雷达电子战原理

张永顺　童宁宁　赵国庆　编著

国防工业出版社
National Defense Industry Press

雷达电子战原理

张永顺　童宁宁　赵国庆　编著

国防工业出版社

·北京·

图书在版编目(CIP)数据

雷达电子战原理/张永顺等编著. —北京:国防工业出版社,2006(2006.3 重印)

ISBN 7-118-04216-1

Ⅰ. 雷… Ⅱ. 张… Ⅲ. 雷达对抗—理论 Ⅳ. TN974

中国版本图书馆 CIP 数据核字(2005)第 124604 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100044)

新艺印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 17½ **字数** 403 千字

2006 年 3 月第 2 次印刷 **印数** 3001—5000 册 **定价** 28.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)68428422 发行邮购:(010)68414474

发行传真:(010)68411535 发行业务:(010)68472764

前　言

本书由“军队 2110 综合电子战”学科建设项目资助出版。

电子战作为指挥控制战和信息战的关键要素和手段，在现代战争中具有重要的作用和意义。随着军事电子技术的发展，电子战的内容和作战方式发生了重大的变化，电子战已经从防御性的行动发展为既有防御性又有进攻性的电子作战行动，从只有软杀伤手段发展到既有软杀伤又有硬杀伤的复合手段，从单个系统的对抗发展到系统对抗和体系对抗，目前电子战已成为决定战争胜负的重要因素。

新电子战定义将电子战划分为电子支援、电子攻击和电子防护三大部分。电子支援指在指挥员授意或直接指挥下对有意或无意的电磁能辐射源的搜索、截获、识别和定位的行动。电子攻击指使用电磁能或定向能，以削弱、压制或瓦解敌方作战能力为目的，对人员、设施和设备的攻击。电子防护指采取行动保护人员、设施和设备，防止敌方利用电子战削弱、压制或瓦解己方战斗力。电子战新定义包含了目前电子战领域的所有内容，同时反映了电子战的作战形式。

雷达电子战是电子战的重要内容之一，主要指雷达领域的各种电子战战术和技术。雷达电子战的作战对象包括预警雷达、目标指示雷达、制导雷达、火控雷达以及无线电引信等，其技术体系主要包括雷达电子侦察、雷达电子干扰、雷达反辐射攻击、雷达电子防护和综合雷达对抗技术等。

本书将按照新定义的电子战分类进行章节的安排，包括四章内容。第一章主要介绍电子战的基本概念、雷达电子战的基本内容、电子战的历史与教训；第二章介绍雷达电子支援的基本原理和技术，包括雷达侦察概述、侦察的作用距离、对雷达信号频率的测量、对雷达方向侦察的方法和技术、对雷达定位的方法和原理；第三章介绍雷达电子攻击的基本原理和技术，包括对雷达电子攻击的基本概念、干扰方程及有效干扰空间、对雷达的有源干扰、对雷达的无源干扰、对雷达的杀伤性压制、对雷达的隐身技术；第四章介绍雷达电子防护的基本原理和技术，包括雷达反侦察技术、雷达抗干扰技术、导弹武器系统抗干扰技术、雷达对抗反辐射导弹技术、雷达反隐身原理。本书可供电子对抗专业本科生使用，也可供相关专业研究生作为教学参考。

本书由空军工程大学张永顺教授、童宁宁教授和西安电子科技大学赵国庆教授共同编写完成。空军工程大学戴国宪教授审阅了全书并提出了许多宝贵意见，博士研究生李兴成、孙宏伟、薛晓峰、杜刚等在本书编写方面作了大量的辅助工作，在此表

示感谢。

由于雷达电子战涉及到多个学科领域，其技术发展日新月异，许多新理论、新技术正在研究和发展之中，因此，本书写作上可能存在一些缺点和不足，敬请专家和读者批评指正。

作 者

2005 年 12 月

目　录

第一章 绪 论

现代军事技术的一个重要特点，就是越来越广泛地采用电子技术，其中，无线电电子技术起着极其重要的作用。战略和战术武器普遍应用无线电探测、控制、通信等电子技术，必然导致电子战技术的迅猛发展。迄今，电子战已经成为现代战争必不可少的重要组成部分。从本质上看，电子战是指敌对双方在电磁频谱领域中广泛进行的一种对抗性军事行动。现代战争中，电磁频谱的应用深入到战争的各个领域，频谱从声波开始一直延伸到无线电波、红外、可见光波，直到紫外和更短波长的全部频域；作战范围从海、陆、空直到太空的广大空域，应用于军兵种武器的各种运载平台。因此，在电磁频谱对抗中，敌对双方综合电子对抗实力已成为影响战争全局的关键因素。在现代高科技战争中，处于电子战弱势的一方，将失去制电磁谱权，失去制电磁谱权即意味着失去对整个战争的指挥权，丧失制空权和制海权。在这种情况下，性能先进的兵器也难以发挥作用，难以在整体上组织起有效的军事行动，将处于被动挨打的地位。因此，大力开展电子战的研究和电子战装备的研制具有重要的意义。

1.1 电子战基本概念

1.1.1 电子战定义

一、电子战旧定义

电子战(EW，electronic warfare)旧定义为：使用电磁能量测定、利用、削弱或阻止敌方使用电磁频谱，并保护己方使用电磁频谱的军事行动。电子战通常包括电子支援措施、电子干扰措施和电子反干扰措施三部分。

电子支援措施(ESM，electronic support measure)包括对电磁辐射能量的搜索、截获、定位和识别等，用以迅速判明威胁的性质，为立即采取军事行动(如电子干扰、电子抗干扰和电子对抗部队的战术运用)及时提供战术情报，并为实施作战计划、指导战斗行动以及供给与防御效果校验等提供相应的支援。

电子干扰措施(ECM，electronic countermeasure)就是为阻止或削弱敌方有效使用电磁频谱而采取的措施，其中还包括了为阻止敌方获取电子情报而制造假目标、假信号数据等措施。

电子抗干扰措施(ECCM，electronic counter-countermeasure)是指在电子战环境中，为保证己方有效地使用电磁频谱所采取的措施。主要包括反电子侦察、抗电子干扰和抗反辐射导弹等措施。根据电子设备本身的设计要求考虑电子抗干扰措施是电子抗干扰措施的特征之一。

二、电子战的新定义

图 1-1-1 给出了有关电子战正式的军事术语和电子战的新定义。

新定义的电子战包括三个方面电子支援、电子攻击和电子防护。

电子支援:在指挥员授意或直接指挥下对有意或无意的电磁能辐射源的搜索、截获、识别和定位的行动。

电子攻击:使用电磁能或定向能,以削弱、压制或瓦解敌方作战能力为目的,对人员、设施和设备的攻击。

电子防护:采取行动保护人员、设施和设备,防止敌(己)方利用电子战削弱、压制或瓦解己方战斗力。

新定义是在原来电子战定义的基础上发展而来的。显然,新定义增强了电子攻击能力,即使用激光、微波辐射、粒子束等定向能武器、反辐射导弹和电磁脉冲来摧毁敌方的电子设备。此外,扩大了电子防护的使用范围,电子防护不仅包括保护单个电子设备(EC-CM),而且还包含采用如电磁控制、电磁加固、电子战频谱管理和通信保密等措施。因此,所有使用电磁波的设备(如雷达、通信、C^3I 系统、导航、敌我识别、精确制导、无线电引信、计算机和光电武器等)都是电子战的作战对象。由于电子进攻与军事电子装备和系统的电子防护构成矛与盾的对抗关系,每项电子技术的进展都会引出相应的对抗措施,而这种对抗措施必然会引起一种新的反对抗措施。因此,电子战对抗双方的斗争永远不会结束。

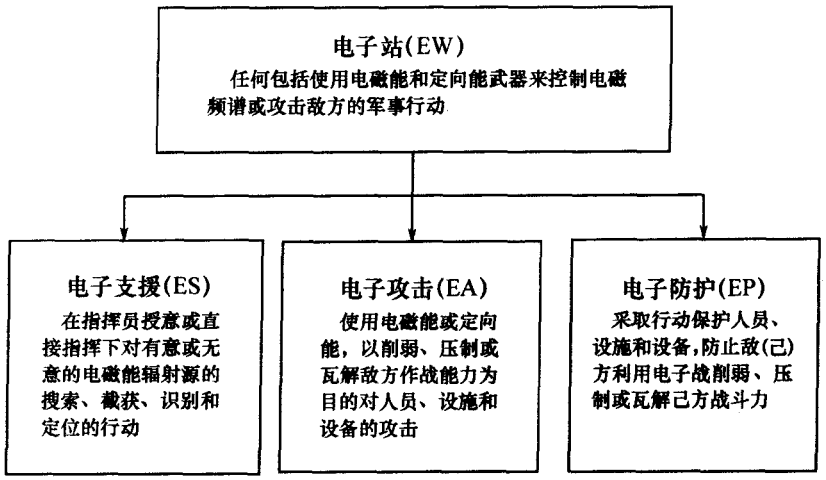

图 1-1-1　电子战术语

三、电子对抗

我国有关部门根据对立面相互斗争的哲学原理,用电子对抗取代电子战,其内容包括侦察与反侦察,干扰与反干扰,隐身与反隐身,摧毁与反摧毁。

此外,俄罗斯将电子战称作"无线电电子战斗",其定义为:用于探测、侦察和随后进行的无线电压制、摧毁敌人的指挥控制系统和武器系统的一类综合方法,以及对己方部队无线电电子资源及系统的保护。俄罗斯电子战内涵的主要部分是干扰破坏敌电子设备之间的无线电通信、反干扰以及对干扰和反干扰行动的保障(主要指建立必要的兵力与兵器、阵地区域电子设备和电子战的信息保障,以及隐蔽己方电子设备的重要信息等内容),其

本质就是瘫痪敌指挥、控制和通信系统。

1.1.2 电子战的分类

电子战包含了使用电磁频谱进行对抗的各个领域，内容十分丰富，有多种分类方法。按照具体的无线电电子设备或器材来分可分为：雷达电子战、通信电子战、光电电子战、引信电子战、敌我识别系统电子战、C^3I（通信、指挥、控制和情报）系统电子战、声纳电子战等。按照空间来分可分为：空中电子战、太空电子战、陆地电子战、海上电子战、水下电子战等。

从频域上可以将电子战划分为三大类：射频电子战、光电电子战和声学电子战。图1-1-2给出了频段的划分图。

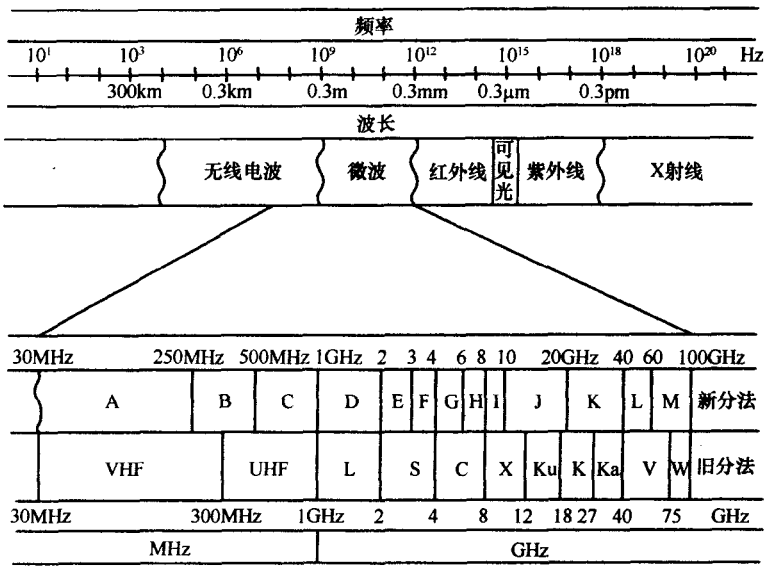

图1-1-2 电磁频谱的划分

一、射频电子战

射频电子战包括雷达、通信、导航、敌我识别、无线电引信、制导等领域的电子战，其设备工作的频率范围为3 MHz～300 GHz。

二、光电电子战

光电电子战的作战频段可分为红外、可见光和激光等子频段，是近距离精确制导武器和高定向能武器工作的主要频段。

光电电子战是指作战双方在光学波段（频率范围在300 GHz以上的红外光波、可见光波、紫外线等波段）运用光学设备、器材和其他设施所进行的电磁斗争。其最显著的特点是：所使用的光电设备和光电武器的精度高、分辨力好且抗电磁干扰的能力强。

光电电子战可分为光电侦察和反侦察、光电干扰和反干扰、光电制导和反制导、光电摧毁和反摧毁等。

三、声学电子战

声学电子战主要用于水下信息的对抗。从次声波至超声波，是声纳、水下导航定位设

备工作的主要频段。

1.1.3 电子战与信息战的关系

信息战就是敌对双方在信息领域的对抗活动，是指通过影响敌方信息和信息系统，同时保障己方信息和信息系统发挥作用，以支援国家军事战略取得信息优势而采取的行动。其实质是利用现代信息技术和手段，通过夺取信息优势（争夺制信息权）来达到自己的军事目的。它既包括了攻击对方的认识和意念，也包括了利用信息优势在实际战斗中打败对手。它既有暴力型，又有非暴力型；既有经济信息战，又有军事信息战，还有文化信息战。

信息战按其性质可分为广义信息战和狭义信息战两种。

广义信息战是指敌对双方在政治、经济、科技和军事等各个领域，运用信息技术手段，为争夺信息优势而进行的对抗。其内容包括：为了维护国家的安全利益，对于信息技术及其产品和系统所进行的研究、生产、装备、使用活动，以及对敌对国家进行的上述活动所进行的侦察、干扰、破坏和技术上的对抗与竞争。它是在平时、危机时期或战时打击对方的社会、经济、政治、工业或军事电子信息系统所采取的秘密或公开的、有控制性、破坏性或毁灭性的行动。其目的是通过取得信息优势来影响对方行为，阻止或避免冲突的发生，或以双方都投入最小的财力、物力和人员伤亡的代价，迅速彻底地赢得战争。

狭义信息战特指战场信息战，即军事领域的信息战，它主要发生在指挥控制、情报和信息系统等部分，是为获取军事行动全范围的信息优势而进行的斗争。其内容包括：使用信息技术手段进行的探测、侦察、引导、指挥、控制、通信、信息处理、伪装欺骗和打击等作战行动，以及针对敌方上述活动所进行的侦察、干扰、破坏和反利用等作战行动，为对抗敌方的侦察、干扰、破坏和利用而采取的对抗措施等。

反映在作战空间上，它是在陆海空天信息多维空间进行的作战行动，既是一种相对独立的作战形式，又渗透到各种作战形式之中；反映在行动性质上，它是以电子战、网络战为主的争夺制信息权的作战行动，既受联合战役的支配和约束，又对联合战役的胜败产生重大影响。

信息战的作战对象可概括为：信息、信息系统、以信息为基础的处理过程、以计算机为基础的网络和决策人员等。信息战要达到的首要目标是压制、削弱、破坏和摧毁敌方的指挥、控制、通信、计算机与情报系统。

信息战作为一种崭新的战争形态，使得现代作战手段进一步增多，使作战速度更快。其特点主要有：

持久性——信息战贯穿于战争的全过程（包括战前和战后）；

多维性——不仅在同一时空坐标内与陆战、空战、海战相互渗透、融合，而且能综合运用政治、经济、技术和军事信息进行特殊战争；

透明性——各参战部队对战况都了如指掌，从散兵到最高统帅部，所有用户都可以通过无缝隙、多媒体通信联络和网络共享信息；

一体性——各军兵种、各类作战系统、作战职能系统、武器平台和各作战单元连成一个有机的整体，信息的收集、管理、传递和拒绝也被信息系统连在一起；

实时性——各级之间接近实时地分发情报信息，作战进程与决策时间几乎同步；

精确性——目标发现就意味着打击，打击目标就意味着摧毁。

因此，在信息时代进行信息作战，首先要对敌方各级部队的决策机构进行信息攻击，通过切断或破坏敌人所有的信息媒介，使敌方指挥机关与部队脱节，从而使敌方部队失去活动方向和活动能力。确保己方进行不间断的、严密的和多频谱的监视与侦察，完整地接收己方部队从远距离发来的传感数据，使信息的准确性与武器的精度相适应，并快速、全面、准确地进行战斗评估。其次，确保己方决策周期比敌人的更短、运行更快，信息提供者应保持高度的战备状态，确保能随时提供所需信息。

从目前的发展情况来看，信息战的作战样式主要分为指挥控制战（C^2W）、民间事务战、公共事务战和网络空间战等，但其核心是指挥控制战。一般的情报作战、电子作战、作战安全、物质摧毁和心理作战均归属于指挥控制战争。因而，这五种作战形式也属于信息战。

一、指挥控制战

指挥控制战（C^2W）的定义为：通过情报的相互支持和综合运用作战保密、军事欺骗、心理战、电子战和实体摧毁等手段，达到抑制信息，影响、削弱或破坏敌军的指挥控制能力，同时保护友军的指挥控制系统免受敌方此类攻击的行动。C^2W 适用于任何作战行动及所有不同级别的军事冲突。

C^2W 适用于作战的各个阶段，不仅在敌对状态期间可以运用，而且在敌对状态之前和敌对状态之后都可以运用。即使在一般性作战行动而非战争的情况下，C^2W 也可以为军事指挥官提供致命性和非致命性杀伤手段，以完成上级部门交给的作战任务，达到遏制战争、促进和平的目的。C^2W 可延缓敌军的作战速度，扰乱其作战计划的制定，削弱其战斗力形成的能力，影响其对作战局势的估计。此外，C^2W 能够将友军指挥控制系统的易毁性及各部队之间互相制约、相互牵制的程度降到最低。

指挥控制战的基础设施是完善的和众多的指挥、控制、通信和计算机（C^4）信息系统，并与周密的、从国家级作战行动到战术级作战行动相关信息和情报支持结合在一起。指挥控制战的基石（基本组成部分）是：作战保密、军事欺骗、心理战、电子战和实体摧毁。

在战场上，综合使用这五种作战样式可产生最佳的协同作用。同时，也可使指挥控制攻击和指挥控制防护作战行动发挥出最大的效能。指挥员通过集中打击敌军对其军队的指挥和控制能力，同时保护友军的指挥控制能力免受破坏，实现作战的灵活性。

（一）作战保密

作战保密（OPSEC）定义为通过辨别、控制和保护与军事作战计划和军事行动有关的信息标记而使敌方无法获得己方能力和意图的过程。作战保密并非一个独立的过程，必须同精心制定的欺骗计划相结合。一个好的作战保密攻击计划将使敌方的情报系统收集不到情报，降低敌方指挥官有效控制部队的能力。作战保密防卫的目的是用欺骗的手段将假信息反馈给敌方，而将己方的指挥和控制信息隐藏起来。

目前，作战保密计划和措施的制定，受到新兴的全球商业部门的严峻挑战。其中，诸如摄像、定位和网络系统等新技术和手段，可以使敌方对友军信息情报的获取达到新的水平。而且，在作战行动期间，不可避免地出现的新闻媒体使得作战保密问题更趋复杂化。新闻媒体向全球听众传播实时信息的能力，可以成为敌军十分有利的信息来源。随着军

队数字化程度的飞速发展和广泛应用，信息安全的重要性也日益增长。

（二）军事欺骗

军事欺骗是指对己方作战能力、作战意图及作战活动等方面的信息进行歪曲和示假，从而有意误导敌方军事决策人员做出错误判断，最终导致敌军采取有利于己方完成任务的错误军事行动。军事欺骗是影响敌军指挥官决策的基本手段，其一般方法是对己方的作战意图、位置、部署、作战能力、活动过程和作战力量进行歪曲、隐蔽和伪装等，使敌方做出与真实情况相反的判断。欺骗的目的是引导敌指挥官按着有利于己方军事行动的方案行动，也就是人们常说的“牵着敌人的鼻子走”。

（三）心理作战

心理作战是一种将信息和指令传递给敌方的政府、组织及个人，以影响其情绪、意志、动机和客观的推理，直至影响其行为的作战形式。心理作战的目的是诱导或加强敌方的态度和行为。心理作战是以具体、真实和可信的信息为基础的。

美军的心理作战能够将分散的信息扩散到敌方的 C^4I 收集系统之中，显示其强大的联合作战力量和先进的技术优势，从心理上给敌方以精神上的震撼，加强敌方必然失败的信念。心理作战因素必须与其他指挥控制战要素、公共事务战略紧密结合、密切协同，以最大限度地发挥信息战争的优势。

心理作战在指挥控制防御战中的主要目的是将敌方在对抗己方力量方面的宣传和假情报的影响降到最小。

（四）电子战

如前所述，电子战是指包括使用电磁能和定向能武器来控制电磁波谱或攻击敌军的所有军事活动，它包含电子支援（ES）、电子攻击（EA）和电子防护（EP）。

在指挥控制战的框架之内，EA 主要用于对 C^2W 攻击，EP 主要用于对 C^2W 防卫，而 ES 既向情报系统提供信息又支援 EA 和 EP。为支援 EA、EP、规避、目标瞄准和其他战术部署有关的快速决策而达到准确实时地识别威胁，用 ES 来搜索、截获和定位电磁辐射源。ES 数据还用来生成信号情报，经处理后，成为情报数据库的一部分。这些更新的情报可用于规划 C^2 系统攻击行动和提供战场损伤评估，并反馈整个 C^2W 计划的效能。

无论是干扰、电磁欺骗还是采用定向能武器或反辐射导弹摧毁 C^2 系统的节点，EA 在作战环境中对几乎所有的 C^2 系统攻击行动都具有重要作用。它还可用于保护已方 C^2 系统免受敌方的攻击。EP 在 C^2 系统防卫中用来保护已方部队的信息安全，使其不被敌方电子支援行动所利用，是保障在 C^2 系统攻击行动中已方部队顺利、不间断地应用电磁频谱的最好手段。

（五）实体摧毁

在 C^2W 中，一项重要策略就是中断敌方 C^2 系统的关键节点。摧毁是完成这一使命的一种方法。而且，摧毁行动仅仅在特定的时间范围内起作用，所以实施时间很重要。通常，只要有足够的时间和备份资源，敌方就可以从摧毁状态恢复过来。从军事观点来看，若要使敌方 C^2 系统功能瘫痪，非常有必要采用实体摧毁。

针对 C^2W 的指挥功能，摧毁的目标是指挥中心。针对 C^2W 的控制功能，攻击的重点则是 C^2 系统的通信、计算机或传感器网的关键节点。对辐射信号的目标进行攻击时，常采用的方法是监视攻击前后信号的辐射情况。如果一个节点被攻击前在辐射而在攻击后

即停止了辐射，那么可以假设摧毁行动至少取得了暂时的成功。摧毁过程得益于精确制导武器的发展，它可对敌方 C^2 系统的各个部分进行外科手术式的打击。

EA 是摧毁过程的重要组成部分，反辐射导弹是摧毁性电子攻击的一种手段。反辐射导弹通过跟随关键传感器或通信链的辐射信号而被制导到辐射源上。这使得在可能遭受反辐射导弹攻击时，传感器或通信链只能停止工作。

定向能武器(DEW)是另一种摧毁性电子攻击手段。定向能武器采用激光、带电粒子或微波/射频波束，其吸引人之处是它们以光速进行攻击。目前，因功率受限，定向能武器在战术使用上还只能对电子设备进行破坏或烧毁。定向能武器既可以直接通过目标接收设备(即天线)进行攻击，此时叫做“前门”攻击；也可以通过电力线、设备外壳、连接电缆或其他泄漏通道进入设备，这种方式叫做“后门”攻击。

二、民间事务战(CAO)

民间事务是通过在全球信息环境中为其扮演一个综合的、相互作用的角色来支持信息战争的。无论在和平时期、冲突期间，还是在战争中，当启动了民间事务的保障作用时，就如同杠杆一样产生力矩，使得实施军事行动、加强战斗力量、寻求信息优势等得到提高。在作战区域(AO)内，虽然各种冲突的范围和条件各异，但是，民间事务活动能在军队力量、地方政府和平民大众中建立、维持、产生影响，并充分利用各种关系来促进军事行动的实施。

可以通过建立民事—军事作战中心(CMOC)使全球信息环境中的关键因素和影响产生相互作用，如非政府组织(NGO)、民间自愿组织和当地政府等。民间事务各部门通过在公众机构、经济、公共设施、语言、文化和公共信息等方面运用其技术和经验，以及通过收集与指挥官的关键信息需求(CCIR)相关的信息，来支持军事行动。民间事务个人在情报收集及作战计划过程中发挥着复杂而重要的作用。民间事务计划人员必须考虑所有可用的支持和信息，以确保成功地完成民间事务任务。

三、公共事务战

大多数军事行动完全是在公众详细研究、观察的情况下实施的。国内和国际新闻媒体报道在快速形成公众议论焦点及形成公众意见方面起着主要作用。新闻媒体是公众分析、评论作战目的、任务和行动的讲坛。对公众来说，媒体是一个重要的信息通道，它能够影响政治、战略、作战计划、决策以及作战任务的成败。当前，实时性的信息以比以前更快的速度被处理、发送并广为传播。这一现实情况极大地缩短了地面所发生的事情与国家军事战略目的、目标之间的距离。

公众事务人员的作用体现在以下几个方面：通过创造能产生自信心和支持军队作战的条件来帮助指挥员；提供公开、独立的报导，并将这些报道发送给部队和士兵；寻求平衡、公正和可信的信息形式，通过完整、准确、及时和畅通的信息流报道军队的战斗经历。指挥员、参谋人员和广大士兵在与媒体打交道时，必须平衡好作战安全与其他作战需求之间的关系。

上层领导明确给国内、外听众提供平衡、公正、可信的信息非常重要，并且在做决策的过程中必须将公共事务综合考虑进去。指挥员在制定计划过程中，必须保证使公共事务作战与其他战斗作用的发挥保持步调一致，并促进公共事务、民间事务和心理作战行动的尽早协同。在作战计划实施期间，保证信息交换过程连续、各种信息不冲突、具有一致性

至关重要。

四、网络空间战

网络空间作战是一种与指挥控制战、民间事务战、公共事务战等信息战形式有着根本区别的全新作战样式。网络空间作战样式的出现是信息战的一个根本性的标志，在信息战中处于特殊的地位，发挥着特殊的作用。

随着以计算机技术为核心的信息技术的迅猛发展，计算机网络已经进入军事、政治、经济、社会的各个领域。在军事领域，各种信息设备普遍联网，形成了庞大的信息系统，尤其是C⁴I系统的建立，将包括众多的计算机在内的各种信息获取、处理、控制和传输等设备联为一体。因此，以计算机为核心的信息网络已经成为现代军队的神经中枢，其性能优劣和状态的好坏不仅直接影响军队战斗力的发挥，而且一旦信息网络遭受攻击并被摧毁，整个军队的战斗力就会降低甚至丧失，国家军事机器就会处于瘫痪状态。正因为信息网络的这种极端重要性，决定了信息网络必将成为信息战争的重点攻击对象，而信息网络自身的易受攻击性也决定了信息网络必将成为信息战争中最容易受到打击的对象。一种全新的以计算机系统和网络为主要对象的信息网络攻击和防护作战模式已经出现并不断发展。

网络空间战与其他信息战样式相比，具有以下几方面的特点：

作战力量的广泛性——无论国家、地区、组织还是个人，无论军人还是民众，只要具备一定的计算机知识，掌握一定的网络攻击手段，就有可能进入其中对其进行攻击。

作战手段的知识性——网络空间作战人员是通过操纵计算机键盘和鼠标，利用其丰富的计算机技术知识，尤其是侵入计算机网络和传播计算机病毒等方面的技能来实施作战。这就使得网络空间作战的手段具有高智能性和知识性。同时，作战手段的知识性也是现代知识战争的重要标志。知识战争是以知识对抗为核心的作战行动。在知识战争中，知识在战争中的地位和作用超越了其他因素跃居首位，占有主导地位，起核心作用。

作战空间的广阔性——网络空间战不受地理条件的制约，只要是网络能够到达的地方都可能发生网络作战。因此，网络空间战的作战空间将更加抽象和广阔，一些传统战场概念（如国家之间的地理分界线、地理上的距离等）将不再适用，或变得越来越模糊。

作战时间的连续性——网络空间战几乎不受任何外界自然条件、天候因素、地理环境的影响，没有白天和夜间的区别，其作战时间具有连续性，是真正全天候、全时空的连续作战。网络空间战的出现淡化了战前、战时、战后等时间观念。

作战领域的一体化——在网络化战场上，网络实现了陆、海、空、天、电磁空间的融通，对任何一维空间的争夺都将对其他空间作战产生影响，使得作战空间一体化。通过网络，各种作战力量得以形成一个整体。在网络的支撑下，战斗力量联为有机整体，共享网络作战资源，同时，各作战部队之间在网络的联通下，也可以相互支援、密切配合、形成整体合力，实现作战力量的一体化。在网络化战场中，作战平台已不再只是打击兵器，而是横向连接、纵向贯通的打击系统。一方面与侦察、通信、指挥、控制、情报等子系统相通以确保作战效能的充分发挥；另一方面又与其他作战平台系统横向联网，以共同形成火力网，实现作战平台的一体化。在网络空间作战中，要把握战场的主动权，必须紧紧抓住以下几个

关键性因素：威胁响应、信息抗毁、毁伤评估、信息进攻和系统阻断。

随着军队对计算机网络的依赖性不断增大，利用计算机网络进行截取、篡改、控制、破坏、讹用敌方信息，摧毁敌人的信息系统使其丧失信息能力的攻势行动—网络攻击战，已经成为信息时代的一种新型作战方式。就目前的技术和使用情况而言，网络攻击战的两种主要的作战手段是：计算机病毒和网络“黑客”。

（一）计算机病毒

美国计算机安全专家认为：计算机病毒是一种程序，它用修改其他程序的方法将自身的拷贝、可能演化的拷贝放入其他程序，从而感染其他程序。由于这种感染特性，病毒可以在信息流的过渡途径中传播，从而破坏信息的完整性。可以看出，计算机病毒实质上就是一组通过复制自身来感染其他软件的程序。当程序运行时，嵌入的病毒也随之运行并感染其他程序。在军事领域，一旦军队的C^3I系统、武器信息控制系统的计算机染上这些病毒，整个作战体系就会瘫痪，无法正常发挥应有的效能。可以说，计算机病毒是现代网络攻击战的头号杀手。它直接影响着现代军事网络的正常运行和安全稳定。目前，尽管已经研制出各种病毒检测程序和软件，但是，人们仍然很难彻底根除这些计算机病毒。这是因为信息共享和信息交流是计算机网络的最大特点，计算机系统不可能没有信息共享，而计算机病毒又与信息共享相联，这种互联互通为计算机病毒攻击提供了可乘之机。

计算机病毒对网络攻击具有以下几个特点：攻击的隐蔽性强、传染性强、潜伏期长、破坏性大。计算机病毒的这些特点，使其具有其他武器所没有的优越性。在军事领域，军事信息系统的核心设备和信息武器装备的关键装置，都将成为计算机病毒攻击的主要目标。在网络战中，由于整个作战对网络和计算机的依赖性日益增大，一旦病毒开始发作，就会席卷整个网络，不仅使作战C^3I系统、计算机网络、雷达系统和各种传感器失效，而且会使由计算机控制的各种高技术武器系统（如现代化的飞机、舰艇、坦克、导弹等装备的自动驾驶、火控和制导系统）失灵甚至瘫痪。鉴于此，计算机病毒已经成为网络攻击战的一种新型作战方式，许多国家已将计算机病毒攻击战作为一种新型作战样式加以研究，并将计算机病毒用于军事对抗，以干扰、破坏、瘫痪敌方信息系统，使其无法正常发挥效能。

（二）网络“黑客”

“黑客”是指那些非法进入计算机系统窥探、窃取和破坏计算机网络的不速之客，他们都是熟练掌握计算机知识和技能的行家里手。在军事领域，“黑客”对军用计算机网络攻击的目的，主要包括情报窃取、威胁、干扰、瘫痪和摧毁等。可以说，网络“黑客”是继计算机病毒之后的第二号杀手，它能有效地利用计算机网络进行情报侦察，或者利用网络控制对方的指挥系统，瘫痪对方的C^3I系统，制造混乱或进行欺骗。

但是，网络“黑客”与计算机病毒不同。如果说计算机病毒作为一种没有生命的计算机程序还可以预防、可以杀毒的话，那么，网络“黑客”则是隐藏在暗处的计算机高手，令人防不胜防。随着国际互联网的发展，为了特定的目的，运用特殊的手段，通过民用网络就可以轻松地进入敏感的军用计算机网络，光顾军事要害部门，从事非法活动，给国家安全造成威胁。与计算机病毒攻击相比，网络“黑客”攻击除了隐蔽性强和破坏性大之外，其最大的特点在于攻击源很难查出。