

全军军事科研工作“十五”重大课题

计算机网络战综论

戴清民等 编著



解放军出版社

编 审 人 员

编 著 者 戴清民 戚世权 李新生

(以下按姓氏笔划顺序)

王劲松 毛 毅 兰汉平

朱学永 伍晓华 孙乐昌

杨志强 林春应 陆余良

陆 捷 祝 利 郭振和

黄曙光 梁亚声

统 稿 戴扣虎

主 审 沙自平

参加审定 卢文举 王伯俭 柳文华

陈力民

《计算机网络战综论》鉴定委员会

主任委员 王厚卿

委 员 (按姓氏笔划顺序)

刘永祥 刘继贤 任海泉

沙自平 张盘洪 肖稳田

李德毅 凌永顺

序 言

人类智慧的结晶——计算机从诞生之日起，就向世人展示出神奇的魅力。最初，它只是少数科学家才能触及的蒙着神秘面纱的高科技宠儿，但在短短几十年内，随着技术的进步，计算机网络横空出世并飞速发展，它极大地促进了人类社会生活习惯、生产方式、思想观念等各个方面的根本性变化，加速了人类迈向信息社会的步伐，成为信息社会的重要支撑。托夫勒曾经说过：“人类进行生产、生活的方式就是人类进行战争的方式”。随着计算机网络在军事领域内广泛地应用及作战行动对网络的高度依赖，计算机网络空间成为军事斗争领域中又一个崭新的战场。可以肯定，在未来信息化战场上，以计算机为工具在网络空间进行的激烈对抗将成为战争的重要作战方式之一。

作为一种新兴的作战方式，计算机网络战围绕的中心和焦点依然是战场信息，因此计算机网络战和电子战一样，同样也是信息战的重要内容和支柱。在信息化战场上，信息从以往战争中的边缘地位被拉回到作战的中心位置，通过各种计算机网络在整个战场飞速流动并发挥着至关重要的作用。而战场计算机网络的广泛运用能真正实现诸军兵种联合作战的统一指挥，陆、海、空三军互通共享信息、指挥员与战斗员之间的透明，真正实现实时或近实时的发现、指挥和打击行动，成为新的战斗力倍增器。作战的指挥、控制和协同对战场网络的依赖性空前增大，战场网络的瘫痪也就意味着整个作战体系的崩溃，交战双方围绕和运用战场网络进行的争夺将异常激烈、紧张和复杂多变。正是因为战场计

算机网络的极端重要性，围绕着破坏敌方计算机网络系统和保护己方计算机网络系统的计算机网络战必将成为未来作战中的又一关键。

为在未来高技术领域的军事对抗中，使与世界军事强军相比处于劣势的我军能够拥有一定的局部优势，进而创造以劣胜优的必要条件，我们必须充分利用计算机网络战这个特殊的作战方式，与具有强大高技术优势的敌人进行“不对称”作战。计算机网络战是我军进行“不对称”作战的重要手段之一，是一个最佳的切入点。从这个切入点入手，我们可以集中有限的人力、物力和财力，“不与龙王比宝”，低成本地破坏敌对国家的政治、经济、军事，乃至整个社会的信息基础设施及其运转，瘫痪敌方的军事、金融、通信、电子、电力系统，运用心理战和战略欺骗等手段，动摇其军心、民心和政府信念，达到遏制敌对国家发动战争或使其丧失战争能力的目的。

《计算机网络战综论》一书，从计算机网络技术和计算机网络对抗在军事上的应用两个方面，全面介绍了计算机网络的基本知识，首次完整、系统地提出了计算机网络战理论体系，并将其作为我军信息战理论重要内容，单独作为一个课题作专门研究。它的出版发行，标志着我军的信息战理论研究又进入了一个崭新的阶段，它是我军现代军事理论研究的重要成果，对我军的现代化建设将起到重大的推动作用。

目 录

第一章 绪论	(1)
第一节 计算机网络的基本概念.....	(2)
第二节 计算机网络战的基本概念	(13)
第二章 计算机网络技术基础	(34)
第一节 计算机网络结构	(34)
第二节 计算机网络软件	(61)
第三节 网络互连技术与设备	(70)
第四节 国际互联网	(93)
第三章 计算机网络战战场环境	(103)
第一节 计算机网络战战场环境的范畴.....	(103)
第二节 计算机网络战战场环境的特点 及其对作战行动的影响.....	(111)
第三节 军用计算机网络.....	(117)
第四章 计算机网络攻击	(123)
第一节 计算机网络攻击概述.....	(123)
第二节 计算机网络存在的安全漏洞.....	(132)
第三节 计算机网络信息截获.....	(143)
第四节 计算机网络攻击手段.....	(153)
第五章 计算机网络防护	(179)
第一节 计算机网络防护概述.....	(179)
第二节 计算机网络防护的主要手段.....	(190)
第三节 计算机网络防护规划和管理.....	(219)

第六章 计算机网络战的组织与实施	(232)
第一节 计算机网络战的基本要求.....	(232)
第二节 计算机网络攻击的组织实施.....	(238)
第三节 计算机网络防护的组织实施.....	(264)
第七章 计算机网络战建设	(270)
第一节 计算机网络战理论研究.....	(270)
第二节 计算机网络战部队建设.....	(283)
第三节 计算机网络战武器装备建设.....	(290)
第四节 计算机网络战人才培养.....	(295)
第五节 计算机网络战作战动员.....	(303)
后记	(321)

第一章 绪 论

20 世纪 80 年代,在马岛之战、中东战争及美利冲突等一系列高技术局部战争中,电子战作为一种极为有效的作战手段向世人展示出其强大的作战威力。在随后的几年中,伴随电子技术的进步,电子战得到了飞速的发展。到了 90 年代初,海湾战争的爆发,把电子战推向了一个更高的发展阶段,成为电子战发展的一个重要里程碑。随后,电子战理论开始进一步地更新和扩展,电子战的概念、作战手段、作战样式等内容不断地得到拓展和完善,其中一个最引人注目的新概念就是计算机对抗。

计算机对抗的提出,是因为计算机技术在越来越多的电子系统中得到了应用,使信息系统的智能化、自动化程度得到了很大的提高,从而极大地提高了军队的作战能力和社会生产力。但事物总有其两面性,由于计算机的核心地位和作用,使得其遭到攻击的后果将是灾难性的。为此,一些军事专家率先提出要实施计算机对抗,目的就是通过对计算机芯片和与电子信息系统相关联的电子计算机进行干扰和破坏,从而降低电子信息系统的作战效能,达到原先意义上电子战的作战目的。但随着信息技术的发展,计算机网络逐步普及和应用,并渗透到整个社会的政治、经济、文化、军事和社会生活的各个领域,原先意义上的计算机对抗已经不能满足军事斗争的需要了。人们迫切需要建立一种新的军事理论来反映和揭示计算机领域斗争的本质,并通过对这一理论的深入研究,找出计算机领域斗争的规律,更好地指导计算机领域的斗争行动。

在这种情况下,如果我们还将计算机领域的斗争放置在电子战理论的框架体系之下,就很难突破电磁领域军事斗争规律的束缚,也很难让人们把握计算机领域斗争中的本质属性。为此,我们有必要建立一种新的理论体系,这种理论体系必须能够涵盖计算机领域对抗的各个方面,这种新的理论就是我们在本书将要研究的计算机网络战。

第一节 计算机网络的基本概念

计算机网络缩短了人与人之间的空间距离,使人们有机会与分布在世界各地的人进行实时的信息交流,极大地提高人们的工作效率和学习效率,也有机会分享全人类创造的知识财富。在现代社会中,人们的生产、工作、生活和学习已离不开计算机网络。计算机网络也大大地提高了军队的作战能力,是现代军事力量不可缺少的重要组成部分。现代世界各国都把计算机网络看作现代军队的信息基础设施,重点建设,大力发展。

一、计算机网络的定义

什么是计算机网络?多年来并没有一个严格的定义。现在通常把计算机网络看作是利用通信线路将具有独立功能的计算机连接起来而形成的计算机集合。在网络中,计算机之间可以借助通信线路传递信息,共享各种软件、数据和硬件等网络资源。对普通用户来说,网络通常是透明的,一般他们并不知道网络的具体结构和管理方法,也不了解其他用户的操作情况,但他们可以充分运用网络上丰富的信息资源,享受网络提供的各种服务,用户和网络的关系如图 1-1 所示。

在计算机网络发展的不同阶段,人们从不同角度提出计算机网络的定义。在计算机网络发展的早期,人们从计算机与通信技术相结合的广义观点出发,把计算机网络定义为“计算机技术与通信技术相结合,实现远程信息处理和进一步达到资源共享的系统”。

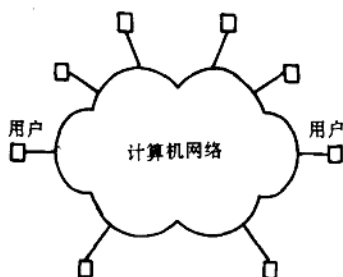


图 1-1 用户和网络的关系

美国信息处理学会联合会在 1970 年从共享资源角度出发,把计算机网络定义为“以能够相互共享资源的方式连接起来,并各自具备独立功能的计算机系统的集合”。

随着“终端——计算机”通信发展到“计算机——计算机”通信,从物理结构上看,计算机网络又可定义为“在协议控制下,由多台功能独立的计算机、若干台终端、数据传输设备以及通信控制处理机等组成的系统集合”。它强调计算机网络是在协议控制下,通过通信系统实现计算机之间的连接。网络协议是区别计算机网络与一般计算机互连系统的标准。

综上所述,可以把计算机网络定义为:凡将地理位置不同,并具有独立功能的多个计算机系统通过通信设备和线路连接起来,且以功能完善的网络软件(网络协议、信息交换方式及网络操作系统等)实现网络资源共享的系统,称为计算机网络系统。

二、计算机网络的功能

计算机网络主要有以下四个功能:

(一) 数据传送

这是计算机网络一项最基本的功能。通过计算机网络可以实

现文件传输、电子邮件和声音、数据、图形、图像等多媒体信息的传递。它是计算机网络其他功能的基础。

（二）资源共享

这是计算机网络最有吸引力的功能。它包括计算机软件、硬件和数据的共享。所谓共享是指网络中各地的资源能够互通有无，用户能在自己的位置上部分或全部地使用网络中的软件、硬件和数据。这样某些专门的软件可在各终端上调用，省去了购买和安装软件的开销，一些高级的特殊的设备则可向全网开放（如高性能的激光打印机），从而使整个系统维护和数据处理的费用大为降低。

（三）提高计算机的可靠性和可用性

计算机网络中几台计算机可通过网络彼此互为后备机，一旦某台计算机出现故障，它的任务就可由网络中其他计算机来执行。这就避免了在单机使用的情况下，一旦出现故障则整个系统瘫痪的现象，提高了系统的可靠性。另一方面，当网络中的某台计算机负担过重时，网络又可将新的任务转交给网络中较空闲的计算机完成，提高了每台计算机的可用性。

（四）实现信息分布处理

计算机网络内的用户可以根据问题的性质和要求选择网内最合适的资源来处理，以便问题能够迅速而经济地得到解决。对于综合性的大型问题，可以采用合适的算法，将任务分散到网内不同的计算机上进行处理。此外，利用网络将多台计算机连成具有高性能的计算机系统，解决大型问题，比用同样性能的大中型机的费用要低得很多。

三、计算机网络的基本组成

计算机网络一般由主计算机、终端、通信处理机、通信设备及信息资源等网络单元经通信线路连接而成，如图 1-2 所示。

（一）主计算机（HOST）

主计算机是计算机网络中承担信息处理的计算机系统。主计

算机配备有功能齐全的硬件和软件系统，具有很强的信息处理能力，还有相应的各种接口，可以快速地与网络交换信息。

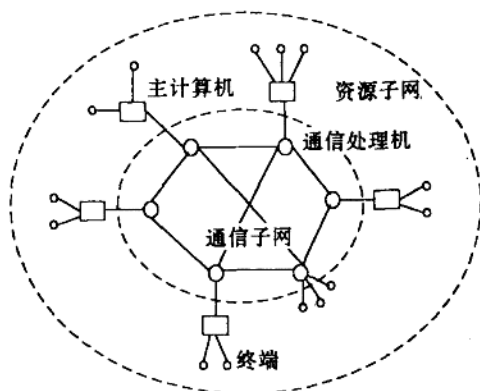


图 1-2 计算机网络的基本组成

(二) 终端 (Terminal)

终端是网络中用量大、分布广的设备，直接面对用户，实现人一机对话，并通过它与网络进行联系。终端种类很多，如键盘显示器、智能终端、会话型终端、复合终端等。

(三) 通信处理机

通信处理机也称作结点计算机 (NC——Node Computer) 或叫前端处理机，是设置在主计算机与通信线路单元间的计算机，负责通信控制和通信处理工作。它可以连接多台主计算机，也可将多个终端接入网内。通信处理机是为减轻主计算机负担，提高计算机效率而设置的。

(四) 通信设备

通信设备是数据传输设备，包括集中器、信号变换器和多路复用器等。集中器设置在终端密集地区，它把若干个终端用低速

线路先集中起来再与高速线路连接,以提高通信效率,降低通信费用。信号变换器提供不同信号之间的变换。不同传输介质采用不同的信号变换器。通常用电话线作为传输线。电话线只能传输模拟信号,但主计算机和终端输出的是数字信号,因此在通信线路与主计算机、通信处理机和终端之间都需接入模拟信号与数字信号相互转换的变换器。

(五) 通信线路

通信线路用来连接网络的各个组成部分。按数据信号的传输速率不同,通信线路分高速、中低速和低速三种。一般终端与主计算机、通信处理机与集中器之间采用低速通信线路。各计算机之间,包括主计算机和通信处理机之间及各通信处理机之间采用高速通信线路。通信线路可采用电缆、架空明线和光导纤维等有线通信线路,亦可采用微波通信、通信卫星等无线通信线路。

按照数据通信和数据处理的功能,计算机网络可分为两层:通信子网和资源子网。通信子网由结点计算机和高速通信线路组成独立的数据通信系统,承担全网的数据传输、交换、加工和变换等通信处理工作,即将一个主计算机输出的信息传送给另一个主计算机。资源子网包括主计算机、终端、通信子网接口设备及软件等,它负责全网的数据处理和向网络用户提供网络资源及网络服务。

(六) 信息资源

信息资源是用户最为关注的问题之一,也是计算机网络建设中的一个关键。网络上的资源主要包括数据库、文本、图像、声音和视频信号等信息类型,涉及军事、政治、经济、文化、商业、医学等诸多方面。

四、计算机网络的分类

现在大大小小的计算机网络系统众多,性能各异,其分类标准也很多,常用的分类方法主要有以下几种:

(一) 按网络的连接距离分类

按网络的连接距离可分为局域网、城域网、广域网和互连网等几类，如表 1-1 所示。

表 1-1 网络的分类

距离	应用场所	采用网络技术
10 米	室内	局域网
100 米	建筑物内	局域网
1000 米	校内	局域网
10 千米	城市	城域网
100 千米	国家	广域网
1000 千米	陆地	广域网
>10000 千米	全球	互联的广域网

1. 局域网 (Local Area Network, LAN)。局域网的地理范围一般在 10 公里以内，属于一个部门或一个单位组建的小范围网络，传输速率一般在 1Mbps 以上。例如，一个学校或研究所内组建的网络就是一个局域网。局域网的特点是组网便利、使用灵活，可用多种介质通信，传输速率较高，是目前计算机网络中最活跃的一个分支。随着社会信息化的不断发展，为了更好地发挥网络作用，局域网也可以连接到广域网上。例如，一个学校的校园网就可以连接到 Internet 这种广域网上，这样校园网上的用户可以享用广域网上的许多资源，也可以和广域网上的用户通信。局域网的基本组成和广域网相似，但由于局域网的涉及的范围与规模较小，故有一些方面与广域网不太一样。例如，局域网没有通信处理机，通信处理功能由网卡实现；局域网在逻辑上也可以认为是两级子网结构，但在物理上却不明显等。

2. 城域网 (Metropolitan Area Network, MAN)。城域网扩大了局域网的范围，其作用范围在广域网和局域网之间，是一种规

模较大,适应于大城市地区使用的网络。城域网的传输速率也在 1Mbps 以上,分布范围在几公里至 100 公里范围内。

3. 广域网 (Wide Area Network, WAN)。广域网也称为远程网,它是由多台地理上分布很广的计算机组成的网络,分布范围可以从几十公里至数万公里。一个国家或国际间建立的网络都是广域网。广域网一般采用电信部门提供的通信装置和传输介质,规模大,能实现大范围内的资源共享。Internet 也可被认为是由多个广域网互连而成的大型广域网。

(二) 按网络的开放性分类

1. 全封闭网络。这类网络是一般的计算机局域网络,它们与外界无任何通信联系,也没有数据、程序、指令的交换。

2. 半封闭式网络。这类网络一般是带有无线链路的区域网络,他们与外界无信息联系,只是在本地网络系统内存在信息流动。但由于网络通信链路是由有线和无线两种方式组成,所以信息在传递过程中,有一部分信息暴露在空中。一般的战术 C⁴ISR 系统大都属于这种系统。

3. 公共网络上的节点系统。这类系统是公共数据网络上的节点,他们共享公共数据网络上的软件、硬件资源,一般它们不允许非授权用户使用它的系统资源,这种公共数据网络一般是异种机(微型机、小型机和大型机)互连的广域网。

(三) 按网络的适用范围分类

按网络的适用范围可分为公用网和专用网。公用网一般是指国家电信部门建造的网络,为社会公众提供服务,只要按电信部门规定的方式交纳费用,任何人都可以使用。例如 Internet,我国的教育网、金桥网等,都是公用网。

专用网是某个部门为本单位或本系统的工作需要而专门建立的网络,这种网络一般只为本单位或本系统内部提供服务。本系统以外用户一般不能进入这种网络。例如军队、大企业、大公司 etc 自行建设的专用网。

(四) 按网络的属性分类

按网络属性可分民用、军用和军民共用计算机网络。

1. 民用计算机网络：指为全社会政治、经济、文化和其他活动提供服务的网络。如 Internet，我国的教育网、金桥网，以及各大企业、大公司建立的专用网。

2. 军用计算机网络：指专门为军事活动服务的计算机网络，如军事信息网络，指挥控制网络，军事情报网络等。军用网络的一个重要特点是具有较强的专用性和保密性。常用的军用网络有下列几种：

军用信息网络。这类网络主要用于传播和交流军事信息，为军队内部提供各种信息服务。例如，用于远程军事教育，信息查询，情报交流，文件传递等。

指挥控制网络。这类网络用于对部队的指挥控制。指挥控制网络根据其用途的不同又可分为战略指挥控制网络，战役指挥控制网络，战术指挥控制网络，以及军兵种的指挥控制网络等。

作战平台和武器系统控制网络。这类网络是指直接用于控制作战平台和武器系统的计算机网络，如国土防空系统中武器控制计算机网络，舰载武器控制系统中的计算机网络等。

军事情报网络。这类网络用于军事情报系统各个子系统的控制，侦察任务的分配和协调，侦察情报的汇总、分析、处理、分发，并可以提供各种军事情报服务。

3. 军民共用网络：指平时是军民共用，战时供军事运用的计算机网络。由于建设和维护大型计算机网络的费用相当高，所以许多国家除了建立专用的军用网络，还利用业已存在的民用网络来传递军事信息，形成了军民共用网络，以满足战时和平时需要。

五、计算机网络在现代战争中的地位和作用

高技术条件下的现代战争，具有战场范围广，参战兵种多，战斗十分激烈和战场态势变化急剧等特点。因此，现代战争的作战

指挥、武器控制、后勤保障等就与计算机网络的高效、稳定的运行密切相关。从某种意义上说,正是由于有了计算机和计算机网络才有现代高技术战争。20世纪80年代以来世界上几场大规模的局部战争表明,当今各种军事活动都高度依赖计算机网络,网络的性能对高技术现代战争的进程和结局具有重大的影响。其主要作用可归结为下列几点:

(一) 使战场更趋透明

利用计算机网络可以迅速地将各种传感器获取的信息汇总到指挥控制中心,从而使指挥员能全面地掌握战场态势,为正确地部署、运用部队和更有效地使用各种兵器提供了条件。另外,计算机网络使得部队的信息处理能力得到极大地提高,使部队的决策水平也有了相应的进步。美军通过数字化部队演习发现:足够的数字化传感器和通信线路意味着能够获取以前意想不到的情报信息量。但是必须对这些情报进行分析处理,才能得到真正需要的情报,否则指挥官将很快会被潮水一般的信息所淹没。完全解决这一问题牵涉到多种因素,但最根本的就是利用计算机网络提高信息处理的水平和能力。因此现在计算机网络是战场情报侦察和指挥自动化中不可缺少的装备。

(二) 使指挥更加顺畅

现代信息技术使指挥、控制、通信、侦察、监视一体化系统的传递和处理能力大为提高,战场更为透明,作战指挥的速度和能力大为提高。如美国总统通过 C⁴ISR 系统向第一线部队下达命令只需 3~6 分钟,越级向该部队下达命令只需 1~3 分钟;美国的战略空军司令部平均每天可处理 2.7 万条情报信息,雷达探测到目标后 10 秒钟即可传到指挥部,且可同时处理 2500 个目标;“赛其”防空系统的区域指挥中心,可同时对 100 批目标实施拦截指挥;北约组织的“奈其”防空系统,每个指挥报知中心能同时跟踪 200~400 个目标,用地空导弹拦截的整个过程为 2 分钟;野战和舰队防空指挥系统,从发现目标到发射地对空导弹的时间已