信息战的理论及应用

刘小平　巨亚红

（中国船舶重工集团扬州 723 研究所　扬州　225001）

摘　要　分析了信息战及其相关概念信息和信息优势，评述了信息战理论的最新进展：联合信息作战和网络中心战，探讨信息战理论在科索沃战争和阿富汗反恐战争的应用。

关键词　信息战　网络中心战　信息优势

人类正进入信息时代，信息优势已取代火力优势，成为敌对双方争夺的首要目标，从而产生了一种新的战争理论和战争形式——信息战。自 1991 年的海湾战争以来，军事学家和未来学家都认识到军事冲突中的中心资源——从物理武器转移到控制和发动物理域战争的抽象信息过程和内容。1999 年的科索沃成为信息战的试验场，2001 年的 9.11 事件和其后美国发动的反恐战争，更是将信息战的理论发挥得淋漓尽致 。

1　信息战的理论及相关概念

信息是以任何方式存在于任何媒体中的事实、数据和指令，它是人类按照约定的表示方法赋予数据的意义。相同的信息对于不同的接收者可能有不同的意义。因此，可以给包括情报机构在内的信息收集者和使用者提供“混合信号”。

信息优势是指通过收集、处理和分发不间断信息流的能力，同时利用或阻止敌人进行同样活动的能力而产生的作战优势。可以通过三个相互依赖的活动取得信息优势：信息管理；情报、监视和侦察；信息战及相关活动。情报、监视和侦察收集数据并产生情报，信息管理在指挥控制系统内分发和使用相关信息，信息战则应用这些相关信息保护己方的指挥控制系统，攻击敌方的指挥控制系统并营造信息环境。它们都是达到和保持信息优势所必须的，但绝对的和持久的信息优势是不可能的。

信息战则是按照统一意图和计划实施，对敌方的信息和信息系统进行攻击，同时运用和保护己方的信息和信息系统来夺取信息的获取权、控制权和使用权，进而夺取和保持信息优势与制信息权而采取的各种行动。

信息战可分为进攻性信息战和防御性信息战。进攻性信息战是在情报的支援下，综合使用建制内的和支援的能力和行动，影响敌方决策者或他方，以达到或促成特定目标的实现。进攻性信息战通过制造己方可用信息与敌方可用信息的质量差异来获得信息优势，其手段包括摧毁、扰乱、削弱、拒绝、欺骗、利用和影响等。从产生的效果来看，可分为物理效果、句法效果和语义效果。物理效果是摧毁敌方信息系统中的物理部分，中断其服务；句法效果是攻击敌方系统的操作逻辑，使之反应迟缓、行为混乱；语义效果是摧毁敌方系统中维持可靠性和真实性的部件。防御性信息战是指为保护己方信息和信息系统而进行的策略和程序、行动、人员以及技术的综合和协调。防御性信息战保证己方获得及时准确的相关信息，同时阻止敌方利用己方的信息和信息系统。

信息战作为一种作战理论，有两个新的意义：一是信息战的作战概念是新的，有别于传统的作战理论，它将战争的范围从物理域拓展到信息域和认知域；二是将战场空间扩展到传统军事范畴之外的民用和商用基础设施，即国家所有的信息资源和过程都是潜在的信息战武器和攻击目标。

2　信息战的组成要素和相关行动

信息战包括 8 个组成要素：网络战、情报战、电子战、作战保密、心理战、军事欺骗、实体摧毁、信息保障。

网络战是指敌对双方通过信息网络（包含有限和无线网络）对敌方的信息、信息系统进行攻击，同时保护己方信息、信息系统的行动。网络战既可以在国家战略层次实施，体现为对敌方本土各种关键基础设施中的信息和信息系统的攻击，也可以在战役和战术层次实施，体现为对敌方局部战场信息和信息系统的攻击。

网络战由计算机网络攻击和计算机网络防御组成。计算机网络攻击是用来扰乱、阻止、削弱或破坏计算机和计算机网络内存贮的信息或计算机和网络自身的行动。为最大限度地发挥效能，网络攻击往往与其它信息战手段结合使用，可以支援、帮助和加强心理战行动以及机动、纵深打击、电子战、火力支援和军事欺骗行动，可以拒绝、欺骗、破坏和摧毁敌方的指挥控制节点、武器系统、通信系统、信息和网络。计算机网络防御是指为保护和预防信息、计算机和网络免受敌方阻止、扰乱、削弱或破坏而采取的防御措施。它包括探测非授权的网

络活动、监视敌方计算机网络攻击行动以及防护己方计算机及网络的所有措施，如访问控制、恶意计算机代码与程序探测、入侵监测工具等。

情报战包括电子(信号)情报战和人工情报战，是实施信息战的前提和重要保证。电子情报战的主要手段是电子侦察与反侦察。

电子战是信息战在电磁频谱空间的体现，是使用电磁能和定向能控制电磁频谱或攻击敌军的军事行动，其基本着眼点是夺取"制电磁权"。电磁空间是信息存在和依附的最重要最核心的载体，是现代战争信息获取、传递和利用的最主要媒介，是战争双方控制与反控制的焦点。夺取了制电磁权，就为最终夺取制信息权创造了有利条件。

传统的心理战、军事欺骗在新的电子网络多媒体领域中必将发挥更加重要的作用。在信息战条件下，作战保密的难度更大。

实体摧毁以物理攻击为主，以使敌方信息系统、物理目标丧失工作能力或被彻底摧毁。攻击范围包括从关键人员到各种信息系统及其依附的平台的硬件和关键部件。

信息保障是为确保信息与信息系统的可用性、完整性、可靠性、保密性和不可复制性而采取的行动，包括为信息存贮系统提供相应的防护、监视与反应措施。可靠性是确保用户或信息接受方身份的正确性，不可复制性是保证信息发送方身份的正确性。

公共事务行动的目的是使受众间的信息得以及时交流。公共事务行动应和信息战计划协调一致，并符合政策、法律规定和安全规定。民事行动与信息环境中关键组织和个人的交流发挥着重要的作用，它能影响、开发或控制信息基础设施，可以支援和促进信息战任务的完成。新闻媒介和其他信息网络越来越被政府领导人、大众和军方所依重，这对国家意志、政治方向以及国家安全目标和政策产生了重大影响。

3 信息战理论的发展

美国关于信息战概念和作战的研究始于20世纪70年代，直到90年代，这些研究才得以公开。此后，美国各军种及西方国家不断地探讨和完善信息战的理论和应用，如联合信息作战、网络中心战等。

联合信息作战是在危机和冲突(包括战争)期间，为达到某一特定目的或促进目的的实现，而对一个或数个特定敌方实施信息作战行动的总和。联合信息作战应用于各种级别的战争，渗透于作战的所有方面，贯穿于军事行动的全过程。其最终战略目的是影响现在的和潜在的敌方决策者的意志，使其停止威胁美国国家安全利益的行动。在战斗和战役范围内，信息进攻和信息防护的目的是信息、信息传输线路、信息收集和处理节点，以及人员与信息系统之间的交互活动。而在和平时期和危机发生的初期，联合信息作战作为一种遏制手段将发挥巨大的作用。

网络中心战最初由美海军于1998年提出，其后得到了美国防部和三军的广泛关注。网络中心战的实质是利用计算机信息网络对地理上分散的部队实施一体化的指挥和控制，其核心是利用网络把各种探测器、武器系统、指挥控制系统有机地联系在一起，对敌方实施快速、准确、连续的打击。它能使分散配置的部队发挥整体优势，依靠快速的指挥速度获取战争优势，通过网络化提高战斗力。其作战结构是可互操作的上级作战网络：联合监视跟踪网络、联合数据网络和联合计划网络；网络结构是三个相互耦合的网络：探测装置网络、交战网络和信息(通信)网络；战争同时发生在物理、信息和认知三个作用域。

4 信息战的应用

1999年的科索沃成为信息战的试验场。以美国为首的北约，为夺取战场制信息权，对南联盟的指挥控制中心、通信枢纽等进行猛烈的空袭。同时运用多种手段，以软硬攻心战瓦解南联盟的抵抗意志，如外交恫吓、轰炸南国家电视台等。计算机网络战成为科索沃战争最受关注的焦点，美国防部称之为首次网络战争。南联盟和俄罗斯的黑客攻击了白宫、北约总部等多个北约国家的网站。美国黑客也侵入南联盟的官方网站。网络攻击的主要手段有：a. 多人同时通过 ping 命令向某站点发出请求，使服务器过载；b. 发送大量邮件，使邮件服务器堵塞；c. 发送邮件病毒；d. 黑客及黑客程序；e. 电磁脉冲炸弹，爆炸时产生强烈电磁脉冲，干扰和摧毁没有防护的电路。

信息战具有不对称性，即力量相对弱小的一方可以对强大的一方进行信息攻击。美国的信息战专家们，多次虚构了恐怖组织利用信息战手段打击西方发达国家的场景。9.11事件是不幸而言中。基地恐怖组织摧毁了美国的经济金融枢纽——世界贸易中心大厦，对美国的打击和影响并不亚于一次核爆炸。恐怖组织自知在信息战手段上不能与美方抗衡，因此尽量避免使用移动电话等无线通讯设备，转而利用色情网站的图片来传递情报。

在美国对阿富汗的军事打击中，美方掌握了制信息权。作战保密程度高，实行新闻封锁，取得了情报优势；通过卫星、无人机、特种部队的情报侦察，克服了地形复杂的困难，取得战场信息优势；电子战与空袭相结合，摧毁塔利班的雷达、防空设施、指控系统；广泛开展心理战，通过"自由阿富汗"电台、无线广播飞机、传单等，瓦解、分化塔利班部队；借助北方联盟的力量，"以阿制阿"。美军利用强大的信息优势和火力优势，迅速打赢了反塔战争。

参 考 文 献

1 Edward Waltz. Information Warfare: Principles and Operations. Boston: Artech House, 1998

2 王智远等. 联合信息作战. 北京：军事谊文出版社，1999

3 刘春生，刘樟树. 美军对阿富汗军事打击的几个特点和启示. 航天电子对抗，2002；(2)

(责编：京辉钧)