在离目标区 1 6 0 千米、4 8 千米和 1 3 0 千米的空域对伊军防空雷达、通信系统进行压制性大功率干扰，为空袭飞机的突防和攻击提供远、中距支援干扰或随队掩护干扰，使伊军处于雷达迷盲、通信中断、制导失灵的被动挨打困境。

除了以上“软杀伤”外，在轰炸正式开始前 1 0 分钟，多国部队出动了大批 F - 4 G “野鼬鼠”反雷达战斗机，发射了“哈姆”反雷达导弹摧毁伊军正在工作的雷达或迫使其关机，使雷达不能正常发挥其作用。

就这样，多国部队通过“软硬兼施”的杀伤手段夺取了整个战场的制电磁权，为下一步大打出手创造了条件。

在空袭过程中，多国部队继续对伊拉克方面实施不间断的电子情报侦察，一旦发现新的电磁威胁系统

，便立即对其加以干扰或摧毁，丝毫不给其生存的空间和余地。

多国部队在最初 24 小时内所出动的近 2,000 架次飞机中，大部分是电子战飞机，足以说明在第一阶段空袭中电子战所占的分量。

除了实施无源干扰和有源射频干扰外，多国部队还广泛采用了红外线干扰曳光弹和有源红外干扰机等光电干扰措施，以干扰伊方的红外制导导弹和探测器。

正是形形色色的电子战装备使得军事实力并不太弱的伊军变成得又聋又哑又盲。“白雪”计划的顺利实施，使得伊军在开战之前就注定了必然失败的命运。

另外，海湾战争中 C<sup>3</sup>I 系统更是功不可没。

海湾战争中，以美国为首的多国部队，投入的总兵力达 50 万人，共有包括飞机、坦克、装甲车、军舰、防空导弹发射架等在内的各种独立机动作战单位数万个。战区指挥官必须从时间、空间、目标、进入方向等方面进行统一协调，否则，不仅发挥不了整体力量，反而会误伤自己人。在协调这场大物质流、

大信息流的作战行动中，多国部队充分发挥了 C<sup>3</sup>I 系统的巨大威力。

在战略一级，美国本土和海湾战场之间通过全球军事指挥通信系统和国防部通信网保持着不间断的联系。各种信息通过卫星传送到美国本土的指挥控制中心，经过计算机处理，又迅速反馈到战场指挥部，整个程序只需几分钟就可以完成。美国的全球军事指挥控制系统由 40 多个指挥中心、10 个测控预警系统和 60 多个通信系统组成。其国防部通信系统主要包括自动电话网、国防交换网、自动数字网、国防数据网和国防卫星通信系统等，拥有微波、卫星、短波和有线等综合通信手段，线路遍及五大洲 75 个国家和地区。海湾战争中，美军用于通信的主要是联合战术信息分发系统，它保密性好，抗干扰能力强。这一系统的终端被装备在飞机、坦克、装甲车上，连结着每一个战术作战单位，形成一个四通八达的战术指挥通信网。甚至美国总统可以在本国与前线的任何一个士兵直接通话。先进的 C<sup>3</sup>I 系统，使“运筹于帷幄之中，决胜于千里之外”成为现实。



## 电子战中的“非对称作战”

所谓“非对称作战”，就是在力量对比悬殊的状态下，交战双方之间的较量。发生在1999年的科索沃战争，就是一场典型的“非对称作战”。北约一方是拥有高技术武器装备，由十多个军事强国组成的武装集团，而南联盟一方则是孤军奋战，且武器装备至少落后一至两代，数量更是相差悬殊。而这种悬殊，体现最明显的无疑是电子战领域。

战争爆发后，美军及北约注意综合运用电子战优势，以精确打击为作战样式，始终掌握着战争的主动权，同南联盟进行着“我打得着你、你打不着我”的非对称较量。美军及北约运用各种手段，使战场上的一切情况都在自己的“视野”之中，对北约一方面透明；而使南斯拉夫军队变成“瞎子”和“聋子”。为了取得制电磁权，北约布置了40多架性能先进的电子战飞机，高空侦察机和空中预警机，其中包括现在世界上最先进的EA-6B“徘徊者”、F-4G“野融鼠”和EC-130H电子战飞机。EA-6B“徘徊者”电子战飞机主要用来干扰地面各种警

戒、火控和引导雷达，干扰频率范围为 6 4 兆赫至 1 . 8 万兆赫，可对数万平方千米内的电子目标实施有效干扰；F - 4 G “野鼬鼠”电子战飞机可探测、识别和定位脉冲雷达与连续波雷达，并用所携带的 A G M - 8 8 反辐射导弹或“百舌鸟”导弹进行干扰压制与摧毁，它是对付南联盟“萨姆- 6 ”地空导弹系统的有效武器之一；E C - 1 3 0 H 电子战飞机是专门用来对抗自动化指挥系统的大功率电子干扰飞机，干扰频率范围为 2 0 至 1 , 0 0 0 兆赫。此外，在作战中，北约军队还使用了一次性通信干扰机，该机由飞机或火炮投掷，落地后自动生出天线释放干扰，完成干扰使命后定时自毁；北约还释放无人机作电子诱饵，引诱南军雷达开机，以准确测定其配置和准确性能，为成功实施电子干扰和反雷达导弹攻击创造了条件。在对南联盟电子信息进行“软杀伤”的同进，北约还使用信息化兵器实施“硬打击”。其中主要是使用“哈姆”反辐射导弹袭击雷达系统，首次动用了 B - 2 隐形轰炸机轰炸南联盟经过加固的指挥中心等硬目标。在太空中，北约有 5 0 余颗卫星组成的侦察网，对南联盟进行 2 4 小时不间断侦察，为自己的部队提供

及时准确的战场态势情报；还有由 24 颗导航和定位卫星组成的全球卫星定位系统，为美军武器装备提供全天候、高精度的位置、速度和时间数据。以美国为首的北约通过以上电子战手段，完全掌握了制电磁权，使南军处于被动挨打的非对称境地。

远程精确火力打击是美军最大的优势，也是美军非对称作战的主要样式。在此次科索沃战争中，北约充分发挥巡航导弹、精确制导炸弹、集束炸弹等精确制导武器的优势，对南联盟军事、政治和经济等目标，实施非接触性远程精确火力打击，使南军无法进行有效还击。海湾战争中，美军以“战斧”巡航导弹为代表的远程精确制导武器，初试锋芒，但其使用比例不到 10%；1998 年 12 月“沙漠之狐”空袭伊拉克行动中的使用比例 70%；而空袭南联盟行动中使用的精确制导武器则已达到 90% 以上，特别是全球定位系统技术的使用，使精确制导武器具有更高的命中精度和更远的打击距离，为美军实施非对称远程精确火力打击提供了可靠的作战技术手段。其中最具有代表性的精确制导武器是巡航导弹和精确制导炸弹。据报道，北约空袭 70 多天向南联盟发射了 2

，000多枚巡航导弹，其中海基“战斧”巡航导弹是由亚得里亚海上的军舰发射的，其距离最远为1400千米，最近也有700千米。其空射巡航导弹主要由B-52轰炸机在距离目标500千米以外发射，依靠卫星制导，攻击目标。其他如F-117A、F-16和F-15等战斗机一般均在南军防空火力区之外发射空地导弹。特别值得注意的是，美军在此次对南空中打击中，还使用了新型卫星精确制导炸弹。该型炸弹由B-2隐形战略轰炸机在万米以上高空一次投放16枚，然后返回美国本土基地，16枚炸弹在全球定位系统的引导下，分别攻击16个目标。此外，为了给南联盟军民造成巨大心理恐慌与精神压力，美军于5月3日首次使用了石墨炸弹。该炸弹由激光制导，内装雷达测高仪，使其在数百米高空爆炸，形成大面积石墨粉团，飘落在发电和供电设备上，造成短路并破坏输变电设备。美军一次炸弹袭击就造成贝尔格莱德市70%的范围断电。美军这种非对称作战样式，大大降低了人员和装备的损失。北约空袭南联盟历时78天，尽管南军殊死抵抗，竭力发挥己方作战优势，也击落一架F-117隐

形战斗机、数十架其它飞机和几十枚巡航导弹，但由于没有制衡美国及北约的电子作战技术手段，始终无法摆脱被动挨打的局面。

美国及北约军队没有对南发动地面进攻，其原因除了政治和外交等方面的制约因素外，军事上主要是美军就是要以非对称作战征服南联盟。越南战争以来，地面作战一直是美军惟恐避之不及的恶梦。美国军人在越南战场上的惨重伤亡，使美国国内的反战浪潮一浪高过一浪，美国当局最后不得不从越南撤军；海湾战争是在空中打击 38 天，伊拉克作战力量几乎全部瘫痪的情况下，才发起地面进攻的。美军在索马里的地面行动中仅有 18 人的伤亡，便在国内一派反对声中撤军。追求战争低死亡率、最好是零死亡率是美国及西方的价值观所决定的。地面作战死亡概率最大，这使得美军必然竭力避免地面作战。南斯拉夫人民具有英勇不屈、反抗外来侵略的民族精神，有善于打游击战的传统。南联盟境内多是高山丛林，便于地面游击战。美军只有避免地面战，才能实现其非对称作战的意图。

其实，非对称作战对我们来说并不是什么新鲜东西，中国人提出的以己之长，攻敌之短，可以说是最早意义上的非对称作战。

### 在“非对称作战”的另一端

1999年3月27日，美军一架F-117A隐形战斗机被南联盟军队击落。这是不可一世的F-117A自问世以来第一次被击落，从而结束了F-117A不可战胜的神话。南联盟军队在以劣抗强的作战中，取得了击落几十架飞机和几十枚导弹的战绩。

在科索沃战争中，尽管南联盟军事力量处于绝对的劣势，但英勇的南联盟军队并没有坐以待毙。他们根据国际、国内形势的发展变化，积极进行了战争准备。特别是针对北约高技术军队实施长时间、大规模空袭作战的特点，进行了反空袭作战准备和电子战领域的研究，并在实战中取得了令人瞩目的效果。

近年来，南联盟军队积极研究了高技术条件下反空袭作战的特点，尤其针对多国部队多次袭击伊拉

克、波黑战争中北约轰炸塞族的作战特点，采取军队内部研究与学术界交流等形式，进行了认真、细致、全面的研究。基本上掌握了高技术军队实施空袭作战的强项与弱点，研究了隐蔽防护和打飞机、打巡航导弹的战术，具备了一定的对抗敌空袭的能力。如南联盟军队在研究中发现，虽然北约的侦察手段很先进，可以利用侦察卫星、预警飞机、高空侦察机和地面传感设备，实施大范围的侦察监视，但并不能完全掌握战场情况，尤其是对经过伪装的地面目标、假目标和活动目标的侦察识别能力较弱。因此，南军采取了加强地面目标伪装、设置假目标、适时机动重要目标等针对性措施。

南联盟军队根据现代战争中空袭、反空袭作战地位作用突出的特点，重点加强防空力量建设。其空军除航空兵外，拥有 8 个地空导弹团、15 个防空炮兵旅，陆军拥有 7 个防空团和 1 个地空导弹旅。在注重增加防空部队的同时，还加强了反空袭武器装备的建设。南联盟军队引进了前苏联多种型号的防空导弹，包括“萨姆-2”、“萨姆-3”、“萨姆-6”等导弹千余枚，发射装置百余部。对原有装备进行了

改造，经过改进的米格 21 型战斗机，雷达和火控系统的性能相当于米格-29。根据高炮和便携式防空导弹造价低，隐蔽性、机动性好，打击低空目标歼毁率高，抗干扰能力强的特点，装备了近 2,000 门各种口径高炮。

针对北约空袭的特点和规律，南联盟军队广泛采取了沿航线设伏、突然打击等战法，收到较好效果。如针对北约有隐形飞机、电子战飞机、反雷达飞机和性能良好的雷达、火控系统等情况，采取了适当保持无线电静默，远程、近程雷达逐段接力开机，地空部队密切协同，防空导弹、高炮突然发射(开火)等战法；针对巡航导弹巡航高度低、飞行速度慢、外壳薄的弱点，在分析判断航路的基础上，采取从远距离开始，由远而近设置地面侦察、观察哨，防空兵器多层、多道设伏打击的战法。

在防空力量使用上，南联盟军队既重视防空导弹的使用，又注重发挥高射火炮的作用，采取防空导弹与高射火炮的混合配置的方法，既有效弥补了不同兵器在射程、射高上的不足，又增强了防空力量，在敌强烈电子干扰下的防空作战能力得到提高，针对精



确制导武器对目标信息依赖大，打击活动目标精度下降等弱点，适时机动防空兵器，变换阵地位置。这一措施降低了防空力量的损失，保持了防空作战能力，也保证了适当的时间、地点对反空袭力量的需求。北约空袭持续相当长的时间以后，美参谋长联席会议主席谢尔顿称南联盟“完整的多层次的防空系统，使天空充满着危险”。

南联盟军队积极开展战场电子战，使北约未能取得预想的战场制电磁权。北约军方在评价南联盟军队战场电子战能力时认为，南联盟军队的指挥、控制、通信与电子系统的完善程度，比美国面对的伊拉克、北约面对的波黑都要高得多。南联盟军队有效的战场电子战，迫使北约不断加强电子战力量，在最初就强调集中电子战能力绝对优势的情况下，进入空袭第二阶段，又从伊拉克战场调来了一个雷达电子干扰中队，并增派了3架“捕食者”和8架“猎人”无人侦察机。

北约空袭发动前，南联盟加强了对科索沃反叛力量的清剿；空袭开始后，对各国新闻记者的采访加强了限制，并宣布驱逐北约参战国的记者；战争期间，

组织群众不间断地进行昼夜巡查，清除北约谍报人员；每次空袭过后，严密封锁空袭现场，限制记者进行实地采访。以上举措控制了重要情报的知情范围，增强了保密性，使得北约侦察空袭目标情报和进行空袭效果评估变得非常困难。值得一提的是，南联盟在反空袭期间，还成功破获了一个北约间谍网。在注意反情报泄露的同时，南联盟军队还通过秘密渗透等多种手段，积极展开情报侦察。北约人士称，空袭效果不理想的一个重要原因，可能是南联盟军队及时得到了北约实施空袭的情报。



自从开战以来，以南通社为组织中心，专门开设了以“科索沃危机”为专题的电脑网址，宣传南联盟进行的反侵略战争，发动了电脑专家以互联网为媒体，向北约发动计算机网络战。1999年3月29日，美国白宫网站因受“黑客”攻击而无法工作，北约国家轰炸行动中最依赖的英国与西班牙气象局网站损失惨重；3月31日，北约的互联网址及电子邮件系统连续遭到电脑“黑客”的网上攻击，部分计算机系统受重创；4月4日，北约军队网络通信一度陷入瘫痪。在这场无声的战争中，美国及其他北约成员国未能占据上风。

### 车臣上空，一“足”遮天

2000年3月18日，俄罗斯代总统普京向世界宣布：俄军在车臣的大规模军事行动即将结束。俄罗斯为维护国家统一、反对民族分裂、打击恐怖主义而进行的近8个月的第二次车臣战争，终于实现了俄军的全面胜利。

尽管车臣战争在高新武器的使用方面不及海湾战争和科索沃战争，但与第一次车臣战争(1994—1996)相比，俄军这次明显加大了高新技术的使用，为最终取得车臣战争的胜利，奠定了强大的物质基础。

格罗兹尼郊外的山区，冰天雪地，炮火连天，只见4架飞机呼啸而过，车臣非法武装的据点顿时被火光吞没。这是被北约称为“蛙足”的苏-25强击机正在实施对地火力突击。在这次俄军清剿车臣叛军的作战中，苏-25强击机家族身手不凡，以强大的攻击力、极低的战斗损失，给世人留下了深刻的印象。“蛙足”逞强车臣上空，一“足”遮天，皆因俄军能够从阿富汗战争中汲取有益的经验，20年来，持之以恒地依据正确的战争构想，选择最有效的技术对苏-25强击机进行了全面的升级改造，先后推出了苏-25T、苏-25TM等一系列新的机型，使老装备战斗力大为增强。

为了全面压制敌人的对空火力，新苏-25在设计时也别具匠心。苏-25装了反辐射导弹，这在世界各国众多的强击机中可谓独树一帜，突入敌军导

弹和高炮的有限射程之后，可用反辐射导弹摧毁火控雷达，使高炮、导弹无法准确攻击。根据过去的经验，防空部队为了对付反辐射雷达，往往采用将雷达突然关机的办法，而苏-25也使出了新招：它装备了一种名为“旋风”的导弹。这种导弹不仅可以捕捉雷达波并随波而去摧毁雷达，还可以在电视设备和无线电控制系统的配合下，有效攻击那些突然关机的雷达阵地。这种导弹获得“火力长上了眼睛”的美誉。极强的“电磁硬杀伤”使“蛙足”攻击时技高一筹。这次车臣战争中，苏-25对非法武装分子设在车臣境内的许多火力点进行了电磁软杀伤和精确火力打击，战果辉煌。

强击机在作战中的战损率是一项重要的评估原则。美军在越战的战损率是2%；但后来的几次中东战争，强击机的战损率有所上升。俄罗斯专家通过研究和实验发现，在前沿地带，敌方构筑了严密的防空火网，此时若是释放干扰敌人的预警系统，往往会引起敌军的警惕，使突防作战产生了许多不确定性。于是，专家们确定了一个新原则，就是在敌人的防空地域实施广泛的机动，绕过敌人的火力杀伤。但是把理

论变成现实并非是一件容易的事。中东战争中，埃军的 4 架米格- 1 7 试图超低空突袭以色列的“霍克”防空导弹阵地时，就发生了撞地事故。针对此类问题，俄为新苏- 2 5 设计了性能优良的自动驾驶仪，飞行员可以利用自动驾驶仪作超低空飞行，在绕过敌军防空阵地时，不必担心发生米格- 1 7 那样的事故。苏- 2 5 的自动驾驶仪可以将各种事故告警信号转为控制信号，传递到相关设备进行处理，自动调整飞机以避免事故。特别是在夜间进行突防作战时，自动驾驶仪是飞行员节省体力，减小紧张度的最佳选择。同时苏- 2 5 上还装备了先进的测向雷达，以确定飞机在敌人的雷达探测、导弹追踪范围中的准确位置，及时为飞机提供最合理的飞行高度，最大限度地避免被敌军攻击。此次车臣战争中，苏- 2 5 强击机利用先进的雷达，多次从车臣非法武装意想不到的时间、地点突入车臣腹地进行全天候轰炸，来无踪去无影，令叛军防不胜防。

在突防作战的最后阶段，飞机难免要进入敌军的火力杀伤圈。为此，新苏- 2 5 装备了新式有源干扰吊舱。这种干扰吊舱可以对付连续波、脉冲和单脉冲

制式的雷达。干扰吊舱开机后，可同时释放欺骗式和杂波式干扰，全面压制敌方防空火力的制导系统。除了“电磁防护”外，在对付敌军“热寻的”对空导弹方面，苏-25强击机也有长足的进步。在进入战区后，苏-25为了保证机载非制导武器的精度，必须降低飞行的高度，这就为敌方的红外制导导弹提供了攻击时机。为此，苏-25采用先进的红外抑制技术，使飞机表面和发动机的热辐射大大降低，比早期型号降低了三分之二。同时，新型苏-25利用机械光电设备加强了利用热辐射形成假目标的功能，利用铯材料制成的强放电管将假目标信号向外辐射，使敌军发射的导弹在受到假目标的引诱后偏离跟踪飞机的轨迹。车臣非法武装虽然拥有红外制导的“毒刺”、“星烁”等先进的单兵防空导弹，确未能击落一架苏-25系列强击机。

这次车臣战争中，“蛙足”在电子方面的成功，使它在车臣上空“一‘足’遮天”，成为战场上的一颗明星。

俄军挥师车臣，双方在电子战的另一个领域——因特网上也进行着激烈的较量。车臣非法武装为获取

某些势力的支持，将车臣问题国际化，使用英文在国际互联网大肆列举俄军的“暴行”，声称俄罗斯践踏车臣民族。俄军针锋相对与之进行斗争。对西方进行了适时、有力的反击，最大限度地争取国际社会的理解和支持；对国内有力的宣传，极大地调动了全体军民的战斗意志；对车臣实施的全方位、大强度的心理战，有效地震慑了车臣非法武装的抵抗心理。这一切都为俄军最终达成战略目标、取得剿匪全面胜利，发挥了重要的作用。



### 三、纵横驰骋——分析电子战

#### 独特的风景线

提起空战、陆战、海战、导弹战，人们都会想到在电影、电视里所看到的飞机穿云破雾、坦克铁甲隆隆、大炮放声怒吼、军舰劈波斩浪、导弹直刺云天的壮观场面。然而对电子战是什么样子，却总感到不好捉摸。通过前面我们所介绍的德国最大的战列舰“俾斯麦”号沉没海底、日本联合舰队司令长官山本五十六毙命空中、美国神秘的高空侦察机 U - 2 被击落、海湾战争中伊拉克手脚被缚等一系列战例，不难察觉，在这些令人震惊的事件背后，有着一只无形的巨手在操纵着。它以看不见、摸不着的电磁波为渠道，通过电子信息，敌对双方互相破坏作战部署，控制、指挥着人和各种武器对抗，并逐步发展成为现代战场上形形色色的电子对抗样式，也就是电子战。在这场交战不见面、杀人于无形的斗争中，更多的只是窃听与反窃听、侦察与反侦察、干扰与反干扰、摧毁与反摧

毁等真假难辨、虚实参杂的“软”杀伤和“硬”打击，软硬兼施——电子战所发挥的“力量倍增器”作用，令人大开眼界。特别是海湾战争以来的现代高技术条件下局部战争中，不但有无线电通信对抗、雷达对抗，还有光电对抗；不但有陆海空电子对抗，还有外层空间的电子对抗，以及红外线、激光、反卫星武器等。

在无数战例面前，人们已经认识到：在现代高技术局部战争中，胜利必将属于最善于控制和运用电磁频谱的一方。在面对新军事革命的挑战中，人们更加迫切地需要了解电子战、深入认识电子战，以揭示电子信息、数字化时代战争的本质和规律。为此，在下面的内容中，我们着重从认识与分析的角度向大家介绍有关电子战的一些基本知识。

### 风雨历程电子战

20世纪初，电子对抗萌芽生长于战争舞台。在不到100年的时间里，电子战以其惊人的速度和进程，形成一种全新的作战样式，并构成现代战争中

一道独特的风景。贝卡谷地之战、美利锡德拉湾冲突、海湾战争等都表明了夺取制电磁权的极端重要性。一位外国军事评论家指出：“具有完善的电子战能力的国家，在其领土周围筑起一道强大、灵活、高效的电磁屏障，这是一道无论哪个国家都不能贸然入侵的肉眼看不见的万里长城。”

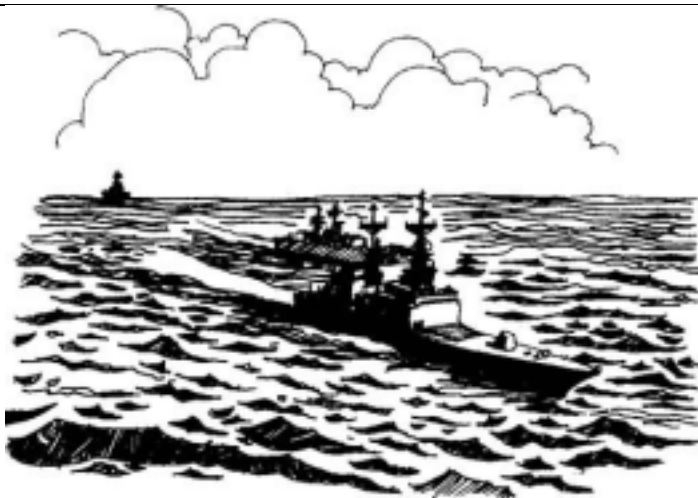
电子对抗(E C M —E l e c t r o n i c C o u n t e r M e a s u r e s )，是指利用电磁能和定向能以控制电磁频谱或用电磁频谱攻击敌方的军事行动。它利用电磁波探测、识别敌方使用的电磁频谱和电子设备，并根据探测、识别的结果，采取各种电子措施和非电子措施(如施放有源干扰、无源干扰和发射反辐射导弹等)干扰、阻碍敌方电子设备的正常工作，甚至破坏其电子设备，从而保证己方的电子设备正常应用电磁频谱，发挥最佳效能。美国及北约国家称这种作战手段或作战方式为“电子战”，俄罗斯称其为“电子斗争”。电子战主要包括电子侦察与反侦察、电子干扰与反干扰、电子摧毁与反摧毁、隐身与反隐身、制导与反制导等，所涉及的对抗领域有雷

达对抗、通信对抗、光电对抗、水声对抗等。电子战被认为是继陆、海、空战之后的第四维战场。

从一定意义上说，电子对抗的实质就是敌对双方为争夺电磁频谱的控制权(即制电磁权)所展开的斗争。制电磁权，犹如制空权、制海权，是指在一定的时间和空间范围内对电磁频谱的控制权。夺取了制电磁权就意味着己方能够自由使用电磁频谱，不受对方电磁威胁和限制；同时剥夺了对方使用电磁频谱的自由权。制电磁权有其时空性。在总体上处于相对劣势的一方，并不是一筹莫展，若科学指挥、合理集中力量，能在某一时域或地域内，夺取局部制电磁权。

电子战是随着无线电通信的出现而产生的，第一次世界大战中的无线电通信对抗构成了早期的电子战。

。



1914年8月，英国对德国宣战不久，当时在地中海游弋的英国“格洛斯特”号巡洋舰发现了两艘德国巡洋舰“盖本”号和“布莱斯特”号，随即用无线电向海军部报告，企图调集力量予以消灭。但德国巡洋舰侦听到“格洛斯特”号和海军部之间的无线电通信联络，便施放无线电噪声干扰，破坏其通信联络，以避免英舰的监视和跟踪，安全撤到土耳其的达达尼尔水域，补充煤炭和给养，然后炮击了俄国的军事要塞塞瓦斯托波尔。

这是有史以来，电磁波第一次成功地用于干扰敌人的通信。从电子对抗的观点看，是首次用电子进攻

(干扰) 代替枪炮防御, 电子斗争初露锋芒。可以这样说, 这次通信干扰是电子对抗的真正开始。至此, 以无线电通信对抗的侦察、测向和干扰为主要内容的早期电子对抗已全面形成。

电子对抗形成到今, 其发展大体经过以下三个阶段:

第一阶段, 第二次世界大战爆发前夕和二战期间。此时, 雷达和飞机已广泛运用于实战, 电子对抗也从通信对抗发展到了导航对抗和雷达对抗, 制导对抗初见端倪。各国共研制了数十种电子侦察、积极干扰和消极干扰设备, 奠定了电子对抗发展的基础。

通信对抗方面。大战期间, 英国为中断德国飞机与地面指挥所的无线电通信联络, 德国为保持通信顺畅, 双方展开了激烈的通信对抗, 尽管德军采用了增加发射机功率、拓宽通信频带、改变信号传递方式等抗干扰措施, 但始终未能摆脱英军的干扰。

导航对抗方面。1930年, 德国的络伦斯公司研制成一种无线电导航系统, 用来帮助飞机在夜间和能见度很差的情况下安全着陆。3年后, 德国的科学家汉斯·诺兰德将络伦斯系统用于提高飞机投弹

的准确性，不久获得成功。这样，电子对抗便从通信对抗发展到导航对抗。1942年夏，英国电信研究院研制成功了欧巴导航系统，该系统在技术上有很大突破，接近雷达导航系统。1943年3月5日英国轰炸机依靠该系统，成功地夜袭了德国克虏伯军工厂，工厂损失惨重，使希特勒大为震惊。

雷达对抗方面。第二次世界大战中，英国饱受空袭之苦，伦敦日夜遭到德国飞艇和飞机的轰炸。当时对付空袭有两种方法：一是人员躲进防空洞，二是用战斗机和高炮打敌人的飞艇和飞机。但都需要提前发出空袭警报，才能有时间做好准备。为此，英国非常重视用新兴的电子技术来对付同样是新兴的飞机的威胁。他们认为，运用电磁波反射的原理，有可能提早发现远方的飞行物。于是加紧研究雷达技术，终于在1935年6月，由科学家沃森—瓦特研制出了工作在11兆赫兹，探测飞机距离达17英里的第一部探测飞机的实用雷达，1936年3月，其改进型能发现75英里处的飞机。雷达用于防空作战后，立即显露锋芒。于是以无线电通信对抗为主的电子对抗发展到了雷达对抗，大大地拓宽了电子对抗的领域，使

电子对抗在整个战争中的地位和作用更加重要了。它远远胜过几千架飞机和几百艘军舰。大战中的雷达对抗主要表现在对警戒雷达和机载雷达的侦察与压制。

制导对抗方面。第二次世界大战后期，出现了制导武器，随之诞生了制导对抗。1944年2月，盟军缴获了落在利比亚沿海没有爆炸的一枚纳粹德国空军的亨舍尔 293 制导炸弹，从弹头上拆下一台完整的制导接收机，从而搞清了它的工作方法。与现代的制导系统相比，它还处于原始阶段。美国又研制成了 M A S 大功率专用干扰机。它的干扰功率 250 瓦，机内装有接收机，能在 41 至 51 兆赫频段内进行瞄准干扰，并针对制导系统使用的音频采用调制干扰，还用假指令使制导炸弹偏离方向，大大提高了干扰效果。首批生产 49 部，从此，制导炸弹失去了作用。但德国人为了避免盟国的制导干扰，研制了 V - 1、V - 2 地地大型导弹，分别采用程序和惯性制导系统。它按预定轨道飞行，不受电子干扰的影响。V - 1 于 1944 年 6 月 8 日第一次袭击了伦敦，这是世界上首次使用地对地导弹。



第二阶段，50年代到越南战争期间。从50年代到越南战争前，电子对抗曾一度被冷落。越南战争中后期，随着各种战术导弹、制导炸弹和用雷达控制的火炮等广泛使用，促进了电子战的全面发展。电子侦察活动自第二次世界大战结束以来，一直在不间断地进行着，电子侦察卫星、无人驾驶侦察机、投掷式电子侦察设备等多种侦察手段相继投入使用。针对炮瞄雷达和制导系统的应用，发展了各种欺骗性干扰技术，研究了专门摧毁雷达的反辐射导弹。专用的电子战飞机、一次性使用的干扰机等数百种电子战装置、器材装备部队。脉冲压缩雷达、频率捷变雷达、跳频电台等各种抗干扰能力强的电子设备不断涌现。各国研制的电子对抗设备达四、五百种。由于光电探测和制导技术在军事领域的应用，电子战又扩展到光电领域，新型电子对抗技术，如红外对抗、激光对抗、专用电子对抗飞机、反辐射导弹、计算机用于电子对抗等，促进了电子对抗战术的进步，使一度冷落的电子对抗，得到了迅速发展，引导人们向电子对抗的新领域进军。

制导对抗。当时的导弹与第二次世界大战末问世的导弹有了很大不同，采用了无线电、雷达、红外、电视或激光制导手段，命中精度大大提高，对抗导弹的攻击刻不容缓，因而，可以说导弹是电子技术的结晶，它已成为广义电子对抗中的一种武器。所以有人说，导弹所带来的是更高层次的电子技术的对抗。

越南战争初期，美国为对付越“萨姆-2”地空导弹的威胁，在1966年初生产出ARP-25机载雷达告警接收机，首先安装在战斗轰炸机上。它侦收到“萨姆-2”的“扇歌”雷达搜索发射的电磁波后，接收机自动将其输入计算机，由计算机把主要参数与“扇歌”雷达参数相比较。如果其主要参数与“扇歌”雷达的参数相同，飞机座舱里的红色告警指示灯立即闪亮，飞行员的耳机里同时听到制导雷达电磁波产生的音响。当制导雷达由搜索状态转换到跟踪状态时，由于雷达电磁波的重复频率增高，使耳机里的音响变得尖叫起来。告警接收机显示出信号来自的方位，表示导弹将要飞来，飞行员迅速做规避机动甩掉导弹。美军使用雷达告警接收机后，飞机的损失开始大大减少。几个月后，美军装备了AGM-4

A “百舌鸟”反雷达导弹，又称反辐射导弹。这种导弹依靠其头部的电子设备，接收雷达波束，能自动沿着波束飞向雷达将其击毁。从此拉开了电子对抗“硬杀伤”的帷幕。1970年后，美国人又在“百舌鸟”导弹上加装了记忆电路。即导弹一旦进入雷达波束，就能把飞行方向锁定。即使雷达关掉高压，仍能按原来波束方向前进，从而使命中率大为提高。

专用电子对抗飞机。越南使用了萨姆-2 雷达控制的57毫米高炮后，地面防空武器对美军飞机的命中率大为提高，直接威胁着美国的空中优势。由此，美国投入了大量的人力、物力研制专用的电子对抗飞机。

美军在战场上先后使用的专用电子对抗飞机有EB-66、EA-6A、EA-6B、EA-1E和EA-3A等。这些专用电子对抗飞机比第二次世界大战时的由轰炸机改装的电子对抗飞机有了很大的发展：一是专门为电子对抗设计制造的；二是采用了多种电子对抗设备。其功能和性能大大提高并日趋完善，能完成掩护己方作战飞机的突防攻击和返航任务。

1971年开始使用的E A - 6 B “徘徊者”基本型电子对抗飞机，是越南战场使用的最先进的电子对抗飞机。它的主要特点是采用系统综合接收机对有源干扰系统和无源干扰系统进行管理，保障自身携带的电子对抗设备对敌方的电磁威胁作出快速反应。它是美国海军在E A - 6 A的基础上改进而成的。第一架于1968年5月试飞，1971年交付部队使用。越南战争中，美军还使用了“野鼬鼠”电子对抗飞机，它先于己方的轰炸机或与轰炸机混合编队深入袭击目标附近的上空，用其携带的电子设备对地面防空系统的电磁辐射进行探测、识别和定位，再发射反辐射导弹摧毁辐射源，为轰炸机扫清障碍。

光电对抗。战争中光电对抗的兴起，使电子对抗扩展到了新的领域。美军把电视制导炸弹和激光制导炸弹等高命中率的炸弹叫“灵巧炸弹”。美军利用这些“灵巧炸弹”轰炸越南的重要目标。越南人利用激光制导炸弹必须不间断地用激光引导才能有效的弱点，摸索了一些施放烟幕和喷水等对抗激光制导炸弹的对策，用这些东西拦住激光，制导炸弹失去引导控制而炸偏。如越南人民军在保卫河内的安富发电厂战斗

中， 施放烟幕、喷水，高度超过建筑物 3 米，遮挡面积为目标的 2 —3 倍，烟幕浓度为每立方米 1 克。美军投入了几十枚激光制导炸弹，仅有一枚落在围墙附近。

第三阶段，从 7 0 年代到现在。2 0 世纪 7 0 年代以来，电子技术、航天技术、精确制导技术、隐形技术等飞速发展，电子对抗也相应进入了一个新的阶段。随着各种制导武器在局部战争中的大量而成功的使用，电子对抗的范围由无线电通信、雷达领域扩展到制导反制导以及红外、激光和水声等领域，并在战争中发挥出更大的作用。特别是中东战争、英阿马岛战争和美军空袭利比亚等作战中，电子对抗得到了广泛运用，并取得了引人注目的成功。1 9 8 6 年美军空袭利比亚时，以强烈的电子干扰为先导，使 2 0 0 千米以内的利军雷达全部失灵，并陷入瘫痪状态，以致利军防空兵器只能盲目对空射击，发射的防空导弹无一命中目标，美军利用自身强大的电子对抗技术，有效地保证了两个航母编队、1 6 0 架飞机的作战行动。

海湾战争提供了高技术条件下电子对抗全面发展和在战争中具有更为重要作用的新战例。这场战争以电子战拉开序幕，强大的电子进攻贯穿战争始终。早在“沙漠盾牌”行动期间，美军就对伊方实施了广泛的电子侦察，基本上掌握了伊军指挥、通信、导航、雷达系统的电磁频谱。开战之前，美军电子战飞机飞临战场上空，对伊拉克实施强压制电子干扰，使 200 千米范围内的伊方雷达迷盲，光电传感器失效，通讯中断，指挥失灵，武器失控。当巡航导弹爆炸时，巴格达城防部门甚至搞不清是导弹打的还是飞机炸的。直到 40 分钟以后，美机向巴格达总统府和通信大楼俯冲攻击时，伊拉克才开始实行灯火管制。战争期间，美军实施电子战的主要方式，是将电子战飞机、预警飞机与各种作战飞机混编成联合攻击编队，在地面和海上电子战部队的配合下，以干扰、欺骗和火力摧毁等手段，最大限度地压制、削弱伊军的武器系统和指挥通信系统，隐蔽己方的行动企图。在多国部队空袭作战所出动的飞机架次中，执行电子战任务的就占 20%。多国部队使用先进的电子战装备，通过实施广泛电子侦察，获取了伊军的电磁频谱；通过

实施电子伪装和佯攻，达成了作战的突然性；通过实施有源干扰和无源干扰，开辟了隐蔽的空中走廊；通过实施强大的电子压制，切断了伊军通信联络，使其丧失了指挥控制能力；通过运用反辐射导弹等精确致导武器，摧毁了伊军雷达和电子战装备，为作战扫清了障碍。由于多国部队综合运用了各种电子战手段，有效地保证了己方作战行动的顺利进行。

随着电子信息技术在军事上的广泛运用，C<sup>3</sup>I 对抗、计算机病毒对抗等一系列新型对抗领域相继发展起来，给电子战增添了新的内容。各国普遍应用最新的微电子技术和计算机技术来提高电子战装备的自动化程度和快速反应能力，实现了电子战装备的多功能、宽频段、大功率、小型化、固体化、高机动性和高抗毁性，以对付未来的高密度的复杂电磁环境。现代电子战已从早期的自卫和监视发展成进攻型的软、硬杀伤，既有了防御性的电子战，又有了进攻性的电子战。在前面提到的海湾战争中，以美国为首的多国部队装备有大量电子战装备，除了专门的电子战飞机和无人机外，从外层空间的卫星，到高、中、低空分层部署的飞机，乃至地面的战车、水面的战舰和水下

的潜艇，都配备有电子战装备，构成了多层次、全方位、全频段的严密的电子战体系。电子战装备技术先进，种类齐全，既有有源干扰设备，又有无源干扰设备，既有雷达对抗设备，又有通信和光电对抗设备，既有软压制，又有硬杀伤武器。总而言之，在这一阶段，许多新技术、新器件得到了广泛运用，电磁频谱不断得到开发，调制形式多样化，特别是数字技术、计算机和微处理机的广泛应用，使电子对抗设备进入了具有快速反应、功率管理、全自动化和自适应能力的综合系统的崭新时代。这一阶段的电子对抗已作为一种崭新的作战手段，在局部战争中大显神通。

### 形形色色的电子对抗技术

随着军事技术的发展，电子对抗所包含的技术范围越来越广，电子对抗的范围在频谱上已大大超过以往的限于射频(无线电波)范围的概念，迅速向两端扩展，即向低的声频和高端的光频扩展)电子对抗已呈现包括光学和声学对抗的新局面。



射频对抗即通常指的是电子对抗，包括通信对抗、雷达对抗、制导对抗(主要指雷达制导)、导航对抗、遥控遥测对抗等。这些设备多工作在电磁波频谱图的射频段，即包括通常的无线电波段和微波段。因此，整个射频波段都是进行电子对抗的领域。在这个领域中，导航系统多工作在超长波、长波、中波和短波段；通信多工作在中波、短波和超短波段；雷达、制导系统多工作在超短波和微波波段。

光学对抗又叫光电对抗，它包括红外对抗和激光对抗两大范畴，通常电视制导也列入光学对抗范围。光学对抗波谱范围从远红外起一直延伸到 X 射线、射线，已成为电子对抗的重要组成部分。

声学对抗主要是利用声学设备进行探测和反探测的措施。从发展来看，次声武器的发展必须使声学对抗范围扩展到频率低于 20 赫兹的次声频段(注：由于人一般只能听到 20—20,000 赫兹之间的声音频率，低于 20 赫兹的声波就被称为次声波)。次声波人耳虽然听不见，但人体内脏器官的固有频率却在 3—17 赫兹之间，根据前面介绍过的共振原理，我们可以理解，高强度的次声波能引起人体内脏器官

的强烈共振，导致人恶心、痉挛、休克、血管破裂乃至死亡。

电子对抗的实质就是敌我双方为争夺电磁频谱的控制权(即制电磁权)所展开的斗争。

电子对抗的范围，在频域上包括声学对抗、射频对抗和光学对抗(光电对抗)三个领域。从空间上可分为地面、海上、空中、空间和水下。就使用装备而言，可分为无线电通信对抗、雷达对抗、光电对抗和 C<sup>3</sup>I 系统电子对抗等技术。

### C<sup>3</sup>I：电子对抗的明星

C<sup>3</sup>I 系统是军事指挥自动化系统。它主要由指挥(C o m m a n d)、控制(C o n t r o l)、通信(C o m m u n i c a t i o n)与情报(I n t e l l i g e n c e)等分系统组成，也有人根据该系统的核心——计算机(C o m p u t e r)，称之为 C<sup>4</sup>I 系统。从功能上看，它是指挥员使用软、硬武器作战的指挥手段。其实质是一个信息系统，是实施信息战的一种综合性战略、战术系统，它是信息获取、信息

传输、信息处理、信息应用(指挥决策)和信息对抗,指挥软、硬武器参战,保持己方部队获取信息优势的一个大系统,也是一个军事电子系统。 $C^3I$ 系统是战场情报、分析判断、决策指挥、作战行动连为一体的军事电子的作战体系,利用它可实施信息战,压制敌方信息系统,保护己方信息优势。因此, $C^3I$ 系统中的电子对抗是实施信息对抗、系统对抗,乃至整个作战体系对抗的基本环节。根据美国1994年的新定义,已把 $C^3I$ 系统对抗改为指挥控制战(Command, Control, War),作战保密、军事欺骗、心理战、电子对抗和实体摧毁是指挥控制战的五大支柱。

在 $C^3I$ 系统领域中的电子对抗系统(除了武器平台自卫性的电子对抗系统要参战外)中,指挥员需指挥独立的电子对抗平台参战。系统对抗、综合对抗几乎包含了电子对抗技术领域的方方面面,雷达、通信、光电、引信、导航、敌我识别、计算机等都有其相应的电子对抗设备,电子对抗的软、硬武器的使用都要在指挥员严密指挥控制下实施。无论是电子防御还是电子进攻,电子战都要严格贯彻指挥员的意图

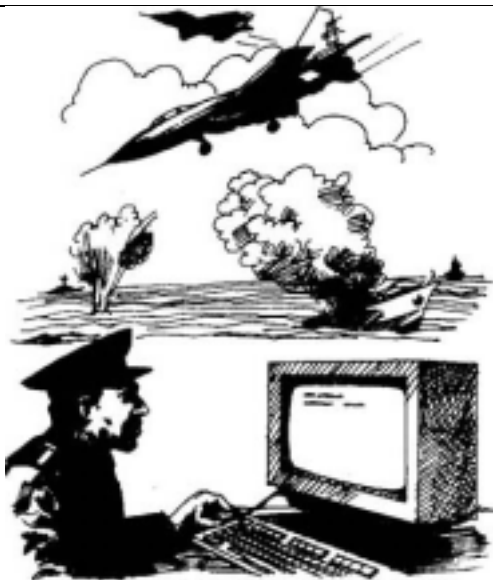
，何时、何地实施电子侦察，何地实施电子干扰，均由各级指挥员统一决策和筹划。电子对抗武器控制系统可向各级指挥员提供决策建议。

分布式综合通信网是  $C^3I$  系统与各类武器系统连接的“粘合剂”。它把  $C^3I$  系统、电子对抗系统和武器系统紧密结合为一体。在未来战争中， $C^3I$  系统是首要打击目标之一，其抗摧毁的生存能力极其重要。机动、隐蔽、伪装、反侦察、反干扰、反摧毁的技术途径和分布式的体系结构均很重要。若采用积极的手段，用己方的电子干扰、欺骗，计算机病毒干扰和反辐射武器系统等电子进攻手段去削弱、破坏、摧毁敌方  $C^3I$  系统，可造成敌高技术武器系统失控、信息传输中断、战场指挥失灵、丧失协调功能和整体作战能力，从而使己方获取信息优势。因此， $C^3I$  系统中的电子对抗系统是完成上述作战功能的电子防卫系统。从目前掌握的情况看， $C^3I$  系统中的电子对抗系统主要有：雷达电子对抗系统；通信电子对抗系统；光电电子对抗系统；计算机病毒干扰系统；GPS（全球卫星定位系统）电子干扰系统；敌我识别干扰系统；引信干扰系统等。

## 电子对抗：战争的重要支柱

在现代战争中，各种先进的武器系统越来越广泛地采用先进的电、光、声等电子信息技术。战场的侦察、监视和警戒，目标的跟踪与识别，导弹制导与控制，武器系统的瞄准与射击，部队的指挥与协同等都是通过电子信息技术来实现的，并构成了复杂密集的电子对抗信息环境。高技术战场实际上是一种信息化的战场。

现代局部战争的实践证明，取得电磁频谱控制权的一方，可依靠强大的电子进攻行动，使敌方的 C<sup>3</sup>I 系统失灵，指挥瘫痪，协同混乱，制导武器失控，从而使敌方战斗力受到削弱、破坏或丧失，同时有效地保障己方电子设备免遭破坏而达到保存自己、消灭敌人的目的。



美国前参谋长联席会议主席琼斯 1979 年曾指出：“电子战必须从自卫和监视转向作为一种武器系统与杀伤武器系统相结合。”美军一些高级将领认为，电子对抗已经是与地面、海军和空间作战相并列的第四维战场。俄军认为“夺取电子优势已成为夺取地面、海上，特别是空中战斗、战役胜利的重要因素。”

未来的高技术战争是电子对抗技术发挥巨大作用的战争。没有制电磁权，就很难有制天权、制空权、制海权、制陆权；没有电磁优势，很难有钢铁优势。

国外有人把电子对抗技术视为与精确制导武器、C<sup>3</sup>I系统并列的高技术战争的三大支柱之一。

电子对抗技术在现代战争中的作用主要表现在：

获取敌方军事情报。在现代战争中，通过电子侦察手段，如使用电子侦察站、电子侦察飞机、电子侦察船、电子侦察卫星和各种投掷式的电子侦察装置，利用敌方指挥系统和武器系统发射的电磁波，截获敌方各种无线电信号，加以分析，查明敌方雷达、无线电通信等电子设备的工作性能、技术参数以及兵器的数量和部署情报，从而判断敌军作战企图。这不仅有效地实施电子对抗的前提，而且是制定作战行动的重要依据，达到“知己知彼、百战不殆”的目的。

破坏敌方作战指挥。在战役和战斗的适当时机有效地施放干扰，可以使对方的无线电通信联络中断，指挥瘫痪，严重削弱其战斗力，从而为取得战役、战斗胜利创造有利条件。1982年黎巴嫩战争中，以色列采用了多种现代化电子对抗手段，集中破坏对手的通信联络和作战指挥系统，以微乎其微的代价摧毁了叙利亚设在贝卡谷地的导弹阵地和大批飞机。进攻前使用无人驾驶侦察机首先查明了无线电通信指挥

频率、萨姆-6 导弹的雷达制导频率；进攻时大量使用电子干扰，使叙利亚阵地通信联络中断，指挥失灵，雷达迷盲，导弹失控。以色列却集中了空军主力，出动了 100 多架飞机，夺取了制空权，仅 6 分钟就摧毁了叙利亚价值 20 亿美元的地面防空系统和 19 个萨姆-6 地空导弹连，使暴露在以色列空军严重威胁下的驻黎叙军，不得不在 6 月 11 日接受停战，显示了电子对抗在现代战争中的重要作用。

掩护突防和攻击。雷达是防御体系中的“千里眼”。它是对空、对海警戒，对飞机、舰艇引导和导航，对火炮控制和导弹制导的重要手段。可以监视千里之外的洲际导弹来袭和敌机活动，为防空作战提供早期准备，可以为导弹反击、飞机截击、火炮瞄准射击提供必要的参数。因此，对敌雷达实施有效的电子干扰、欺骗或摧毁，使其迷盲或破坏，变成“瞎子”，无法引导歼击机截击，使火炮、导弹打不准，这就能使己方飞机、舰艇、洲际导弹顺利突防和攻击，从而达到掩护进攻和突防的目的。

保卫重要目标。在现代防空体系中，地对空雷达干扰是一支重要的战斗力量。因此，在机场、城



市、港口、指挥所、交通枢纽等重要目标附近部署对空雷达干扰设备，对敌机的轰炸雷达实施干扰，使其无法瞄准，导弹失控，炸弹偏离目标，从而起到保护这些重要目标的作用。此外，对重要目标还可使用伪装器材进行适当的反可见光、反红外、反雷达的伪装，可以隐真示假，减少被敌人打击摧毁的机会，达到防御作战的目的。

保障电子设备充分发挥效能。战时，当己方电子设备遭到敌方电子干扰时，适当使用电子侦察设备迅速测出敌方电子干扰频谱及干扰源的位置，采取各种行之有效的反干扰措施，直到摧毁敌方的干扰源，最大限度地保证己方无线电通信迅速、准确、保密、不中断，使雷达探测及时准确，看得远，看得清，制导兵器控制自如，以此保障作战任务的顺利完成。

### 电磁优势：战争的制高点

当今的电子对抗已突破通信、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，从

自卫、监视、干扰等软对抗手段发展成反辐射导弹、电磁脉冲弹等硬杀伤手段。

现代高技术局部战争的实践已经表明，电磁优势已成为现代战场的制高点，电子战已不再是传统的战斗力的辅助部分，而是整个战斗力的重要组成部分。它与火力、机动力等战斗力要素并驾齐驱，从保障措施上升为驾驭电子化高技术战争全局的战略要素。它与火力、机动力相结合，实施整体作战，使部队战斗力得到成倍增长。可以说，在现代战场上，没有制电磁权，就不可能夺取制空权、制海权、制陆权，也就不可能取得战场的主动权。

电子战之所以愈来愈被各国军事家重视，电子战这一新的战争领域之所以会有那么神奇的魅力，其原因就在于现代化军队作战对电子设备的依赖性越来越大，电子战已渗透到战场的各个领域，甚至具有左右战局发展的决定性作用。现代战争中，系统“软”对抗将成为战场制胜的重要一环。高新技术兵器的“软件”构成武器一体化、系统化的重要环节。现代战场的“软”对抗，除了一般的软系统如 C<sup>3</sup>I 系统和电子战系统外，还包括各种硬设备中的电子分系统，这

些系统均以电子计算机为核心。国外有专家指出：“电子技术将在越来越大的程度上成为未来作战能力的关键”。他们在分析影响总体作战能力的因素时，以威慑性、通用性、效益性、全局性、长效性、可用性、技术兼容性、适应性等八项标准进行评价，认为最具影响力的是军用电子技术。这种软系统全面渗透到武器装备之中，从而激化了系统的“软”对抗，使用光电频谱的斗争左右着无形与有形的较量。缺乏制电磁权，就会陷大军于被动。

在现代战争中，电子对抗的地位和作用日益重要。这主要体现在以下三个方面：

首先，电子设备是构成现代武器系统的重要物质基础。现代电子技术的迅速发展及其在军事领域的广泛运用，给军队的指挥通信、军事情报、兵器控制等带来了一系列变化。以电子设备为基础的指挥、控制、通信和情报系统，将战场检测、情况判断、指挥决策和作战行动等有机地联系起来，并成为现代化军队的神经中枢和提高其整体作战能力的主要因素。从武器系统本身来看，电子设备也成为现代化武器装备的主导部分。武器系统一般可分为杀伤装置、运输

装置和控制装置三个组成部分，而现代化武器系统的“大脑”——控制与制导部分，几乎都是由电子装置构成的。电子设备不仅仅是武器装备的配套设备，而且已成为现代化武器装备的核心部分和主导方面。离开了电子设备，现代化武器系统就无法发挥作用。有关统计资料表明，武器装备越现代化，其电子系统的费用所占武器装备费用的比重越大，电子系统在武器装备中的作用也就越明显。如坦克的费用中，电子系统的费用占 30 % 左右；在飞机中的费用中，电子系统的费用占 50 % 左右；在制导武器、智能武器和空间武器的费用中，电子系统的费用已高达 70 % 以上。这说明，现代化军队作战将对电子设备的依赖性越来越大，而正是这种依赖性，增强了电子对抗的地位和作用，并加速了电子对抗向作战的各个方面的渗透。而这种依赖性造成了现代化军队的致命弱点，即这些电子设备一旦受到干扰与破坏，就会失去效能，就会给军队造成极大的被动。因此，以破坏或削弱对方电子设备的使用效能和确保己方电子设备正常工作为核心的电磁优势，就成为现代战场上作战双方激烈争夺的“制高点”。



其次，以软硬杀伤为标志的电子对抗能力，已成为作战能力的重要组成部分，对战争的进程和结局有着重要的影响。20世纪60年代以前，电子对抗主要使用电子干扰等“软杀伤”手段，使敌方电子设备及其武器的功能暂时或者完全丧失。60年代以后特别是80年代以来，使用反辐射导弹对敌方电子设备进行彻底摧毁的“硬杀伤”手段不断得到发展，并逐步做到了软硬两种手段紧密结合，互为补充，以取得最佳的压制效果。海湾战争中，多国部队就曾通过软硬杀伤手段的结合运用，成功地夺得了制电磁权。在“软杀伤”方面，美军投入了近百架电子战飞机，其中EF-111A电子干扰飞机，装有多用途电子干扰系统、金属箔条和红外诱饵投放装置、威胁告警系

统和红外侦察系统，可执行远距离支援干扰、近距离支援干扰、突防和护航干扰等任务，只需要几架这种飞机施放干扰，即可在一定范围的空间形成电子屏障，隐蔽己方作战飞机的航线和机动方式。除专用干扰机外，其他作战飞机也大都装备了机载电子干扰设备。在“硬摧毁”方面，美军调用了62架F-4G反辐射攻击飞机，该机可携带4枚射程为100千米的“哈姆”反辐射导弹。这些导弹具有记忆功能，能在雷达波束突然中断时继续飞向目标，甚至可以盲目发射、无定向飞行，直到发现雷达信号，再锁定目标加以摧毁。F-111和F-117A等也装备了“哈姆”或“百舌鸟”反辐射导弹。英军“旋风”式战斗机装备的“阿拉姆”型反辐射导弹，可根据计算机内预先存储的目标参数，主动搜索和攻击对方雷达。据报道，空袭头5天，多国部队共发射反辐射导弹约600枚，基本摧毁了伊军的雷达系统。目前，各国研制的反辐射导弹已近20种，美、英、法、德、俄等均已大量装备这种导弹。美、德等国正在研制新的反辐射导弹，如美制AGM-136等，可编程控制，发射后飞临目标上空，自动搜索和识别电

磁辐射信号，按优先级别实施攻击。此外，激光、微波和粒子束等定向硬杀伤武器对电子设备威胁也极大，可使激光、红外、电子设备过载、失效甚至烧毁。电磁脉冲弹也正在引起各国兴趣，据称，这是一种事实上的战术核武器，爆炸时能在瞬间发生能量极大的电磁脉冲，足以破坏对方的电子设备，使作用范围内的现代化武器处于瘫痪状态。这种以软硬杀伤为标志的电子对抗能力，使电子对抗作为一种效果显著的新型打击力量而成为现代作战能力的重要组成部分。电子对抗的成败将对作战的进程和结局产生深远的影响。

第三，高技术的发展将继续推动电子对抗不断向新的领域扩展，争夺战场制电磁权的斗争更加激烈。20世纪80年代以来，电子对抗技术一直是国际上军用高技术发展的一个重要领域，世界各国都投入了大量的人力和财力，以争取制电磁权的优势地位。海湾战争中电子对抗新的作战实践以及在战争中所显示出的重要作用，更加推动了这一趋势的加速发展。电子对抗武器系统正在向隐形、毫米波、光电对抗及空间电子战等新领域扩展。其中隐形技术近年来有较

大发展。美军的 F - 1 1 7 隐形飞机已经用于实战，其下一代隐形飞机 B - 2 、 F - 2 2 等也开始装备部队。俄罗斯、日本以及英、法、德等西欧国家也都大力研制隐形飞机。预计在 2 0 1 0 年前后，隐形飞机将占西方发达国家作战飞机的 3 0 % 左右。电子对抗装备领域已由常用频段向整个电磁波谱乃至光波频段发展，并在光电对抗方面取得较大发展，红外和激光探测、制导、告警和干扰装备也将陆续装备使用。电磁波直接杀伤性武器，如正在研制中的化学激光器、粒子束等武器，将成为重要的新电子对抗手段。外层空间电子对抗将日趋激烈，美国等发达国家正在加紧开发空间电子战系统，重点发展卫星对抗、战略导弹对抗和航天器的自卫电子对抗系统。军用计算机病毒正在研制开发，一旦使用，将把人类带进一个新的作战领域。在各领域电子对抗技术发展的同时，电子对抗系统正日益向着一体化方向发展。一体化电子对抗系统是把功能相近、相互关联的整个设备结合为一个系统，通过计算机和数字技术，集告警、侦察、干扰于一身，有源、无源干扰于一身，雷达和通信对抗、雷达和光电对抗以及软硬杀伤武器于一身，在密集而



又复杂的电磁环境中自动分析和识别信号，根据威胁严重程度，排列出干扰和摧毁的优先等级，分配干扰时间和功率，确定作战样式，鉴定作战效果。美国空海军研制的机载一体化电子战系统，就具有雷达和激光告警、干扰、导弹探测和报警功能，并计划将该系统与导航相结合，形成更大的一体化系统。欧洲各国还计划用本国生产的有源、无源一体化电子对抗设备装备下一代战斗机。这种情况表明，现代战场的电磁环境将变得更加复杂，争夺制电磁权的斗争将更加激烈。

### 无所不在的影响

开辟出一条新战线 现代条件下，由于电子技术和外层空间技术的发展，出现了新的战线，即电子对抗战线。通过研究前面所介绍的局部战争，可以得出结论，各国军队在武器、指挥和保障系统中装备电子器材的规模正在迅速增大。没有电子器材，就不能设想实施任何现代作战行动。复杂的电子环境以及作为其组成部分的电子对抗正在成为现代作战行动的一个

新的特征。第一，电子化趋势的表现之一是在执行合同作战任务时更加广泛地使用电子战器材。突然地、综合性地使用电子战器材，能使敌方军队指挥与武器控制系统很难甚至完全不能正常工作，可以减少己方军队的损失，从而能提高执行战斗任务的效能。运用电子战器材达成突然性特别是在初期作战中达成突然性的方法正在不断得到完善。在海湾战争初期，多国部队通过按统一计划，大量集中使用电子战器材充分达成了战役的突然性。在选定方向上实施的首次电子袭击，用于“迷盲”伊军电子侦察器材和防空系统，使伊军得不到有关多国部队意图的必要情报。接着就实施出其不意的强大的航空兵突击和导弹突击。在战争的第一个月中，多国部队共出动飞机 70,000 架次，但仅损失 30 架飞机。第二，近年来，战斗车辆(飞机)越来越积极地采用自卫系统。这方面首先优先完善的是通过坦克(飞机)乘员发现雷达辐射的设备以及施放烟幕或投洒偶极子反射体的设备。许多国家的军队现在已经采用了用于掩护的热辐射诱饵。正在研究使用“反炮弹”来进行“积极防护”的技术。战斗车辆(飞机)自卫的一个新的方向就是运用隐形技

术。为此，要使用减少目标暴露的专门的涂料，研究专门吸收无线电波的材料，美国在制造 B - 2 和 F - 1 1 7 A 飞机时就采取了这些措施。

这一切证明，整个军事发展的一个崭新阶段已经到来。正像 2 0 至 3 0 年代的摩托化改变了军队面貌和武装斗争的性质一样，电子对抗隐蔽无形、攻防兼备、全面渗透的特点，反映出电子对抗战线区别于传统战线的特点，它孕育于传统战线之中，又是传统的延伸。正是由于电子对抗战线的出现，现代战争从总的方面看，就形成了两条相对独立、互相渗透、相辅相成的战线，即火力的、硬的、有形的战线和电磁的、软的、无形的战线。

出现一种作战手段 电子对抗随着科学技术的发展，正沿着从低级到高级、从局部到全面，从作战保障手段到作战手段的客观规律向前发展。自电子战问世以来的相当长时间里，人们对它在战争中的地位和作用看法并不一致。较普遍的观点认为，电子对抗是一项重要的战斗保障措施。但近年来，随着电子对抗装备的更新换代，随着多次现代局部战争电子对抗的实践，人们对电子对抗在战争中的地位作用那种传统

的观念已发生了转变。首先，电子对抗已突破无线电、雷达对抗的范畴，扩展到指挥、控制、制导以及光电、水声对抗诸方面；由单一手段的对抗发展为多种手段的综合对抗；从纯粹的作战保障措施上升为更加直接的作战手段。众所周知，电子对抗的重点目标是  $C^3I$  系统。 $C^3I$  系统是现代化军队的“耳目”、“神经”和“大脑”，是实现空地一体化作战和大纵深立体作战的基础；同时  $C^3I$  系统又是电子技术广泛应用与电子设备高度密集的系统。运用电子对抗手段，可以保护己方的  $C^3I$  系统，干扰敌方的  $C^3I$  系统。电子对抗这种巨大的攻防作战能力，使它已由早期的一种战争作战保障措施上升为现代战争不可缺少的重要作战手段。徐向前元帅在 1985 年的题词中就明确指出：“电子对抗是现代战争的重要作战手段。”其次，过去人们把电子对抗的软杀伤和摧毁武器的硬杀伤相分隔。而今，反辐射导弹的成功运用，以及未来战场上将出现的激光、粒子束和大功率微波束武器，使电子对抗具备了破坏各种电子设备与系统的硬杀伤能力。由于能完成电子对抗侦察、干扰功能的“软件”与具有实体摧毁作用的“硬件”越来越

越紧密的结合，新型的电子对抗将发展成为现代战争中具有软硬杀伤能力的重要作战手段。

形成必备的作战能力 从贝卡谷地之战、美国与利比亚冲突到海湾战争，人们更加深刻地认识到电子对抗的重要地位和作用。现代化军队使用的火炮、坦克、飞机、军舰、导弹等各种武器都不同程度地装备电子设备，指挥现代化军队作战的 C<sup>3</sup>I 系统更是离不开电子设备。正是电子对抗设备在现代化军队中担任着重要的角色，使得一支军队电子对抗能力的高低对作战胜负起着重大的作用。战争实践表明，电子对抗能力已成为衡量现代化军队作战能力高低的重要标志。世界各国对电子对抗极为重视。不惜巨额军费开支，努力保持电子对抗装备的数量优势，不断完善电子对抗组织机构，在陆、海、空军直至师都编有专门的电子对抗部(分)队。电子对抗能力已成为外军战斗力诸因素中的重要成分。电子对抗能力也被列为我军五种现代作战能力之一，电子对抗兵进入合成军序列，说明我军把提高现代化军队的电子对抗能力摆到了十分突出的位置。

促进作战方式的变革和新作战理论的形成 电子对抗手段的运用，为战争实践提供了宝贵的经验，极大地促进了传统作战方式的变革和新的作战理论的形成。

电子对抗成为直接的军事打击力量，促成了电子对抗与火力战结合等软硬一体的新作战方式的出现；电子对抗的广泛运用，正在促进传统的作战方式发生重大变革。以海湾战争为例，地面交战与空中进攻的时间为 4 : 3 8，使空战取胜正在成为现实，战略空袭已构成独立的战争阶段；具有攻防能力的远程作战系统将短兵相接的近战转向远程作战为主；各种先进的作战飞机可以昼夜不停地实施空袭作战，将昼间作战转向夜间作战为主等等。这些作战方式上的改变，在很大程度上都得力于电子技术，特别是电子对抗系统效能的充分发挥。

在作战方式发生深刻变革的同时，新的作战理论也在逐步形成。20 世纪 80 年代以来，美军和前苏联相继提出的空地一体战和大纵深立体战等新的作战理论，都是和电子对抗的运用和发展分不开的。

## 鲜明的战争特征

贯穿于战争全过程，渗透到战场各领域 从时间上看，电子战贯穿于现代战争的全过程。美军空袭利比亚时，电子战就全程使用，其中前 6 分钟完全是电子战，而实际上电子战时间比空袭时间要长得多，从而有效地保证了外科手术式空袭的成功。

从空间上看，电子战渗透到战场的各个领域 关于这一特征，可以从海湾战争得到充分印证。多国部队陆、海、空三军各种电子战装备组成一个严密的立体电子战系统，太空有 18 颗电子战卫星，空中有 260 架电子战飞机和直升机，地面有 39 座电子监听站，海上有数艘电子战舰船，此外，各种武器系统都有其自身的告警自卫电子战装置，构成全频段、全方位、全高度、全纵深、主被动多源综合电子战网系，源源不断地为各级指挥官提供了战场信息。

从范围上看，电子战运用于不同规模的战争和冲突 纵观历次局部战争，无一不包括电子战内容。不仅在局部战争中使用电子战，在边境冲突中使用电子战，而且在外科手术式空袭等作战方式中同样使用电

子战。海湾战争投入电子战装备之多、效果之明显，是大规模电子战的首例；美军空军空袭利比亚则是电子战用于外科手术式空袭的成功战例。电子战不仅不受领土、国界、国际舆论和世界政治气候的影响，而且也不存在领土争端和撤军问题，使用范围极广。

战术手段综合运用，作战效益成倍增长 (1) 巧妙运用电子战战术。以空袭作战为例，电子战的作战重点是压制敌防空系统和指挥控制与通信系统，其战术主要有远距干扰、随行(队)干扰、近距干扰、开辟干扰走廊、遥控飞行器干扰、干扰敌指挥通信、无线电静默等。战术运用的好坏取决于电子指挥官的指挥艺术。在大规模空防作战时，多采用队形外、队形内干扰支援与自卫干扰相结合的战术，美空袭利比亚和海湾战争均采用此战术。对地面目标实施大机群攻击时，多采用近距干扰和自卫干扰相结合的战术。越战时美军干扰掩护 B - 52 实施地毯式轰炸便采用这种战术。对点状目标实施小机群攻击时，采用随队干扰和自卫干扰相结合的战术。单机空防时，只能采用自卫干扰战术。海湾战争初期伊拉克防卫能力较强时，多国部队采用强干扰和摧毁辐射源相结合、干扰机随



队干扰的战术；当伊军防空能力削弱后，则采用近距离干扰战术；当伊防空系统瘫痪时，则改用远距离干扰战术。(2) 综合使用电子战手段。现代战争中，电子侦察与反侦察、干扰与反干扰、摧毁与反摧毁、隐身与反隐身的斗争十分激烈，单一的电子对抗手段难以奏效，但各种手段与战术综合使用却能发挥其整体威力。海湾战争中，多国部队将电子干扰与电子摧毁相结合、有源干扰与无源干扰相结合、通信干扰与雷达干扰相结合、支援干扰与自卫干扰相结合、主攻方向干扰与佯攻方向干扰相结合，使各种电子战手段相互协调、相互补充，迅速夺取了制电磁权。战前以电子侦察为主；临战前侦察与干扰结合使用；战争初期以电子干扰和电子摧毁为主，电子侦察为辅。各阶段均从实际需要出发，综合使用电子战手段。(3) 不断提高电子战效费比。二次大战期间，击落一架普通飞机平均只需 800 发炮弹，而击落一架载有电子对抗装备的飞机则需 3,000 发炮弹，其作战效费比为 3.75 : 1。越南战争期间，美军未使用电子战之前，越军平均用 11 枚导弹击落 1 架美机；当美军采用电子对抗手段后，越军 80 枚导弹才能击

落一架美机，作战效费比为  $7.27:1$ 。第四次中东战争作战效费比则达  $90:1$ 。这就是说，给电子战装备投资 1 元，在二次大战中可以减少损失 3.75 元，在越南战争中可以减少损失 7.27 元，在第四次中东战争中可减少损失 90 元。海湾战争中，电子战的效费比则大大超过以往历次战争。

指挥控制集中统一，协同配合密切一致（1）统一设置指挥协调机构。美军认为，电子战必须遵守统一指挥的原则。电子战从战役指挥到实施过程，包括各种电子装备频谱的分配，对防空设施进行压制、摧毁的分工，都实施统一指挥控制。海湾战争中，中央总部及其军种情报处负责电子战情报的侦察、搜集和分析；作战处电子战作战科负责拟定电子战方案、电子战兵力兵器的配置计划等。在美军看来，现代战争应根据战争规模、作战任务和手中握有的电子战装备，制定周密的作战计划，统一指挥电子作战；同时还要求指挥官要像运用炮兵和航空兵一样善于指挥和运用电子战装备，在软硬两大武器之间合理分配目标，正确控制电磁频谱。（2）集中有效打击重点目标。美军强调，要把集中优势兵力打击要害目标作为电子作

战的一个重要原则。在空袭利比亚中，美军首先集中使用 9 架 E F - 1 1 1 A 和 E A - 6 B 专用电子战飞机对利比亚预警雷达网实施强烈电子干扰，并发射 5 0 枚反辐射导弹攻击利比亚地空导弹阵地，一举瘫痪了利方雷达和地空导弹系统，为实施主攻任务扫清了障碍。在海湾战争中，美军十分强调密集使用电子战装备和兵器，重点干扰和打击对美军构成严重威胁的伊防空系统和指挥、控制、通信中心；在首次空袭前 2 3 小时到开战后 3 天内，美集中使用大量地面干扰站和舰载大功率电子干扰发射机，对已查明的伊军各频段无线电信号实施大规模、全时空的压制性干扰，致使伊军雷达迷盲，通信中断。(3) “软、硬、隐”综合，促进作战效果。在海湾战争中，多国部队将“软杀伤”、“硬摧毁”和“隐形术”三管齐下，取得了良好的效果。在“软杀伤”方面，战争初期多国部队除使用陆基和舰载电子干扰设备对伊军实施强烈电子干扰外，还出动了 E F - 1 1 1 和 E A - 6 B 从空中干扰伊早期预警、目标捕捉和地面引导雷达，E C - 1 3 0 H 飞机干扰伊军的通信和导航系统，致使伊军雷达迷盲、通信中断、指挥失灵。在“硬摧毁”

方面，使用 F - 4 G、F - 1 6、E A - 6 B、A - 6 E、A - 7 E 和 F / E - 1 8 等型战机发射“哈姆”高速反辐射导弹，攻击伊目标引导和目标跟踪雷达，压制和摧毁伊防空雷达体系，致使伊大部分雷达遭破坏，残存的雷达不敢开机。在“隐形术”方面，F - 1 1 7 A 隐形飞机首先轰炸了伊南部加固防空截机指挥中心和伊西部防空作战中心，打开了一个缺口，为非隐形飞机开辟了通道；它率先突破巴格达市区，对巴格达通信大楼和空军司令部等重要目标实施了精确轰炸。它是唯一的能攻击巴格达市区目标和所有 1 2 类目标的飞机。它出动架次只占总出动架次的 2 %，却摧毁了被攻击的战略目标总数的 4 0 %，而且自身无一损失。这充分显示了“隐形术”的独特作用。



### 攻防兼备的战争手段

讲到电子战武器装备人们感到陌生是可以理解的。通过现代局部战争，特别是海湾战争，人们对电子战的认识逐步深化，并且把电子装备也看作是一种武器。美国从1995年后每年出版的《美国国防部技术领域计划》把电子战装备都列入了武器类，认为电子战装备是现代战争的重要作战武器之一。电子战武器装备分为电子战软武器和电子战硬武器两大类。

**电子战软武器** 电子战软武器是敌对双方使用的各种信息侦察装备与各种信息干扰装备进行信息战的非杀伤性武器，即侦察、扰乱、迷惑、欺骗、干扰破坏敌方各种信息装备系统，使其不能正常工作，降低其作战性能或使其完全失效的一种作战武器，故称为软武器。

在过去战争中使用硬武器(热兵器)，没有软武器这一概念。随着电子战装备在战争中的使用才出现了软武器这一概念。例如，使用引信干扰机，可以干扰破坏在同一波束频率范围内所有的引信炮弹，使炮弹在空中爆炸，不能发挥其威力和作用。电子战软武器这种特殊作战效能是硬武器难以达到的。

电子战软武器包括信息侦察和信息干扰两部分。

信息侦察是使用各种信息侦察设备和各种侦察测向与定位设备，对敌方及其战场进行各种信息侦察、记录、分析、处理、传递和利用，并查明敌方各种信息装备与武器系统部署的位置、数量、类型、技术性能参数等，严密监视敌方军事行动和企图，并保障作战时准确地实施信息干扰。

信息干扰是使用各种有源干扰设备、各种无源干扰设备、各种瞄准式和压制式干扰设备、各种欺骗式和模拟式干扰设备以及各种计算机病毒，对敌方的各种信息装备与系统进行干扰和破坏，使其不能正常工作或完全失效，起到非杀伤性武器的作用。

**电子战硬武器** 电子战硬武器是在电子战作战中用来直接杀伤与摧毁目标的电子战武器，主要包括反辐射武器、激光对抗武器、高功率微波武器等。

反辐射武器是采用电子侦察技术原理，对辐射源进行侦察、跟踪与制导、从而达到自动寻的摧毁辐射源目标的一种作战武器。它的发展使电子战从电子侦察反侦察、电子干扰反干扰发展到了电子摧毁反摧毁的硬杀伤作战领域。

反辐射武器目前包括由反电磁辐射武器、反光电辐射武器、反声波辐射武器等。反声波辐射武器主要用于海军舰艇攻击水下声纳装置。它自动寻的，跟踪声波辐射源，从而摧毁声呐装备和舰艇，是声呐对抗战的一种有效手段。

**激光对抗武器**，包括激光侦察告警与激光干扰设备以及反激光辐射武器。激光干扰就是使用激光武器

对光电控测设备和光电武器系统进行干扰、致盲和摧毁。反激光辐射武器是对激光辐射源进行自动寻的跟踪而摧毁激光辐射源的一种武器。激光对抗武器是现代战争中电子战光电领域作战的重要武器之一。

高功率微波武器是以电子为能源的电子战硬武器。它是以光束摧毁目标，并具有软硬兼施、攻防兼备的作战效能。高功率微波武器的发展将使武器发生划时代的变革。



## 四、遥看千河——展望电子战

### 电子战理论在突破

电子战将成为陆、海、空、天战场的核心。未来战场将由陆、海、空、天与电子战构成“五维战场”，交战双方将首先在电子战领域展开激战，并渗透到陆海空天各维战场。战争的立体性、纵深性、快速性、机动性、破坏性将进一步增大。电子技术的飞速发展，促进了武器装备进入电子化新时代，使现代武器装备电子设备的含量得以不断提高。据外军统计，电子设备采购费占飞机的 35% - 55%、占导弹的 45%、占军用卫星的 66%、占指挥系统的 85%。今后这种费用将会更高，电子设备将成为各种武器系统的核心。电子设备与系统已成为现代武器装备的“心脏”、“耳目”和“神经”。

战场电子战环境复杂。未来战场电子战环境有两大特点：一是电子装备种类繁多、部署密度大、电磁信号密集。据西方军事家计算，2000年以后，

重要作战地区集团军地域内敌对双方部署的电台多达 6,000 余部；一架战术飞机在重要战区上空 3000 米以上高度飞行时，可能受到 800 多部雷达的照射。这就要求电子侦察系统具有电、声、光各种体制的综合侦察能力；干扰设备要具有适时干扰上百部雷达并能同时干扰 10—20 部重点威胁的火控雷达的能力，否则作战飞机难以完成自卫的突防作战任务。

二是电子战频谱更加扩展，信息特征更加复杂。未来战争将使用各种先进的雷达、通信、导航、电子对抗、光电设备以及声、光、电多种制导手段的武器系统，构成密集而复杂的电子战信号环境。以雷达为例，50 年代信号特征比较简单，到 80 年代就相当复杂了。预计到下世纪初军事装备所用频段，将从 0.5—18 千兆赫扩展到 0.05—140 千兆赫，加上光电设备的频谱，那时电磁信号所占用的频谱将包括从超长波到光波波段在内的极宽的频域。

C<sup>3</sup>I 对抗将成为电子战的重点 C<sup>3</sup>I 系统是由侦察与预警系统、保密数字通信网络、电子化指挥决策支持系统以及电子战系统综合而成的一体化系统。战场情况侦察、目标的探测识别、武器系统的控制、

陆海空天多兵种协同作战的指挥通信、决策的制订、计划的实施，无一不依赖于  $C^3I$  系统。由此可见， $C^3I$  系统是军事实力与威慑力的重要组成部分，成为未来战争的关键要素。美国前总统里根曾说：“ $C^3I$  系统是我们的战略威慑力量中的一个决不可忽视的因素。”美国正在建立一个生存能力强、保密度高、可靠性好的全球  $C^3I$  系统。未来  $C^3I$  系统将是战略、战役、战术通用的、机动与固定兼容的、攻防能力兼有的、多功能相结合的综合性系统。国外已经把  $C^3I$  系统和武器控制系统作为一个整体来考虑，在设计一种新武器系统时，把  $C^3I$  系统的主要组成部分纳入其总体设计之中，以实现未来战场  $C^3I$  系统和武器控制系统的综合化。 $C^3I$  的特殊作用使得交战双方越来越把  $C^3I$  对抗作为电子战的重点。未来战争中  $C^3I$  对抗将更加突出。 $C^3I$  系统的核心是大量的电子计算机，发达国家正在加紧研制的计算机病毒主要就是针对  $C^3I$  系统的。美军正在研制高效能的军用计算机病毒，它是电子战场上的暗中杀手，可通过有线和无线方式感染对方的计算机系统，以破坏对方的指

挥、控制和通信系统。计算机病毒武器的问世和发展，将使未来战争的 C<sup>3</sup>I 对抗更加激烈复杂。

交战双方更加重视软硬杀伤一体化。未来电子战武器将趋于集电子侦察、识别、定位、压制和摧毁功能于一体，发展多层次、多功能、多用途的反辐射武器。反辐射武器包括反辐射导弹、精确定位攻击系统和袭击无人机。美军目前装备的 A G M - 8 8 A 反辐射导弹在空袭利比亚和海湾战争中发现目标后立即进入导引搜索状态，直到摧毁辐射源。精确定位系统——美“陆军战术导弹系统”已开始装备部队。西方国家也正在研制袭扰无人机。

正在研制的第四代空空、空地导弹具有自动截获目标和抗电子、抗红外干扰的能力，可同时发射多枚导弹、攻击多个目标，并具有全天候、全方向、全高度攻击和发射后不管的能力。

美国研制的机载一体化电子战系统耗资 5 亿美元，它集侦察、告警、干扰于一身，由机载计算机控制，可覆盖整个电磁频谱，能对付射频、毫米波、红外和激光的威胁信号，它代表机载电子战装备的发展方向，将装备于 F - 2 2 战斗机和 B - 2 轰炸机。

21 世纪的前 10 年，将处于武器电子化和电子武器化的重大变革时代。近年来，美、俄大力发展定向能武器，并在强激光武器和微波波束武器方面取得重大突破。这种直接使用光电能量和电磁能量来摧毁和杀伤目标的武器的出现，预示着武器装备的发展将产生质的飞跃。这种武器不用弹药，只要有电能供给就可进行连续射击，摧毁目标，而且经济、简便、作战效能高。这种电子武器既能直接探测目标信息，又能直接摧毁目标，无疑这是电子装备的一次革命，对未来战争将产生划时代的影响。

总之，未来电子战，在作战领域上要考虑陆、海、空、天电子战场；在地球上要考虑立体大纵深空地海一体作战；在频域上要考虑声、光、电、红外整个电磁频谱；在功能上要考虑雷达、通信、导航、敌我识别及制导武器的综合对抗。

### 电子战技术在发展

目前，电子战技术已成为国防科研的重要内容，其发展重点和趋势主要表现在以下几个方面：

C<sup>3</sup>I 对抗与反对抗是电子战发展的重点。电子战的对象是比较广泛的，其主要目标是指挥、控制和通信系统，防空(指挥)雷达系统，武器制导(指挥)系统等。这些系统中最重要的是指挥、控制、通信和情报系统，即 C<sup>3</sup>I 系统。C<sup>3</sup>I 系统对抗就是以敌方的 C<sup>3</sup>I 系统为对付的目标，在情报部门的支援下，综合运用作战保密、军事欺骗、电子干扰和实体摧毁等手段，阻止敌方获得情报，影响、削弱或破坏敌方 C<sup>3</sup>I 的能力，同时保护己方 C<sup>3</sup>I 系统免遭敌方的破坏。由于 C<sup>3</sup>I 对抗的目标包括敌方高级和低级指挥所、情报中心，以及进攻和防御部队的指挥所，所以 C<sup>3</sup>I 对抗能打破作战中电子能力的平衡，在战役战斗中起着非常重要的作用。

C<sup>3</sup>I 系统是国家和军队威慑力量的重要组成部分，是现代化军队的神经中枢。一旦 C<sup>3</sup>I 系统遭到破坏，整个作战体系便会陷于瘫痪，因此，C<sup>3</sup>I 对抗必须成为电子战的焦点。20 世纪 80 年代以来，外军 C<sup>3</sup>I 对抗系统已经有了很大的发展。目前，发展 C<sup>3</sup>I 对抗系统的基本着眼点是发展综合电子战系统，其基本发展趋势是：

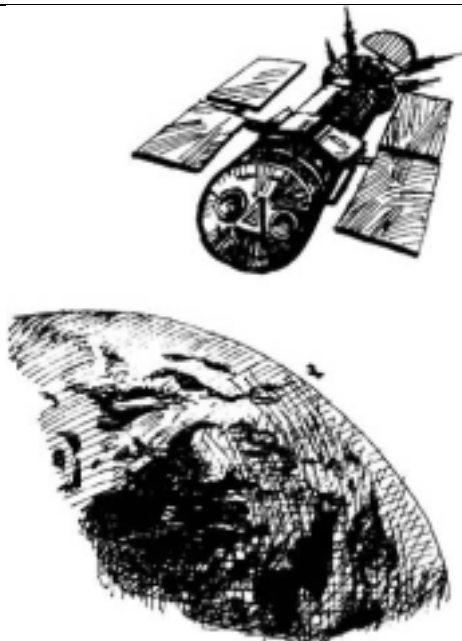
(1) 发展一体化、多功能的  $C^3I$  及其对抗系统。一体化、多功能的  $C^3I$  及其对抗系统由侦察与预警系统、保密数字通信网、电子化指挥决策系统、电子干扰与反干扰系统等组成，能够快速、准确地搜集和处理各种信息数据，预测各种威胁，判断最大威胁和选择最满意的指挥作战方案，更好地发挥整体作战优势。就  $C^3I$  及其对抗系统发展目标来说，国外规划的目标是逐步建立起全方位、多层次的全球系统。而  $C^3I$  对抗中干扰的频率范围可以从微波一直到可见光、远红外线，其干扰的方式可以有源的，也可以是无源的，可以是远距离干扰，也可以是伴随式干扰和联合干扰，形式多种多样，几乎达到无所不包的程度。如美军已经研制 I N E W S 全频谱电子战系统，其适用范围包括毫米波、红外、激光频谱，能对威胁告警进行数据处理、选择最佳反应方式实施干扰和功率管理等，是强有力的对付  $C^3I$  的电子战系统。

(2) 实现  $C^3I$  与武器系统综合化。国外发展  $C^3I$  系统的严重教训是与武器系统脱节，不仅浪费了人力、物力和财力，而且效能不高。目前把  $C^3I$  及

其对抗系统与武器控制系统作为一个整体考虑，在设计一种武器系统时，把 C<sup>3</sup>I 系统的主要组成部分纳入整体综合设计工作之中，以满足未来作战的需求。

(3) 发展机载和星载预警系统。情报侦察是 C<sup>3</sup>I 对抗的基础，因此外军十分重视预警系统的发展。美国军事专家经过分析得出，发展机载预警可使美国防空系统的效率提高 15 至 30 倍，可使美国用于本土防空的截击机数量减少 60%。80 年代的几场局部战争已充分显示了机载预警系统的重要作用。当前发展预警飞机的国家，除了美、英、法、俄外，已扩大到德、日、以色列等国，而且技术越来越先进，如以色列研制的“费尔康”预警机首次采用了先进的固体相控阵雷达技术。星载预警系统是超级大国尤其是美国重点发展的预警系统。据报道，美国研制的 3 颗装有红外探测设备的地球同步卫星可覆盖全球，并将预警系统与反导弹武器系统相结合，以进一步提高防御能力。





(4) 发展保密、抗干扰性能强的通信系统。通信系统是 C<sup>3</sup>I 系统的基础，通信对抗是 C<sup>3</sup>I 对抗的核心。在战争中干扰破坏敌方通信系统的正常工作，使其通信联络中断、指挥失灵，是通信对抗的目的。国外非常重视通信技术的发展，目前大力发展的主要通信设备有卫星通信、保密数字通信、激光通信、毫米波通信、扩频通信、快跳频通信、自适应通信等。在有线通信方面主要发展光纤通信，以构成抗干扰能力强的通信系统。

(5) 提高  $C^3I$  自动化、智能化水平。未来战争中战场信息量之大、变化之快，使一般  $C^3I$  系统难以满足需要，因此，美国和西欧国家正在广泛采用分布式系统网络结构、高级软件和人工智能技术，使  $C^3I$  系统信息实时处理和决策过程实现自动化、智能化。

隐身与反隐身技术是电子战技术发展的新领域。隐身技术或目标特征控制技术是电子战的产物，是为防止武器和平台被探测设备发现所采取的综合措施。目标特征控制技术能减小武器和平台系统的可探测特征，如飞机的雷达和红外信号特征，从而提高武器系统的突防能力、生存能力和作战效能。隐身技术是综合性高技术。运用材料科学、电子学、光学、声学、气动力学等多学科知识，通过采用吸波材料，隐身外形设计，冷却、消声等技术，可降低飞机、导弹、舰船、战车等武器系统被探测的概率。隐身技术萌芽于第二次世界大战期间，开始由于技术不够成熟，研究重点仅停留在雷达隐身方面，因而处于电子战的从属地位。后来在军事需求的推动下，经过多方面深入的理论研究和实际试验，逐步得到全面发展和广泛应用。

，并成为人们关注的焦点之一。当前，隐身技术的应用已有了突飞猛进的发展，F - 1 1 7 A 隐身战斗机、B - 2 隐身轰炸机已经用于实战，预计未来服役的新一代轰炸机、战斗机、预警机、巡航导弹、水面及水下舰船、地面战车大多将具有隐身能力。

隐身技术的发展和應用，给雷达的探测带来了新的威胁和挑战。一场隐身与反隐身技术的较量正在展开。目前国外发展的反隐身技术主要还是在雷达技术方面，如发展米波和毫米波雷达、双基地雷达、超视距雷达、激光雷达、谐波雷达、机载预警雷达、被动雷达和光电探测系统等，同时提高雷达的威力，采用先进的信号处理方法，改善信号与噪音的比值。此外，还将大力发展能摧毁隐形飞行器的导弹和电磁微波武器。随着反隐身技术的提高，隐身技术也不断发展，例如采用高性能的新型吸波材料，采用“探测——记忆”雷达和低截获率雷达等。总之，用于电子战的隐身与反隐身技术的发展，将是一个具有战略意义的技术领域。



计算机病毒对抗是电子战技术发展的新课题。计算机病毒实际上是一种依附在各种计算机程序中的一段伤害性自我繁衍的计算机程序。它通过磁盘或计算机网络传染，能破坏计算机的正常运行。之所以称之为病毒，是因为它像自然界生物病毒一样能使其他计算机程序受到感染，并在计算机系统或网络中得以繁殖、潜伏和扩散，从而使整个计算机系统或网络紊乱和瘫痪。

计算机病毒产生于 80 年代初期，1987 年以后开始迅速蔓延。由于计算机病毒具有种类多、繁殖感染力强、传播快、危害大等特点，因此一出现就受到电子战专家的广泛重视。他们正在努力探寻计算机病毒的“放毒”途径和“解毒”、“防毒”办法。计

计算机病毒对抗已成为各国军界研究电子战的新“热点”。

目前，计算机病毒对抗还处在研究、发展、完善阶段。可以预计，计算机病毒的出现将推动电子战向更新、更宽的领域发展，其发展趋势将在后面的章节中具体介绍。

对抗计算机病毒的基本方法有：建立自己的集成电路生产工业，实现计算机的完全国产化；改造引进的计算机系统，建立安全人口；研究病毒检测方法，提高抗病毒能力；加固电子信息系统，提高抗电磁脉冲；严格管理，提高人员素质等。

电子战技术的新发展增强了电子战的应变能力。电子战技术难度大、技术变化快、作战对象广，只有技高一筹，才能克敌制胜。这种状况促进电子战技术不断出现众多的新思想、新观念、新技术，以不断增强电子战的应变能力。

(1) 电子侦察设备。它主要用于查明对方电子设备的类型、数量、配备、部署和变动情况及电子设备的技术性能，以便为判明敌人企图、采取对策和实施干扰提供依据。外军装备的电子侦察设备主要有雷达

告警接收机，通信、雷达侦察接收机，通信、雷达测向定位系统。电子侦察设备的发展动向，一是扩展电子侦察设备的工作频段，将原来的 1 8 吉赫(1 吉赫 = 1 0 0 0 , 0 0 0 赫兹) 扩展到 4 0 吉赫，甚至高达 1 4 0 吉赫，以满足侦察毫米波的需要；二是提高侦察设备的灵敏度和测向精度；三是采用微处理器，增强侦察测向设备的功能；四是发展快速机动的小型测向设备；五是研究新体制的侦察测向设备，主要是研究以声光和数字技术为基础的新型侦察接收机。

(2) 电子干扰设备。它主要用于对敌方的通信和雷达设备实施扰乱和欺骗，以降低其效能，使之失效。外军装备的电子干扰设备主要有有机载有源干扰系统 and 无源干扰物投放系统、舰载干扰系统和地面干扰系统。电子干扰设备目前的发展动向，一是提高干扰功率，主要是发展大功率固体器件和功率合成技术，研究大功率微波和毫米波干扰机；二是发展计算机控制的“自适应”电子对抗系统，以提高电子对抗系统的灵活反应能力；三是积极研究多波束和相控阵电子对抗系统，如美国雷声公司研究的 A N / S L Q —3

2 舰载电子战系统，可同时干扰 80 部雷达；四是研究跳频通信干扰设备，以对已投入使用的跳频电台实施干扰；五是向一体化通用系统发展，即把功能相近、相互关联的数个设备结合为一个系统，同时适用于多种平台。

(3) 光电对抗设备。光电对抗是指作战双方在光频段进行的电磁波斗争。光电对抗设备的发展起步较晚，但速度很快，特别是美军在 90 年代研制装备了不少光电对抗设备。光电对抗设备目前的发展动向，一是大力发展光电对抗设备，如激光告警器、红外告警器；二是在继续研制新型红外诱饵弹的同时，积极研制红外干扰机和激光干扰机等设备。红外诱饵弹是常用的红外干扰器材，主要用于对付全向红外寻的导弹和双色红外制导导弹，美国正在发展温度较低的红外诱饵弹。红外干扰机和激光干扰机现已经装备部队使用，未来将发展更灵巧的红外干扰机和一次性使用的激光干扰机。随着光学器材制造技术的突破，不断发展，将有可能出现通用的光电、红外对抗系统。

(4) 反辐射武器。又称反雷达武器，它是利用敌方雷达的电磁辐射，搜寻目标、跟踪直到将辐射源摧

毁的武器。海湾战争中多国部队使用了相当数量的反辐射导弹，打击伊拉克的防空雷达系统并取得了一定的效果。反辐射武器技术的发展主要是进一步扩展导弹导引头的频率覆盖范围，采用复合制导技术，制导与控制系统全数字化以及广泛采用反辐射无人机。反辐射无人机是为克服反辐射导弹功能或作用有限的弱点而发展的一种新型反辐射武器。反辐射无人机上载有雷达探测和导引装置及战斗部。它与反辐射导弹相比，具有造价低、巡航时间长、使用灵活等优点，通常将其发射到战场上空或目标雷达上空巡逻飞行，一旦雷达开机，机载导引头便立即捕获目标，并控制无人机攻击雷达。

(5) 综合电子战系统。这个系统是把不同种类、不同型号、不同频段和不同用途的电子战设备和电子战系统进行综合设计、综合控制、综合管理、综合运用，构成一个综合性的、一体化的、数据综合、自动响应、资源可以重新组合的电子战系统。目前，已经投入使用的综合电子战系统有机载一体化电子战系统和舰载一体化电子战系统。这些一体化电子战系统集成整个武器装备平台的电子设备、光电设备(包括通信、



导航、敌我识别、火力控制、航空或航海控制、电子战等系统)于一体,进行管理、控制和运用。一体化系统采用了先进的功率管理技术,具有很强的有效辐射功率和最佳的干扰技术,可及时提供多种复合干扰模式,同时对付多种威胁。今后将发展技术上更先进的大范围一体化综合电子战系统,美军正在研制和 I N E W S 综合电子战系统就是一例。

(6) 分布式干扰。这是指用大量分布在特定空域、地域的体积小、重量轻、价格低、功率小的干扰机或干扰器材对目标实施干扰。它们在目标信号(雷达和通信及其他信号)触发下发射或产生欺骗或压制式干扰信号,在敌方雷达屏幕上形成大量的假目标或许多干扰噪声带,在通信接收机内产生来自不同方向的干扰信号,从而达到用较小的干扰功率降低敌方电子系统的工作效能、掩护己方的目的。分布式干扰系统是一个多点分布、形成网络并可以扩充的系统,生存能力强,不易受到全面破坏。因此,这种以数量取胜的分布式干扰是对抗预警机、多基地雷达、网络通信的有效手段。现在,这种技术在微波、毫米波集成技术日趋成熟的基础上正得到迅速发展。

(7) 微波武器。发展中的高功率微波武器或称电磁脉冲武器的有效功率远比现有干扰机大得多，一般要大百万倍。这种能量虽然尚不足以破坏武器平台，但却能毁坏电子线路和电子元器件，或烧毁高灵敏的电磁传感器，使其永久性致盲，或使计算机不能正常工作。因此，微波武器是可对电子系统实施杀伤的一种新手段。美、德、英、俄等国均在加紧发展这种新型电子战手段。据报道，美国在海湾战争中曾以巡航导弹为运载工具，使用微波攻击伊拉克的防空体系。法国已研制并试验了功率为 200 亿瓦的微波武器。俄罗斯在前苏联微波武器研制取得重要成就的基础上，将可能逐步部署微波武器。种种迹象表明，微波武器是电子战的新成员，将可能大规模用于未来战场。此外，激光武器、粒子束武器也是美、俄等国竞相发展的电子战武器系统。

利用和发展传统电子战技术仍是提高电子战能力的有效途径。所谓传统电子战技术，主要是指消极(无源)干扰技术，如箔条干扰物、干扰丝等。除此之外，还包括各种伪装技术、假目标技术、烟幕技术等。

进一步发展和综合利用这些技术措施是提高电子战能力的有效途径。

消极(无源) 干扰技术是战争中产生、应用和发展起来的一种价廉、有效、易行的电子干扰技术。随着电子战技术的广泛应用, 消极(无源) 干扰技术还将大量使用并得到新的发展。就干扰箔条来说, 当前最显著的变化有: 在材料方面, 早期的箔条是用锡、锌、铝等金属制作的, 目前已由镀铝(镀锌、镀银) 玻璃丝、涤纶丝、尼龙丝取代。在形状方面, 为了增加箔条在空中的留空时间, 制成了空心箔条, 壁厚仅 0.25 毫米; 为了增强干扰效果, 将条状改变为圆形箔片干扰物。在功能方面, 针对电子对抗一体化发展的需要, 目前正积极发展复合箔条, 将微波(毫米波) 反射型涂料与红外气溶胶涂料结合起来, 形成可干扰红外、可见光、微波的宽频带干扰物。在结构方面, 现已研制出不同结构的干扰球、气悬体和干扰绳等。干扰球是将干扰丝制成颗粒状而形成的, 具有良好的使用性能。如果将各种干扰丝制作成更微小的微粒, 布撒在空中, 就形成了由这些微粒组成的气状云, 它可使雷达处于迷盲状态。干扰绳通常是由多股镀铝玻

璃丝和铝箔条制成，主要用于干扰低频雷达。此外，箔(丝)状干扰物另一个变化是发展了气球干扰物，如一种迷彩金属涂敷气球是在气球表面上涂敷既能反射射频也能反射红外和可见光的材料而制成的，它能同时干扰雷达、红外和激光。

伪装网是一种传统的伪装器材。过去的伪装网只能对可见光起伪装作用，而且比较笨重。现在的伪装网已向轻型和综合多光谱的方向发展。美军有一种袖珍伪装网，折叠后可以装在士兵制服口袋里。综合多光谱指一个伪装网具有防可见光、近红外、热红外和雷达侦察的综合防护能力。这种伪装网主要用于伪装价值高的军事目标，并将逐步取代性能单一的伪装网。

假目标可以分散敌人精确制导武器攻击的火力，从而提高真目标的生存能力。假目标主要有充气式、装配式和膨胀式三种。现在已经形成装备的充气假目标伪装器材有模拟坦克、飞机等。它们造型逼真，体积小，重量轻，充放气速度快，并可配有热源和角反射器，能对付从可见光、近红外到雷达波段的探测器。此外，使用聚氨酯泡沫塑料制成的膨胀式假目标

和装配式假目标也正在研究中，前者压缩后的体积为原来体积的  $1 / 10$ 。

烟幕对红外、激光等电磁波具有强烈的干扰和破坏作用，可使激光、红外制导系统无法工作，对保护昂贵的坦克及其它武器装备有很大的作用，所以各国都在发展烟幕器材。目前这方面的研究工作主要是寻找合适的发烟材料或气溶材料。国外研究最多的六氯乙烷和水雾烟幕，可干扰  $10.6$  微米波长的是二氧化碳激光指示器和红外制导武器。此外，国外还研究有色伪装烟幕，如彩色水雾烟幕、绿色伪装烟幕等。

## 新概念武器在研制

在高技术发展不断取得重大成就的基础上研制的高技术武器装备，将是未来国防科技发展的关键。如果一系列令人惊奇的新概念高技术电子战武器一旦研制成功并装备部队，将引起电子对抗、光电对抗的方式、理论和战法的重大变革，并对军事领域产生深刻的影响。

2 1 世纪可能出现的新概念信息化电子战武器装备主要有:

**激光武器** 激光武器是指利用激光束的能量直接杀伤破坏目标或使其丧失作战效能的武器。它分为战术激光武器与战略激光武器两大类。

战术激光武器由激光器件、激光束发射系统(包括对激光束进行补偿的自适应光学系统)和跟踪瞄准系统构成。可能采用的激光器件有氟化氙(D F ) 化学激光器、二氧化碳(C O<sub>2</sub>) 化学激光器、钇铝石榴石(Y A G ) 激光器等, 发射系统由发射望远镜及光路调节部件组成。跟踪瞄准系统包括一组光学传感器及与之相连的数据处理设备。战术激光武器主要包括激光致盲武器、激光干扰武器和激光防空武器, 其作战对象是人员、军事装备上的光电装备及飞机、战术导弹、巡航导弹等。这些激光武器的作战距离一般在几十千米之内, 对激光器的功率、光束亮度及质量要求较低, 利用已有的高技术成果已能研制出来。美国的武装直升机、装甲战斗车, 俄罗斯的军舰、坦克等, 均已装备了这类激光武器。美国步兵装备的手提式激

光致眩器重约 9 千克，大小相当于一支冲锋枪，最大能量输出在波长为 7 5 5 纳米时，平均功率 7 0 瓦。

战略激光武器的基本结构与战术激光武器大致相同，只是各组件的要求不同。可供选择作为战略激光武器的激光器是强激光器，如自由电子激光器(F E L)、核爆泵浦 X 射线激光器、氟化氢(H F)和氟化氙(D F)化学激光器、准分子激光器等。战略激光武器的发射系统和跟踪、瞄准、识别系统在技术上也有很高的要求。战略激光武器大致可分为两类：一类是反卫星激光武器，它们可以干扰、破坏卫星上的仪器设备或摧毁卫星平台；另一类是反弹道导弹激光武器。这两类激光武器均可采用两种部署方式：一是部署在太空的作战平台上(即天基激光器)，二是部署在地面上(即地基激光器)。天基激光器不需要考虑妨碍或限制激光束传播的大气影响，也没有像风动(气流)或地动等影响激光瞄准与跟踪系统精度的外部振动源等，但因需要将尺寸和重量都很大的装备部署在太空，所以运行费用高。天基激光器可选用氟化氢或氟化氙化学激光器。美国的“战略防御倡议”计划，最初还提出以天基核爆泵浦 X 射线激光器作为洲际弹道导

弹最有效的拦截武器。这种核定向能武器是一颗氢弹装置周围安装 50 根激光棒，氢弹爆炸时产生大量 X 射线，每根激光棒从中俘获一定量的 X 射线，从而激励出 X 射线激光，并射向指定目标。被科学家称为“亚瑟王神剑”的这种高能激光器威力强大，能同时摧毁大量空间目标。但核爆泵浦 X 射线激光器可能是所有激光武器中技术难度最大的一种，至少要到 21 世纪中期才能研制成功。地基激光器在设计动力系统和光学系统时可以各自采用相对独立的先进技术，同时，其功率标准、发射时间不受燃料供给的限制，操作维护也比较方便。但由于受地理等条件的限制，地基激光器的有效覆盖有限。此外，地基激光器发出的激光束因受大气的影响会产生损耗和畸变等。为此，必须为地基激光器设计一个混合式的光束控制器、大气补偿及火力控制系统。如地基激光武器的典型作战系统方案之一是，在地球同步轨道上安装一台中继线反射镜，在低轨道上安装一台战斗镜。中继反射镜将地基激光器发射的高能激光束反射给战斗镜，战斗镜将接收到的射束再聚焦射向目标。地基激光器可选择自由电子激光器作为激光装置。



此外，美国目前还提出了一种机载自由电子激光武器的概念，即将自由电子激光器安装在波音 747 之类的飞机上，用于战区防御，摧毁处于助推段的战术弹道导弹。这种机载系统显然有便于部署、使用和维修等一系列优点。

尽管高能激光武器的研究至少已有 10 年以上的历史，并取得了一系列进展，但还有许多关键技术问题(如燃料消耗大、输出功率偏低及光束质量不高等)没有解决。不过可以肯定，由于激光武器具有巨大的优越性，各国在未来国防科技的发展中必将对激光武器的研究予以足够的重视。在下一世纪的某个时候，“亚瑟王神剑”必将开辟国防科技和战争发展史上的新里程。

**微波武器** 早在 20 多年前人们就已经知道，强大的无线电微波辐射会干扰、破坏、甚至烧毁军用设备中的电子元器件。所以，科学家们便设想把高功率微波辐射作为一种武器使用，以便对现代军用装备中的电子系统进行干扰和破坏。例如，用 0.01—1 微瓦/平方厘米的能量，就可以干扰相应频段的雷达和通信设备的正常工作。用 10—100 瓦的强微波

辐射形成的瞬变电磁场，可使金属表面产生的感应电流与电荷，通过天线、导线等，进入坦克和装甲车辆、导弹、飞机、卫星等内部，从而破坏各种敏感元件和电子设备，使武器系统失灵。微波武器的能量如果达到  $1,000—10,000$  瓦/平方厘米的强度，则可在很短的照射时间内使目标受热而破坏，甚至可能引爆武器中的炸药，使武器被毁坏。

微波武器还可用于杀伤人员。其杀伤机理有“非热效应”与“热效应”两种。“非热效应”是用  $3—13$  毫瓦/平方厘米的微弱能量照射人体，可引起人烦躁、头痛、神经紊乱、记忆力衰退等。战时，这种效应可使武器系统的操作人员无法正常操作，甚至使战斗人员丧失战斗能力。所谓“热效应”是利用强微波辐射照射人体，当能量密度为  $20$  瓦/平方厘米、照射时间为  $1—2$  秒时，产生的高温高热可造成人员的死亡。如果能量密度更大时，可以瞬间将人“煮熟”。微波波束可以穿过缝隙、玻璃或纤维进入坦克、装甲车辆内部，烧伤车辆的人员。因此，微波武器将是一种全新的作战手段，它将使军事力量的结构变得更加灵活机动。

高功率微波武器大致有两类：一类是可重复使用的多脉冲微波武器；另一类是单脉冲爆炸式微波武器，如高功率微波炸弹或弹头。

可重复使用的多脉冲微波武器常常也被列为定向能武器之一。它由强微波发射机、高增益天线以及其它配套设备组成，美国已开始进行要领性研究的等离子体脉冲式磁流体动力微波武器就属于这类微波武器。这种武器的技术难度很高，因为一方面，从现行技术水平来看，要达到适合军用平台的重量和尺寸的要求，其储能效率至少还要提高一个数量级；另一方面，由于武器上有电子仪器，在反复使用中，这些电子仪器本身必须能经受住反复的脉冲作用，为此须对天线用超水平的工艺设计，但要解决这一问题是相当困难的。

一次性使用的高功率微波炸弹或弹头是比较可行的概念，美、英和俄等国都在研究这类技术。

高功率微波炸弹既可用飞机投掷，也可用作导弹弹头，或用远程火炮发射。如果其部署在天基作战平台上，可成为一种有效的反卫星武器。据说，在海湾战争的“沙漠风暴”行动之初，美国曾向伊拉克首都

巴格达投下了几枚微波炸弹，以试验其破坏电子设备的能力。21世纪，高功率微波武器将作为一种更新的手段，使电子对抗将更加多样化、复杂化。



**计算机病毒武器** 随着计算机在武器装备和军事活动中的广泛使用，计算机病毒武器也随之产生。所谓计算机病毒，实际上就是一种特殊的计算机程序。就像病毒侵入人体引起人生病一样，它们侵入计算机系统，能够干扰、修改正常运行的计算机程序，破坏其有效功能，并能够复制和自动侵入其他程序之中，使周围的计算机程序也遭到破坏。计算机病毒具有计算机软件的有关特征。比如，它是由程序人员专门设计和编写的；它能按照软件规范的基本要求，以计算机可以运行的代码方式出现；它可以存储在计算机软

盘、硬盘或其它外部设备之中，能够通过计算机系统或网络进行传输等。美军从 1987 年开始研制计算机病毒武器。1990 年 5 月，美国军方曾出资 55 万美元招标，研制干扰和摧毁敌方电子系统的计算机病毒，并耗资 1.5 亿美元成功地研制出微电脑芯片的“电子固化”技术。

计算机病毒具有种类多、隐蔽、繁殖感染力强、传播快、危害大等特点。1988 年 11 月 19 日，美国发生了震撼世界的大规模的计算机病毒感染事件。由于一种病毒侵入包括军用网络在内的国家计算机网络，结果直接经济损失高达上亿美元。各国计算机专家、国家安全部门、金融界等为此大惊失色。又如，海湾战争前夕，美国谍报人员得知伊拉克向法国订购了一批用于防空指挥系统的电脑打印机后，即将一种由美国设计的病毒芯片偷偷装入这批打印机内，从而严重干扰了伊拉克防空系统的指挥，使其在海湾战争中未能正常发挥作用。与此同时，美军派出一批计算机安全专家，对其将在海湾战争中使用的计算机进行了一次全面检查，发现并清除了三种病毒，从而确保了这些计算机在战争中能正常工作。

据国外电子战专家估计，目前进行计算机病毒战的条件已经成熟。21世纪，计算机病毒武器将被列入战略武器库中，而且，计算机病毒对抗也很可能成为未来高技术战争中的一种新的电子对抗手段。

现在已研究出了多种计算机病毒的“施毒”、“解毒”、“防毒”的方法。例如，已发现三种施放计算机病毒的途径：一是利用电磁波传播——将计算机病毒调制到电子设备发射的电磁波中，当其被敌方无线电接收设备接收后，即注入敌方的电子系统，并在其中扩散；二是利用计算机网络中配套设备传播——通过诸如天线系统、电源系统、传感器系统、驱动系统等将病毒注入并传播到与主设备相连的计算机中；三是通过有线线路传播——目前的计算机大多是通过有线线路联网，战争中只要在敌方有线线路上开口并注入病毒，即可使其向网络内的所有计算机扩散。

计算机病毒侵入敌方计算机系统后通常用四种方式进行干扰和破坏：一是“特洛伊木马”式——病毒进入后能暂时或长期潜伏下来，一旦得到指令后便被激活进行破坏，如固化在微电脑芯片中的病毒，就属于此类能潜伏和遥控的病毒；二是负荷过载式——

病毒侵入后，能对自身大量复制，使敌方计算机系统处于超负荷运行状态，从而降低运算速度，并不断出现闭锁状态；三是“刺客”方式——病毒侵入后专门篡改或销毁一些特定的文件、数据、指令等，完成此类“刺杀”任务后又自行清除，不留痕迹；四是强制隔离方式——病毒迫使敌方控制中心与各系统相隔离，造成整个系统的混乱。

计算机病毒武器的作战目标主要是：窃取情报，破坏指挥、控制、通信和情报系统，摧毁经济支持能力。美国军事专家认为，计算机病毒战比核战争更现实、更有效，比任何杀伤性武器更人道，但破坏效果却大得惊人。据估计，若使用病毒扰乱美国银行系统的计算机网络，1秒钟就能盗走1,600亿美元，这将使美国经济崩溃，无法支持任何规模的战争。

21世纪将要问世的新概念高技术电子战武器是多种多样的，甚至千奇百怪，令人应接不暇。除以上所列的之外，还有次声波武器、人工智能武器、电磁炮等等，让我们拭目以待，试看21世纪的电子战场谁将称雄于世。

## 计算机的卫士

在世纪之交的今天，电子计算机特别是微型计算机在军事领域的应用正朝着普及化的方向迈进。21世纪，计算机的应用将在整个军事领域独领风骚，无论是平时军队建设中的武器装备、作战指挥、信息情报、后勤保障和教育训练，还是战场作战中的战斗系统、支援系统和保障系统；大到战略 C<sup>4</sup>I 网络，小到地面士兵装备；高至航天器，低至深海潜水机器人；从总司令部到散兵坑，都不能不依仗计算机的神奇功能。武器发射后不用管，运筹屏幕键盘指挥千军万马，已不再是天方夜谭。然而，军事家们也敏锐地发现，计算机在给现代军事机器注入强大生命力的同时，也使其自身成为重要的作战武器、目标和战场。

计算机的防护是21世纪军事对抗的焦点。计算机及其软件，已成为和必将成为现代化武器装备的灵魂与神经系统，也必定是敌对双方相互打击的核心目标。越是对信息依赖大的国家，越是容易受到信息武器的攻击；如果一个国家的信息联系遍布全球，那它易受攻击的范围也是全球性的。电脑入侵已经成为高



悬于世界各国头上的“达摩克利斯之剑”。任何国家想避开它是不可能的。唯一的选择就是面对现实，积极研究防范手段和对敌实施电脑袭击的方法。美军已经充分认识了这一点，并一再突出强调，在信息战中除了强调主动进攻外，还十分注重对己方信息系统的防护，即进攻性信息战需要有防御性对抗措施。计算机运用越广泛，防护计算机安全的兵员就越多。为适应信息战需要，按照“有独立的基本武器和军事技术装备及其战斗使用方法”这一兵种的划分原则，计算机防护兵必将成为新的兵种。

计算机防护兵的主要作战对象 计算机防护兵虽然目前尚未被正名，但已在美、德、法、英、日等发达国家孕育着。未来计算机防护兵的主要作战对象包括四个方面：

防计算机“黑客” “黑客”是计算机防护兵的重要信息对抗对象之一。所谓“黑客”，是指通过计算机渗透窃取信息和破坏信息系统的人。随着军用计算机网络的形成，特别是军用计算机网络与社会计算机网络的联通，信息高速公路的迅猛发展，互联网络四通八达、遍及全球，为“黑客”入侵军事禁区打开

了方便之门。1996年初，法国国防部证实，其海军参谋部计算机储存的军事机密于1995年7月底被人盗走。这些机密包括几百艘盟军军舰的声音识别密码以及舰只航行图。英国也发生了轰动整个大不列颠岛的“黑客”光顾事件。一些电信公司的电脑操作员，通过公司内部的数据，窃走了英国情报机构、核地下掩体、军事指挥部及控制中心的电话号码，连前任梅杰首相的私人电话也未能幸免。据美国情报专家估计，美军计算机每天受到外界的刺探不下于500次。

1995年9月，美国为了检验其国防情报系统的安全，举行了一次名为“联合勇士”的演习。参加演习的一名年轻上尉军官，用一台从商店买来的普通计算机和调制解调器，在众目睽睽下，几分钟之内便使自己的命令进入了美国海军大西洋舰队的指挥和控制系统，并在舰队司令全然不知的情况下控制了该舰队的一艘又一艘军舰。这位上尉没有依靠任何内线情报，仅凭自己丰富的电脑知识，便将一支舰队玩弄于股掌之间。这场不费一枪一弹，迅速有效的计算机“袭击”，震惊了美国军界。

“黑客”入侵军用计算机如此易如反掌，运用计算机知识就可以攻击敌方指挥、控制、通信等信息系统，可瞬间将敌陷于瘫痪，取得兵不血刃、出奇制胜之效，这已引起发达国家军界的严重不安，担心未来可能出现“电子珍珠港”事件。美国国家战略研究所最近指出，打信息战的手段不仅相当便宜，易于掌握和应用，而且各国都能得到。“只要投入很少的资金，任何国家或实体都可进入电子通信领域这一信息自由流动的空间”，“人人都知道使用信息战手段，信息战是耗资少，无法垄断的作战样式。”

严防“黑客”行动，加强信息安全防护，已成为世界各国日益关注的问题。1996年2月28日，五角大楼的战略情报专家正式提交了一份《互联网络评估》报告，主张美国军方对全球电脑互联网络实行监控。美国防部在1996年就开始计划投资10亿美元为所有的数据加密，以保护信息安全。中国、新加坡、西欧国家、东盟国家都相继对计算机互联网络采取了严加防范的措施。不言而喻，计算机防护专业队伍就会随之悄然兴起。

防计算机“病毒” 计算机病毒是计算机防护兵最艰难、最广泛、最隐蔽的作战对象。从1988年以色列数万台计算机遭受“病毒”攻击而被迫停机起，至今计算机病毒已发展到接近10,000种。计算机病毒可造成死机、扰乱屏幕、破坏数据、摧毁电脑软件。计算机病毒传播手段也不断翻新，令人防不胜防。它们既可以通过有线或无线电传输，也可以预先固化在敌方购置的计算机部件中，或在战时通过投射方式输入敌方电脑系统；既可以实施网络攻击，瘫痪敌方的指挥、控制、通信系统，又可实施单系统攻击，破坏敌方各种作战平台的正常运行。在未来作战中，如能成功运用电脑病毒这一武器，就可以取得不战而胜的神奇效果。美军方人士认为，“用计算机病毒进行战争，比用核武器进行战争更有效”。

众多的计算机病毒归纳起来为两类：一类是目前广泛使用的电子病毒，另一类是程序病毒。电子病毒战已成为一种重要的信息战样式。计算机电子病毒能按各种各样的需要修改和破坏敌方计算机的正常运行。它不易被发现、传染快、潜伏期长，可对敌方C<sup>4</sup>I系统和战争潜力产生毁灭性影响，是未来作战必不可

少的“软战”手段。在海湾战争中，美国特工人员将计算机电子病毒软件，悄悄装入伊拉克从法国购买的电脑打印机里，在战略空袭前以无线电遥控手段将病毒激活，使伊拉克防空体系发生混乱，导致伊军既无还手之力又无招架之功。

程序病毒是一般常理难以捉摸和鉴别的事物。它之所以令发达国家军事部门严重不安，是因为它有可能存在于任何高技术兵器之中。国际上大多数武器专家学者指出，现代武器装备的战斗性能与稳定性的高低，在很大程度上取决于程序元件(软件)的质量和可靠性。因此，程序保障已成为各类作战系统脆弱的一个新因素；军用程序元件(软件)的技术安全又成为作战保障的一个新问题。程序病毒与电子病毒相比，程序病毒一是没有直接或间接的征兆，很难查出；二是可避开敌方防护和识别系统；三是一旦被激活，将使被其侵入的军事系统彻底失灵。

防计算机“渗透” 计算机渗透，是一种用破译敌方计算机通信密码的计算机应用系统，打入敌方通信计算机网络进行侦察与破坏的军事行为。计算机渗透与计算机病毒既有联系又有区别。相同之处是均为

对敌指挥通信系统实施“内摧毁”；不同之处是计算机病毒只能对敌方指挥系统进行破坏，而不能像计算机渗透那样实施侦察。另外，计算机病毒战只有在双方网络软、硬件进行交流或接触的前提下才能发生效应；计算机渗透则不然，只要对方指挥系统开通运转，己方的密码破译系统就会自动而有效地工作，渗透到亦步亦趋的程度。由于计算机渗透不通过人的接触，而是超越时空界限，运用电子信息类比进行侦破和“打入”，因而对方反侦察系统很难发现和跟踪。

英国 16 岁少年布里顿，发明了一种名为“嗅探器”的系统。他运用该系统，通过国际计算机互联网络“渗透”进美国最敏感的计算机系统，破译了包括弹道研究报告在内的大量机密，时间长达 7 个月之久。1994 年春，当朝鲜核检查问题最为紧张的时刻，他又将破译的美国内部情报材料输入到拥有 3,500 万用户的国际计算机互联网络公布于众。美国空军用 3 个月时间对计算机系统进行安全检查时，碰上布里顿的计算机打入网络后一夜未关机退出，才得以将这位小小的不速之客“捉获”。计算机渗透是一种隐蔽性极强，令对方防不胜防的窃密手段；同时它还

可以进行破坏活动，如给敌方系统“注入”假情报和病毒等。



防计算机“杀伤” 计算机系统不仅遭受对方计算机的侦察、破坏、窃密，而且面临作战兵器的直接打击。一是武器的“硬杀伤”。如激光、微波波束等射频武器，通过天线、电源线、传输线和各种接口等导入高功率感应电流和辐射能，击穿和烧毁电子设备而使整个计算机系统被摧毁。二是武器“软杀伤”。如电子战武器中的电子干扰机和微波炸弹、激光炸弹等，通过高强度辐射场的大面积覆盖，使覆盖区域内的计算机系统内部的敏感电子元件和电子线路中某些

元器件产生错误的电流和电压，导致电脑信息丢失、出现错码、控制失灵等电路紊乱或逻辑混乱现象。

## 军队建设的双翼

西方国家有一种代表性看法认为，在工业时代，军队的基础是火力杀伤系统；在信息时代，军队的基础是信息，要打赢高技术战争，信息是取得胜利的本钱，是制胜的关键，必须借助信息这个“力量倍增器”，大力推进军队信息化建设。世界主要军事大国在军队信息化建设方面，大体做法是：

第一，确立信息战理论。基本观点是，在未来战争中将主要使用由精确制导武器、情报支援系统和电子战系统构成的信息战系统；控制“信息源”、“信息流”，夺取“制信息权”，是基本的作战指导思想。

第二，发展信息化武器装备。信息化武器装备主要包括四类：一类是信息化弹药，如制导炸弹、制导炮弹、制导子母弹、巡航导弹、反辐射导弹、末制导导弹等。第二类是信息化作战平台，即装备有大量电



子装备和信息高技术的飞机、舰艇和各种车辆等。第三类是 C<sup>4</sup>I 系统，包括战略、战役、战术级的，以及各军兵种和各部队的 C<sup>4</sup>I 系统。第四类是单兵数字化装备，如“电子头盔”、“士兵综合防护服”等。

第三，建立数字化战场。数字化战场是由通信系统、指挥控制系统、情报传输系统、计算机与战场数据库及各种用户终端组成，覆盖着整个作战空间，能给用户实时提供信息的综合互联网络系统。通过该系统，能实时获取、交换和使用数字化信息，及时满足各级指挥官、战斗人员、战斗保障人员的信息需求。为此，美军成立了数字化办公室，并将执行“信息资源标准化”和“指挥控制数字化联网”计划。

第四，组建信息化部队。主要是以“有利于信息流动”为原则，改革军队体制编制，建立适合打信息战的兵力结构；开设信息战课程，加强信息战训练，培养信息战人才等。

美军在部队信息化建设方面，准备分两步走：第一步是实现数字化；第二步是实现信息化。数字化部队与普通部队在编制结构方面没有多大区别，只是达

成通信数字化、C<sup>3</sup>I 系统一体化、武器装备智能化和作战系统网络化。经论证认为，数字化部队的作战效能约为一般部队的 3 倍。美军计划 2010 年陆军部队全部实现数字化，并于 1997 年 10 月起，选择拟定方案进行实验，目前已完成数字化军一级的模拟实验。

第五，开设信息战课程。为了掌握今后可能发生的信息战之主动权，美国陆海空军和海军陆战队各兵种都设立了信息战办公室，加紧研究现代信息战争。1994 年 8 月开学的首批 16 名信息战军官，于 1995 年 6 月从华盛顿州的国防大学毕业。美国国防大学校长塞尔姜中将认为：“信息时代的情况是与过去截然不同的，它对领导艺术提出了一系列新的挑战”。“国防大学已意识到这一挑战，因而面向未来，正寻求在 21 世纪战争中克敌制胜的答案，目前的关键措施就是进行信息战教学”。信息战教学的重点放在作战方面，而不是信息管理方面。所开设的信息战课程，是信息管理学在研究海湾战争的成功与不足之后所建立的信息战学科，不仅从信息的角度教授传统科目，而且还设置了非传统科目；授课方法也非

常独特，接受了从对抗计算机入侵到利用虚拟现实技术进行模拟战斗等各种五花八门的训练。主要教学对象是培养高级军官和地方领导人；主要培养目标是能通晓 21 世纪作战、能够胜任联合参谋业务的军官。

尽管明确提出建立信息化部队的，目前还只是美国等少数发达国家，其他国家也还没有明确提出数字化概念，但事实上都在计划开发和利用计算机技术和信息技术，大力发展 C<sup>3</sup>I 系统，因而实际上也在实施军队信息化建设。

### 联合作战中的电子战

美军认为，现代战场上，有效的电子战行动是保证取胜的关键途径。美国陆军 FM—31—1 号野战条令中明确指出：“成功地执行情报与电子战任务是空地一体战场的关键”。在以往的多次高技术局部战争电子战战例中已经证实，电子战不仅是一种战斗支援手段，而且还是一种对敌的“软杀伤”手段。为此美军非常重视联合作战中的电子战行动。

联合作战时的电子战原则：美军认为，在联合作战时，除了要具有较低一级的电子战工作的原则外，还必须有适应联合司令部电子战组织、任务和行动的原则。统一进行情报分析综合，而不能把空中、地面和海上部队的情报分开处理；把联合情报与电子战工作纳入整个情报与电子战体系，以便更有效地使用各种资源；集中进行情报与电子战支援；进行平时转战时的训练，使平时的计划、活动和训练能迅速转入战时状态；保持并不断地更新情报与电子战数据库，在情报与电子战工作中，采用自动数据处理。

美军认为，它的大多数作战都是在联合条件下进行的，因此要根据联合作战的具体情报来对情报和电子战原则进行调整。为了有效地协调地工作，联军部队应以下列原则进行电子战：建立联军情报与电子战体制；建立传递情报与电子战资料的渠道；制定标准的电子战工作程序；发展安全可靠的通信能力；确保通晓多种语言的能力；建立联军情报与电子战部队之间的联系；建立共同数据库。美军认

为，按照上述原则，就可充分发挥各军种和联军的电子战能力，通信兼容，情报与电子战共享。

## 信息战中的电子战

在 80 年代以来的几场局部战争中，表现出的海陆空天一体电子战，显示了一些信息战的端倪，并日益向更为深入、广泛的方向发展。仅就空中战场而言，未来空中力量装备的大量电子战飞机，对战略战役 C<sup>3</sup>I 系统具有大功率、全频段、大空间的“软杀伤”能力和对作战体系关键节点的“硬摧毁”能力，在很大程度上将决定战争的进程和结局。据有关专家研究，北约只要在波罗的海至亚得里海约 2,000 千米的正面设置 5 个干扰空域，使用 EF-111 电子战飞机对东欧国家进行电子压制，就可以瘫痪其指挥控制系统。海湾战争中，多国部队首先进行了长时间的空地一体电子战；首次空袭中，使用 F-117 隐形战斗机和“战斧”式巡航导弹摧毁了伊拉克的战略战役 C<sup>3</sup>I 系统的主要节点，在战略空袭战役阶段，共出动 1,466 架次，对伊拉克国家指挥当局、

防空设施和指挥、控制、通信设施进行火力突击，从而破坏了伊拉克的战略战役 C<sup>3</sup>I 系统结构，一举夺得制电磁权、制信息权和战争主动权，为最后的胜利奠定了坚实的基础。面对现代局部战争的一系列现实的挑战，世界各国开始研究其新的作战方针、原则与军队编制、体制等各方面存在的差距与不足，一场新军事革命的挑战正迎面逼近。

世界掀起研究信息战理论的热潮 当前，一场新的军事革命正在世界上以空前的深度和广度进行，而信息战则是这场军事革命的核心内容。近年来，美、俄、英、法、德、日、澳大利亚以及印度等国家的军队，都在大力研究信息战理论，积极准备实施信息战。其中，美军对信息战的研究更为深入，对实施信息战的准备也比较充分。

1976年，美国军事理论家汤姆·罗那在为波音公司写的一份题为《武器系统与信息战争》的研究报告中，首次提出了“信息战争”的概念，并指出“信息战争”是“决策系统之间的斗争”。从20世纪80年代以来的几场局部战争中，各国军事理论家敏锐地觉察到“信息因素”在战争中的作用日益重要

。1984年美军开始使用“信息战斗”的术语。1985年，美海军电子司令部副司令小阿贝·加洛塔少将在美《电子防御杂志》上发表了题为“电子战与信息战”的论文，他在此文中呼吁，鉴于电子战的内涵现已扩展到保护己方的决策能力和攻击敌方的决策能力，因此用“信息战”这一术语取代电子战更为合适。根据海湾战争信息化作战的初步实践，1994年1月，美国防部长佩里下令成立“军事指导委员会”，以指导各军种深入研究信息战的主要特征、战场信息环境及基本原则，并论证试编“联合信息军”的问题。1995年1月，美国防部成立“信息战执行委员会”，以确立国家信息战目标，制定信息战的有关政策。负责美军信息战理论与实践的领导机构——美军参谋长联席会议，于1996年颁发了有关信息战的四个文件：《2010年联合构想》、《参联合主席第3210·01号指令：联合信息战政策》、《参联合主席第6510·01号指令：防御信息战的实施》和《信息战：应用的观点》的小册子。《2010年联合构想》是在信息时代指导三军联合作战的纲领性文件，它提出的“制敌机动”、“

精确作战”、“全维保护”和“精确后勤”这四项作战原则的实施都依赖于信息优势。其他三个文件则强调防御信息战和信息战战法。美国陆军一贯重视信息战研究，认为信息优势是未来战场的制高点，把提高信息战能力作为推行“21世纪部队”计划的主要内容。1996年8月，美国陆军部颁发了《FM100—6：信息行动》条令，提出了陆军部队实施信息战的原则、方式与程序。陆军1998年版的《作战纲要》把作战环境划分为物质、信息与精神三个领域，认为信息领域的信息作战是打赢未来战争的主导作战方式。

俄罗斯军方也正把研究目光投向信息战和信息战武器。这类信息战武器主要是获取或者反获得信息的手段，即无线电电子斗争手段——对侦察、监视、追踪、联合、指挥和控制有极大影响的无线电电子对抗和无线侦听，以及对传统的最新的高精度武器(使用各种射线)进行干扰和压制干扰。这也是未来信息战武器的最重要组成部分。因此，研究信息战武器的实质就是要研究电子战武器。他们进一步论证说，近年来的局部战争经验充分证明，大规模地协调使用电子



战手段，就可以破坏敌方对其军队和武器的指挥与控制，扰乱敌可靠的信息环境，从而夺取信息战的胜利。还有一种大有前途的信息战武器，那就是破坏和反破坏电子计算机软件系统的特殊方法。这些方法的效用只有大规模毁伤性武器才能够与之相比。为此，俄罗斯正在确立未来新军事技术政策的重点，首要的两条，就是研制与改进高效能武器系统、电子战系统，以及研制与改进指挥、侦察和通信技术系统，并使之智能化。并将微电子学、光学、人工智能系统、电子系统、计算机、雷达等 10 项基础研究发展计划确定为“关键防御计划”。

信息战产生于人类技术社会形态由工业社会向信息社会过渡期，其社会属性是信息社会，亦即它是信息社会的作战样式。信息战的技术基础是信息技术。就信息战的概念或定义而言，在目前信息战理论与实践都还不是非常充分的情况下，世界各国的不同人士对信息战的内涵都有着不同的认识和理解。但随着新军事革命的深入发展，外军对信息战的范畴及其相关概念也有了更明确的认识，更合理的区分，比如美国国防部认为：“信息战是通过影响敌方信息系统，运

用己方信息和信息系统，来取得信息优势，以支持国家军事战略的行动”。



信息攻防战第一次登上战争舞台 在海湾战争以来的历次局部战争和武装冲突中，争夺制信息权的斗争一直都贯穿战争的始终。每次美国都能以绝对优势的力量使对手只有招架之功而无还手之力，从而牢牢掌握战场的制信息权。然而，在 1999 年上半年爆发的科索沃战争中，南联盟虽然在硬打击手段方面处于绝对的劣势，无法攻击北约的信息系统，但利用软手段也给北约造成了不小的麻烦。自开战以来，以南通社为组织中心，专门开设了以“科索沃危机”为专

题的网址，宣传南联盟进行的反侵略战争，发动电脑专家以互联网为媒体，向北约组织发动计算机网络战。3月31日，北约发言人谢伊称，自从北约开始对南联盟实施空袭以来，北约的信息系统便连续遭到南联盟等国电脑“黑客”的网上攻击，致使北约部分计算机系统的软、硬件遭到电脑“病毒”的重创。更有消息说，由于受到“黑客”的攻击，美国白宫的网络服务器在3月29日全天无法工作。英国等欧洲国家的一些有关网站多处遭到破坏，北约轰炸行动中依赖性最强的英国气象局网站损失惨重。不仅如此，“黑客”还通过注入“梅莉莎”、“疯牛”等病毒，造成了4月4日北约军队的一部分计算机信息通信系统瘫痪，美军在互联网上的一些电子信箱被阻塞等。这一切表明，信息攻防战已成为双方的另一个战场。

信息作战与电子战的关系 信息作战和电子战同属军事范畴，同在作战领域，两者既有密切的联系，又有很大的区别，甚至是性质上的区别。

两者的联系表现在：电子战是信息作战的“发源地”，信息作战是电子战发展的产物；信息作战涵盖了电子战，电子战则是信息作战的关键部分和核心内

容。同时，两者也有明显的区别，主要有四点： 作战目的不同 。 电子战的目的是争夺制电磁频谱权，而信息战则以夺取和保持制信息权为己任； 作战空间不同。电子战主要在电磁空间进行，而信息战却在比电磁空间大得多的信息空间实施； 作战对象不同。电子战的作战目标是敌方的各种电子设备，信息战的作战目标除此之外，还包括各种信息系统、打击兵器、信息本身的决策者的认识与信念； 作战手段不同。电子战进攻手段主要有电磁干扰、定向能武器攻击、反辐射武器攻击和电磁欺骗等，而信息作战的攻击手段既包括上述电子战手段，也包括远程精确打击、“黑客”攻击、计算机病毒攻击、电磁脉冲武器攻击，以及心理战、情报战、“虚拟现实”战等。

总之，信息作战与电子战不仅有很大不同，前者无论在内涵还是在外延方面，都要比后者丰富得多，广泛得多，影响大得多，而且它们之间本质的区别是，电子战是工业时代军事形态的一部分，而信息作战则属于信息时代军事形态的范畴，比前者又提高了一个层次。

## ● 少年国防教育丛书

神圣的疆域

华夏兵家要地

世纪大阅兵

论剑亚细亚

水下杀手

陆战霸王

蓝天武士

## ● 寂静的战场

战争之魔

看不见的战线

ISBN 7-5324-4314-0



9 787532 443147 &gt;

ISBN 7-5324-4314-0/N·522(儿)

定 价:

8.00元