“信息战条件下电子战技术与装备的发展”和
“特殊体制雷达及其对抗技术”研讨会

论 文 集

电子对抗专业情报网
一九九八年九月 • 烟台

前　言

近几年来，国内外军事技术专家对信息战/电子战（IW/EW）的内涵及其发展进行了热烈了讨论。IW/EW 已无可置疑地成为新军事革命的焦点。研究电子战与信息战的相互关系，电子战在信息战中的地位和作用，以及电子战在未来数字化战场中的使用问题。必将促进具有中国特色的 IW/EW 的发展。

本文集收集了 IW/EW 方面的论文，可供深入研究电子战、信息战同行参考。本文集同时也收录了有关雷达和雷达对抗、通信和通信对抗方面的新技术、新设想的文章，可为电子战技术研究人员提供一些有益的启示和帮助。

本论文集共收录了 32 篇论文，诚挚地感谢电子对抗专业情报网内各成员单位、联络员和论文作者的大力支持和协助，为促进网的学术交流活动做出了贡献。

编　者

1998 年 8 月

目 录

信息战的新发展

林 峥

北京 750 信箱 邮编 100039

〖摘要〗本文分别论述了信息战的基本涵义及其发展过程以及未来战争信息网络系统与计算机系统信息战的发展.

【关键词】信息战 电子计算机对抗

一、信息战的基本涵义

信息战是敌对双方在信息领域里进行的战斗，是己方为夺取战场信息的获取、传递、分析、处理和使用信息的控制权，即夺取“制信息权”；同时干扰破坏敌对方信息的获取、传递、处理和使用信息的能力所进行的信息斗争。

美国陆军于 1996 年 8 月 27 日颁布的野战条令 FM100-6 在“信息作战”中，对信息战作了如下定义：“信息战是为了影响敌方的信息、信息处理、信息系统和计算机网络；同时保护己方的信息、信息系统和计算机网络，而获得信息优势所采取的各种行动”。

美国国家军事战略认为信息战是美国诸多军事能力的组成之一。其目标是夺取信息优势，使整体力量迅速优于并控制敌军。其战略目标是通过利用、阻止和影响行动，攻击敌方国家信息基础设施，同时保护己方的信息系统，夺取并保持决策的优势。

从信息战的定义和内涵来看，信息战就是敌对双方使用信息战装备，侦察和干扰破坏敌方信息系统与装备，同时保障己方的信息系统与装备不受干扰和破坏，而获得信息优势所展开的信息斗争。

二、信息战的发展过程

信息战起源于通信对抗战。无线电通信发明之后，装备了军队作战使用，从而导致了侦察干扰破坏通信正常工作的通信对抗战的出现。最早可以追述到 1905 年 5 月的日俄“对马海战”，日本联合舰队与沙皇俄国舰队在日本的对马海峡，展开了一场大规模的海战，战斗前日本使用无线电侦察设备侦收到了俄国舰队的无线电通信信息，而在俄国舰队航线上设伏，在战斗中日军使用了无线电通信干扰，使俄军舰队无法联络和指挥作战，在日军舰队攻击下只能四散溃逃，被各个击破。俄军 19 艘军舰被击沉，7 艘军舰被俘。伤亡 11000 人，俄舰司令罗津斯特文斯基受重伤，并成了日军的俘虏。此后，通信对抗装备技术得到了迅速的发展。

第二次世界大战中，雷达在战争中的应用，特别是警戒雷达和炮瞄雷达在战争中发挥了重大的作用，给作战飞机带来了严重威胁和损失，而导致了雷达信息对抗战的发展。无线电与光电信息制导武器的发展和应用，对现代战争带来了新的威胁，从而又促进了侦察干扰破坏这些精确制导武器的信息战发展。雷达信息对抗和制导武器信息对抗，在越南战争和中东战争中发挥了巨大作用。如在越南战争期间，越南人民军使用了苏制 AS-2 地空导弹，击落了大量美军飞机，开始给美军飞机带来了严重威胁，后来美军大量使用了信息侦察和干扰装备，使美军作战飞机的损失率由越战初期的 14%，下降到战争后期的 1.4%，大量减少了作战飞机的损失。又如，在第三次中东战争的海战中，由于以色列舰艇上没有信息战装备，战斗中埃及海军导弹快艇向在地中海上的以色列“艾拉特”号驱逐舰发射了 4 枚苏制的“冥河”式反舰导弹，一举击沉了“艾拉特”号驱逐舰，使西方军事家大吃一惊。此后，以色列总结了经验教训，大力研制对付反舰导弹的信息侦察干扰装备和对抗措施，而在第四次中东战争的海战中，埃及和叙利亚的导弹快艇向以色列舰艇发射了 67 枚“冥河”式反舰导弹，由于以色列采取的有效的信

息对抗手段，而无一枚导弹命中，说明信息战在反信息制导武器方面的重大作用，从而促进了制导武器信息对抗战的发展。

C^3I 系统的发展，对现代战争带来了新的威胁，从而又导致了侦察干扰破坏 C^3I 系统的 C^3ICM (C^3I 对抗)信息战的发展。典型的战例是 1991 年 1 月的海湾战争，战前美国首先采用了各种信息侦察手段，详细掌握了伊拉克 C^3I 系统的情况，而战争一开始首先采用了强大的信息干扰手段，干扰破坏了崛伊军的 C^3I 系统,使伊军的整个军事作战指挥、控制、通信和情报系统瘫痪，而使伊军完全处于被动挨打的地位，显示了信息战在现代战争中的威力和作用。

现代信息技术与计算机技术的飞速发展，促进了军事信息系统与信息化武器装备系统的发展，对现代战争又带来了新的威胁，进一步促进了对抗军事信息网络系统和信息化武器装备系统的信息战新发展。由于电子计算机在信息网络系统和信息化武器装备系统中的广泛应用，从而采取干扰破坏这些系统中计算机工作的计算机对抗战已经成为目前信息战发展的重点之一。

从以上所述的信息战发展过程可以看出，信息战是从无线电通信对抗、雷达对抗、导航对抗、敌我识别对抗、信息制导武器对抗、C^3I 对抗、C^4I 对抗发展到了目前的有线电网络和无线电网络与计算机系统新的信息战。

三、未来战争信息战的新发展

（一）信息网络系统上的信息战

信息战从无线电信息对抗战开始，发展到了有线是网络信息对抗战。过去的信息侦察和信息干扰都是在无线电信息范畴进行的，有线电信息网络是难进行侦察干扰破坏的，现代信息技术与电子计算机技术的飞速发展，促进了军事信息网络系统和全球信息网络系统的发展。如美国的全球通信、指挥、控制系统和国际互连网络

（Intcret 网） 等，对于军事、政治、经济都产生了重大影响。因此，在未来的战争中，敌对双方都要千方百计的侦察干扰破坏敌方的信息网络系统，使它工作失效和瘫痪，从而促进了信息网络系统上信息战的新发展。

现代信息网络系统，包括无线电信息网络系统和有线电信息网络系统所构成的综合信息网络系统。在现代战争中，若信息网络系统遭到信息战的信息侦察干扰破坏，对于作战的胜败将产生重大影响。例如，在海湾战争中，美军使用了强大的信息战侦察干扰装备与作战手段，侦察干扰破坏了伊军的雷达、通信、导航、敌我识别系统和作战指挥控制系统，使伊军的雷达迷盲、导航迷向、敌我识别系统失效、武器系统失控、通信中断、指挥失灵，造成伊拉克军队被动挨打的地位。

在海湾战争中，美军主要依靠全球军事信息系统在美国防部五角大楼指挥海湾地区的美军作战，由于伊拉克军队缺少现代先进的信息战装备与作战手段，使美军能顺利完成指挥作战任务，以很小的伤亡取得了大的胜利。如果伊拉克军队掌握现代先进的信息战装备，能够侦察干扰破坏美军的通信指挥控制系统与武器信息系统，使美军的雷达迷盲、导航迷向、敌我识别失效、武器系统失控、通信中断、指挥失灵，美军就不会轻而一举的取得胜利，甚至最后可能以失败告终。

现代信息战特别是信息网络系统与计算机系统方面信息战的发展，将对未来战争带来新的威胁，由于美军远离国土去海外作战，特别是指挥海洋舰队和航空母舰作战，完全依靠全球军事信息系统进行作战控制与控制，若遭到信息战的侦察干扰破坏，其作战就会处于瘫痪状态，从这方面看来，美军最害怕的是信息战，所以强调信息战的作用，重视信息战的发展。

在信息网络系统的信息战方面，美国重点发展全球信息网络对抗系统，侦收、截获、窃取别国的各种军事、政治、经济等信息情报。与此同时大力研究自己信息网络系统的信息防护技术，以防敌

方侦收、窃取或干扰破坏。另外由于电子计算机在信息网络系统和武器系统中广泛应用，所以研究干扰破坏计算机系统，已成为网络系统信息战发展的重点。

（二）电子计算机系统上的信息战

电子计算机系统信息战，就是干扰破坏敌方电子计算机系统，使它不能正常工作或完全失效；同时保障己方计算机系统不被敌方干扰破坏所进行的斗争。因此，计算机信息对抗战仍然是电子计算机干扰和反干扰的斗争。

1、 计算机干扰技术

目前计算机干扰主要有以下几种类型：

（1）计算机病毒干扰(Computer viruses interference)

计算机病毒实质上是一段程序，通过这段程序修改和破坏其他程序。即把自身的拷贝嵌入到其他程序，而实现对计算机系统中的程序进行传染，引起计算机系统或网络系统的紊乱。甚至造成计算机系统工作的瘫痪。这种计算机病毒干扰具有很大潜在破坏性。美国专门组织了一些这方面的人才，从事计算机病毒干扰和反病毒干扰研究工作。

（2）“逻辑炸弹”(Logic bombs)

逻辑炸弹是由计算机系统开发研制者或程序研究人员专门在计算机系统内部埋置的一段独立程序代码，在一定的条件下触发它，可以由隐蔽功能激活它，也可以由外部一定频率的高功率微波触发它，像“定时炸弹”一样在某一关键时刻破坏计算机系统的工作。因此，对于购买外国或敌对国家计算机系统的落后国家，在未来战争中，有可能遭到逻辑炸弹的攻击。

（3）“蠕虫”干扰(Worms interference)

蠕虫干扰是一段独立的程序，通过自我复制方式，从计算机系统和网络上的一台计算机扩展到另一台计算机，造成计算机系统和网络系统的紊乱。它和计算机病毒子扰不同之处是蠕虫干扰程序不

传染修改其他程序。

（4）易损芯片(Chipping)

在计算机使用的集成电路芯片中，设计制造使用一些容易受损功能芯片。例如，其芯片在使用某一段时间之后功能变异或者在接受到某一特定频率时自段。这种易损芯片，对于购买外国计算机和先进武器系统的落后国家来说，将带来严重后果与威胁。

（5）高功率微波干扰(HMP jarmming)

高功率微波束照射到计算机系统和网络时，能使计算机系统功能产生混乱、出现误码、中断数据与信息传输、抹掉计算机记忆信息等现象，甚至可以烧毁电路中的芯片。因此，高功率微波干扰，仍然是对计算机系统带来最大的威胁。

（6）计算机“黑客”(Computer hackers)

所谓计算机“黑客”是指非法闯入计算机系统查看、修改或偷窃保密数据和程序的人称为“黑客”。

黑客是对计算机系统与计算机编程非常熟练的人，能使用各种手段，例如，口令猜测，指令破译、自复制代码、密码破译、使用扫视器、嗅探器、隐秘诊断、并以统计方式识别出计算机系统单元安全弱点来攻击计算机系统和网络，这种计算机对抗战的威胁将日益严重。

据美国有关报告统计，近年来美国国防部信息网络计算机系统受到外来袭击日益增多，1992 年发现有 53 次，1993 年有 115 次，1994 年有 225 次，1995 年达 559 次，而据国防部信息系统局统计，1995 年实际受到袭击的次数可能多达 25 万次，因为绝大多数的袭击是很难被发现的，更难作出有效的反应。据国防信息系统局对国防部计算机系统进行了 3 万 8 千次模拟袭击表明，成功率达 65%，而被发现概率只有 4%，能作出积极的防御反应的还不到 1%。据美国防部官员称，袭击者通过窃取情报、修改或破坏软件和数据、输入有害文件或病毒等手段，可以严重影响国防部的正常工作，美国防部的军事指挥与控制、军事计划与研究、后勤和其他军事作战

信息系统都存在脆弱性，在未来战争中很容易遭到干扰破坏，严重威胁国家安全。

2、 计算机反干扰技术

计算机反干扰也可称计算机防护，目前主要有以下几种方法和措施：

（1）为确保计算机系统安全，免遭“黑客”入侵，采用各种用户身份鉴别技术

过去一般常用的方法是口令鉴别，但容易被窃听者获得口令，所以是不安全的。目前采用比较先进的方法是密钥身份鉴别技术，其中包括三个相互作用的服务器。

A．鉴别服务器(Authentication Serves)

它可以对客户进行最初鉴别。一般是在客户注册时发给的一张密钥加密的许可证，在接到客户使用请求时，经过鉴别服务器进行鉴别，证实客户身份。

B．权限服务器件(Privilege Serves)

它可证明客户的权限，这权限包括客户的专用主标识符号和客户所在群体的专用标识符号，并在许可证上密封这个权限。在接到客户使用请求时，客户必须向许可证授予服务器提供自己密钥加密的许可证，并通过权限服务器验证。

C．许可证授予服务器()Ticketgranti Serves)

它可以向计算机系统中的所有服务器发出经过检测鉴别的许可证。客户进入计算机网络系统时，必须经过以上三种服务器同时进行互检测鉴别，确保信息网络系统的安全。

(2)为了防止计算机系统的信息资源被破坏，采用各种数据完整技术和恢复技术

保证数据的完整性是计算机系统安全的基本要求之一。即在数据处理、存储、传输过程中保持不被修改、不被破坏、不被丢失，而对任何修改与破坏都能发现和及时纠正，如有破坏要采用恢复技

术，使数据准确完整，包括必要的拷贝和异地安全存放等。

(3)为了防止计算机病毒干扰，研制各种防病毒卡

根据各种计算机病毒和传染方式，研制各种防病毒卡，发现病毒可及时清除病毒。另外计算机系统的硬件和软件，都要自力更生，自行研制生产，不要购买外国的硬件和软件，免遭病毒的干扰破坏。

（4）确保计算机系统的安全，要建立计算机内部网络与外界网络隔离开来的“防火墙”

“防火墙”是一种用来阻挡外部信息非法入侵和影响内部网络的安全屏障。它是一个或一组网络设备，用来在一个或多个网络间加强访问控制，对外部网络与内部网络交流的信息进行检查，符合的予以放行，不符合的则拒之门外或不让出来，以防止病毒与黑客的入侵。

（5）重视计算机系统加固技术研究

高能微波武器的发展，将给计算机系统带来新的严重威胁。因此，在研制计算机系统的元器件和芯片时，要重视抗毁加固技术的研究，确保计算机系统与武器系统在未来战争中的安全。

信息战背景下电子战的发展特点

全寿文

总参第五十四研究所 北京 10083

〖摘要〗在当前战场不断向信息化方向发展、信息战理论正在逐步趋于完善的形势下，本文分析电子对抗与信息战的相互关系，探讨电子对抗在信息战中的作用和地位，总结电子对抗的发展方向、发展特点以及未来电子对抗的作战重点。

【关键词】电子对抗 发展趋势 信息战

0、引言

随着电子技术的发展，由信息获取技术、信息传输技术和计算机技术构成的信息技术推动社会向信息化方向发展。信息技术的迅猛发展和广泛应用子军事领域，增加了军队对信息、信息系统的依赖性，引发军队对信息、信息系统控制权的争夺，由此引起了一场以信息战为特征的新军事革命。信息战的发展对传统的电子战提出了更高的要求，开辟了新的领域，提供了更广阔的空间：在信息战背景下，要求电子战在更大的范围内运作；信息技术的不断发展，要求电子战不断发展新的技术和手段；未来数字化战场上电子对抗作战

目标繁多，要求电子战具有多功能一体化，具有综合对抗能力。信息战作战理论的出现，对电子战的发展产生了较大的影响。

1、电子战与信息战的关系

1.1、 信息战是在电子战的基础上形成和发展的

从信息战的出现和发展来看，军事领域的信息战是在以电子技术为支撑的电子战的基础上发展起来的，其主体仍然是电子战。信息战是在人们对电子战认识不断深入，对电子战理论不断丰富的基础上产生和发展起来的，是电子战的高级阶段。电子对抗最初强调的是单个设备之间的对抗。随着科学技术的进步。特别是近二十年来信息技术的迅速发展，以及军队武器装备的信息化趋势，指挥．控制、通信、情报及计算机等信息系统的发展和在战场上的广泛应用，使各个原先分散使用的武器装备构成了统一的作战整体，电子战也从单个设备的对抗转向系统和体系之间的对抗，并强调综合运用多种手段，包括心理战等因素，才能达成攻击的最大效能，从而产生了 C^3 对抗和 C^2 战的概念，为信息战的产生奠定了基础。从理论上看，美军首先从“电子战”发展成为“指挥控制战”，然后再演变成为“信息战”。从目前信息战机构形成情况看，美国的信息战机构大多是由原来的电子战机构改编而来，人员也主要来源于电子战机构，美军认为，信息战与电子战最为相近．由电子战人员来进行信息战具有许多优势。正是海湾战争中多国部队电子战的有效实施，使人们透过电磁领域的这场斗争，逐渐总结出了信息战理论。

1．2 电子战不断向信息战领域扩展

随着电子技术尤其是信息技术的发展，电子战的范畴不断扩大，广泛渗透到各个军事领域，作战对象也从过去的雷达和通信设备扩大到了各种电子系统，作战任务从破坏敌人

和保护自己的情报收集能力和指挥控制能力等，扩大到了破坏敌人和保护自己的信息收集、传输和指挥决策过程。信息战是电子战的发展趋势。

1.3、电子战将是信息战的主要作战方式和手段

随着信息战作战理论的出现，电子战将在信息战中发挥重要的作用，并将成为信息战的重要作战手段。现代战场上信息绝大部分都以电磁能为媒体，处于电子战频率覆盖范围之内。信息战中的信息伤害主要表现为欺骗性伤害、饱和性伤害、污染性伤害、干扰和瘫痪敌方的信息系统、打入敌方信息系统等。而电子战是以敌方的电磁信息设备为主要作战目标的，是对敌信息系统、信息化武器网络的攻击，它包括电子干扰、反辐射攻击、定向能武器攻击和计算机病毒攻击等。可以看出，担负信息战攻击的武器装备其核心部分是电子战装备。电子战武器装备将是信息战武器的主要组成部分，信息战作战手段中电子战武器都不同程度地发挥作用。电子战的作战形式具有信息战的性质，它是信息战在电磁、光电等领域的表现形式。

归纳起来，电子战的发展为信息战的产生奠定了基础．电子战是信息战的核心内容；信息战是电子战的高级形式，是电子战的扩展和升华；电子战是信息战在电磁频谱领域的表现形式，是信息战实施中的一类具体战斗行动。

2、强调制信息权，重视信息获取能力

信息战是以争夺制信息权为目的的作战。在科学技术高度发达的今天，信息已成为一种新的战斗力要素，而且是现代高技术军队作战能力的第一要素，现代战争实质上是信息与火力结合的战争，夺取信息优势是控制战场主动权的关键，谁能在战场上首先打击敌方和瘫痪敌方的信息系统，瘫痪敌方的指挥控制，并保证己方信息系统正常工作，谁就能夺取战场的主动权。信息获取能力是夺取信息权的前提条

件，也是形成信息威慑的重要条件之一。电子对抗侦察是信息获取的重要手段。在信息战环境下，对电子侦察能力要求更高：电子侦察手段更多，包括陆、海、空、天的全方位侦察；侦察频域更宽，侦察频段要求覆盖所有电磁频域，包括微波、红外等等；侦察对象更广，除了对战场上使用的所有电子设备实施电子侦察外，还需要对民用电磁信号进行侦察；全时段侦察，电子对抗侦察在平时和战时都要开展，侦察手段和形式相同，只是强度不同，平时为战时服务。因此，在信息战背景下，未来电子对抗侦察将在全方位、全时段、全频域、采用多手段全面展开。

3、信息战背景下，电子战更具有全民性

信息战作战理论的出现，给国家安全战略带来了新的内容。信息战是以信息武器和信息系统为主要内容的作战，涉及整个国家的信息系统，相应地，为对付信息系统的电磁目标，电子战作战领域也不断扩大。电子战的首要目标是敌对国的整个C⁴I系统，包括金融、通信等涉及国家安全的系统，信息系统集中的城市将成为双方对抗的重要战场；电子侦察、电子进攻的目标将更多地包括民用设备；由于信息传输、互联网络、多媒体等技术的发展，为更多的非军事人员参与战争提供了条件，因此电子战作战人员中除了军事作战人员外，将更多地依赖民事作战人员的参与。因此，信息战既是军队作战的手段，又是国家战略的威慑手段。

4、在完善电子侦察手段的同时，侧重信息防护能力

信息战与常规战争一样包括进攻和防御两方面，而信息威慑的存在主要是基于信息网络的脆弱性和信息安全的重要性。但过去包括美国在内，世界各国在对信息战的理解和落实过程中对信息战防御的研究重视不够。近年来美国国防部的信息系统一再受到“黑客”的入侵，使信息的安全问题逐

渐引起人们的重视。他们感到，要想在未来赢得信息战的胜利，就必须首先保护好自己的系统，只有保证己方的信息系统畅通无阻，才有能力和机会进攻和破坏敌方的信息系统，取得信息优势。美国越来越担心会受到信息战的攻击，积极研究信息战的防护措施：（1）各军种普遍采用“红色小组”方法检查各自信息系统的安全性，即邀请一个经过特殊训练的“黑客”对某一计算机系统进行攻击，以检验计算机网络是否安全可靠；（2）空军重点保护基地信息网络，有报道说空军在1996～2001财年将花费1.2亿美元来研究对抗信息战攻击的预防性措施，并将所有的基地系统用光缆连接起来，通过107个基地网络控制中心监控所有的指挥、控制、通信、计算机和情报活动；（3）美国空军组建第609信息战中队进行防御性信息战；（4）美国陆军制定信息战安全计划；（5）海军也在研究信息战攻击的对抗措施；（6）国防部增加经费保护信息系统安全。

5、要求电子战作战手段多样化，作战功能一体化

随着数字化部队的建设和发展，电子战的作战目标不断增加，并将遍及整个战场，而且目标类型繁多，所以信息战环境下，要求必须具备很强的电子战能力和多种电子战手段。在对抗目标上从通信对抗、雷达对抗、光电对抗向指挥控制、引导和遥感、遥测对抗等多种领域扩展；在对抗手段上将从传统的有源干扰、无源干扰和反辐射摧毁向更广泛的非杀伤性领域扩展，包括定向能武器、电磁脉冲武器、计算机病毒等，加强电子进攻能力。

由于电子战作战空域、时域和频域的扩展，并且渗透到高技术战争的各个领域、贯彻战争全过程，因此，在未来信息战中，需要将各个领域、各种手段的电子对抗设备通过自动化系统融为一体，在作战行动中进行一体化的电子对抗行动，这既是信息战的必然要求，也是电子战自身发展规律所