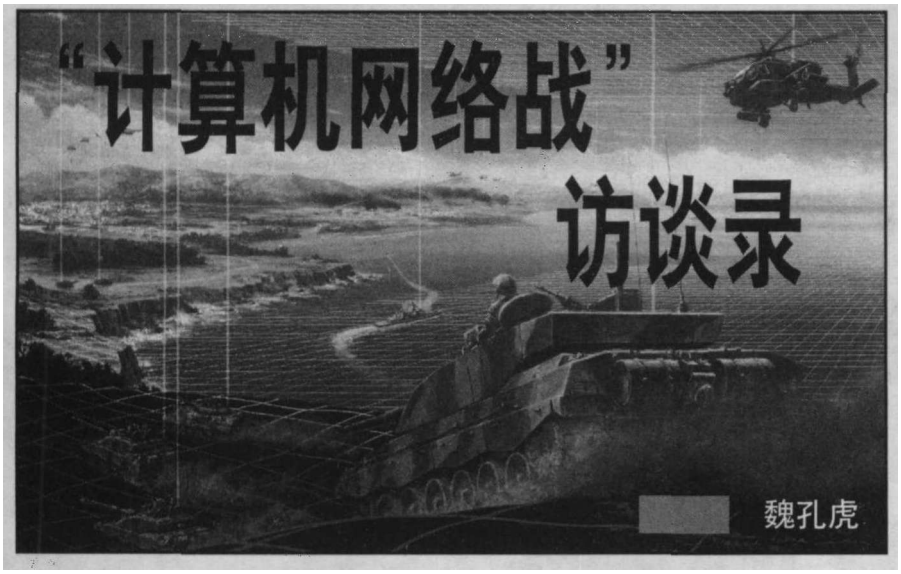


主题词 计算机网络战

21世纪的世界是信息世界，网络是信息世界的神经。近年来，计算机网络战研究日趋深入，如何正确认识计算机网络战的现实与未来，理性地审视计算机网络战的发展进程，是摆在我们面前的重大而又现实的课题。为此，笔者采访了国防大学博士生导师、信息战专家刘增良教授。

计算机网络战离我们并不遥远

魏孔虎（以下简称魏）：刘教授，目前关于计算机网络战的研究方兴未艾，您能否介绍一下计算机网络战产生的背景？

刘教授（以下简称刘）：应该说，计算机网络战的产生是以信息技术为基础，以计算机网络为支撑，以作战需求为牵引的必然结果。

随着以计算机技术为核心的信息技术的迅猛发展，计算机网络已经开始向地球的各个角落辐射。当今全球最大的国际互联网络——因特网的用户以每月递增10%～15%的速度扩大，预计2005年上网用户将达到10亿人。目前，我国上网人数近3000万，上网计算机1000多万台，域名数已达70万左右。在这种情况下，世界各国都在加紧建设国家、地区乃至全球信息基础设施，并最终形成超越传统地理空间概念的所谓“计算机网络空间”。“网络边疆”的概念已经渗透到一个国家的政治、经济、军事和外交的方方面面。在某种意义上，没有网络空间的安全，就没有真正意义上的国家主权和国家安全。

以计算机为核心的信息设备也在军事领域得以广泛运用，已成为军事现代化和武器系统先进程度的重要标志。C⁴I系统的建立，把包括众多计算机在内的涉及信息获取、处理、控制、传输的各种设备联成网络。以美军为例。美国武装部队拥有200多万台计算机和1万多个局域网，重大网络有海军网、空军网、陆军网、后勤网、仿真互联网、巡航导弹网、医疗网等170多个。陆军在进行数字化旅的演习时，战场通信网主要由战术互联网来承担。该网包括1200部计算机、950个互联网控制器路由器、27个战术多网网间联接器路由器、30个路由器、80000多个IP地址，被认为是目前最复杂的计算机局域网络。由此可见，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，一旦信息网络遭到攻击并被摧毁，整个军队的战斗力就会降低甚至几近丧失，国家军事机器就会处于瘫痪状态。因此，信息网络在未来战争中占有十分重要的地位。

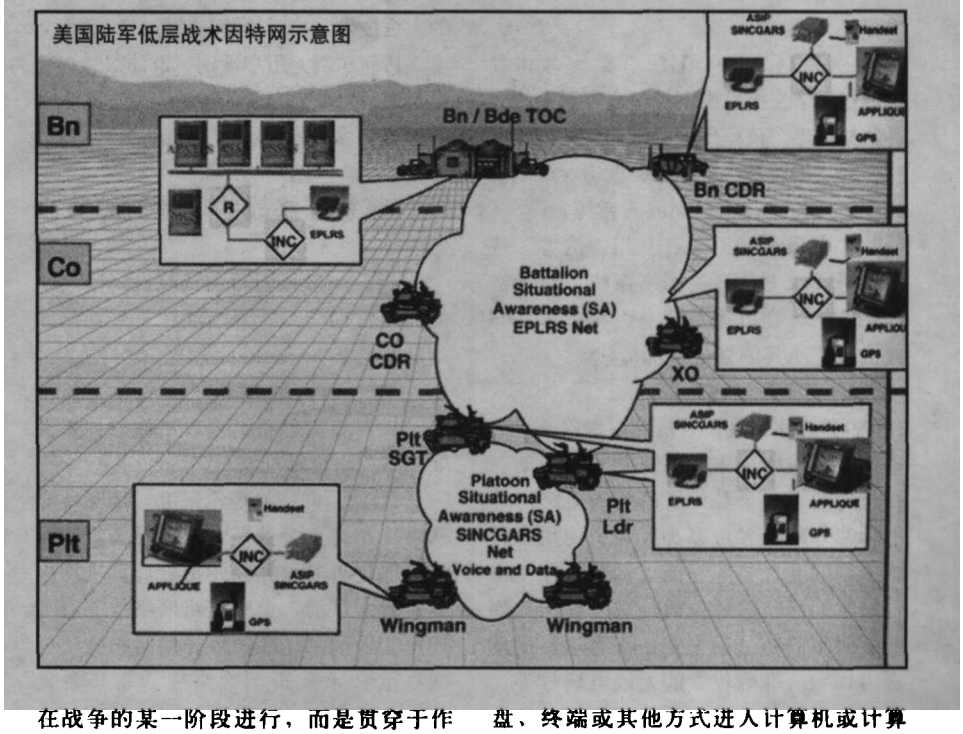
正是因为信息网络的这种极端重要性，决定了信息网络必将成为信息战争的重点攻击对象；而信息网络自身的脆弱性，也决定了信息网络必将成为信息战争中最容易受到打击的对象。目前，这种对信息网络的攻击不再仅仅局限于火力摧毁和电子干扰等传统手段，而将逐步演变成为信息战争中一种全新的作战样式——计算机网络战。

计算机网络战的实质和特征

魏：刘教授，计算机网络战的确已成为一种作战样式，但如何认识它的实质和特征？

刘：目前对于计算机网络战，国内外还没有一个统一的定义。外军“计算机网络战”的概念比较宽泛，有时和“信息战”相重合。如美军认为信息战包括4个组成部分：常规计算机战、常规网络战、非常规计算机战和非常规网络战，网络战属于战略范畴，而计算机战则属于战术范畴。其中，**常规计算机战**在一定程度上可以看作是指挥控制战，它主要包括作战保密、军事欺骗、心理战、电子战和物理摧毁等5个要素。**常规网络战**利用指挥控制战进行战略操纵，并通过联网方式介入社会意识形态冲突，其作战手段也同样包括前述的5个要素。**非常规计算机战**使用指

↓ 北约的野战司令部进行作战指挥的典型场面。网络一旦遭到破坏，其后果之严重不难想象



挥控制战的要素来阻止、削弱或影响敌人的信息交流，可以将它看作是指挥控制战中物理摧毁手段的使用。**非常规网络战**实际上就是大家常说的信息战，国家最高指挥当局利用基于信息的指挥控制战原则特别是信息攻击原则，通过联网方式介入到社会意识形态冲突中。

在我军学术界，对“计算机网络战”的定义在表述上不尽相同。但比较一致的看法是，计算机网络战至少包括以下要素：**作战目标**针对以计算机和计算机网络为中心的信息和信息系统。其中包括信息资源（各种信息源）、信息设备（获取、传输、处理、利用信息的硬设备）、信息系统（应用信息系统和应用软件系统）、信息网络（网络体系有效运转必需的网络标准、通信协议、操作规程、传输编码等）以及信息主体（信息资源的开发者、提供者、管理者和利用者）；**作战空间**主要是网络信息空间；**作战手段**包括以计算机网络技术为主的病毒感染、网络入侵等“软”打击和高新武器装备的“硬”摧毁；**作战主体**是执行计算机网络战的作战部队；**作战层次**包括战略级、战役级和战术级。综上所述，我们认为：**计算机网络战是信息战的一种作战样式，它是指在信息网络空间上对指定的网络信息系统进行的有目的、有计划、有组织的信息攻击和信息防御行动。**简称“网络战”。

计算机网络战的特征，一是作战的效费比高。开发网络战的攻防技术，不像研制和生产硬杀伤武器那样需要巨大的人力、物力和财力的支持，只要具备信息系统的专业技能和少量资金就能进行。如计算机病毒的研制成本低、周期短，而传染性强、破坏力大。二是作战手段多样。作战中，既可以利用黑客技术，又可以利用电磁干扰手段，还可以使用病毒武器；既可以利用传统的兵力、火力进行，又可以利用新概念武器如电子生物武器进行；既可以以小分队实施网上“渗透”，还可以远距离实施网络控制。三是作战行动攻防一体。在计算机网络战中，进攻与防御在任何阶段都是并举的，不再按阶段、划区域、分层次展开。作战行动离不开信息系统的支援保障，信息系统又是作战系统的组成部分。这就决定了网络作战不只是在战争的某一阶段进行，而是贯穿于作战的全过程，甚至包括直接的战场对抗开始之前及停止之后。

计算机网络战的分类与手段

魏：刘教授，作为一种作战样式，计算机网络战通常有哪些类型，作战中有哪些方法和手段？

刘：计算机网络战的分类，可从网络战的作战层次、行动特征、作战性质等不同角度来确定：按作战层次，可划分为战略级、战役级和战术级网络战；按作战特征，可划分为网络入侵战、网络远程控制战、网络阻塞战、网络破袭战、网络节点战、网络虚拟战和网络病毒战等；按作战性质，可划分为网络进攻与网络防御。其中，按作战性质来划分是最基本的方法。网络进攻和网络防御是一个矛盾体的两个方面。网络进攻是一种主动行为，通常目标明确；而网络防御是一种被动行为，通常目标比较模糊。

计算机网络进攻的手段主要有：

(1) “软”打击手段

①**计算机病毒。**是人为编制的、在计算机系统运行过程中能把自身（或经修改后）复制到其他程序内、具有破坏性的一段有害程序。计算机病毒通过软盘、终端或其他方式进入计算机或计算机网络，引起单机或网络运行紊乱，甚至瘫痪。计算机病毒具有传染性、潜伏性、隐蔽性和破坏性四大特点。

②“蠕虫”程序。是一段独立的程序，通过爆炸性的自我复制方式从网络上一台计算机扩散到另一台计算机。

③“特洛伊木马”程序。是隐藏在计算机程序里并具有伪装功能的一段程序代码，使计算机能在仍然完成原先指定任务的情况下执行非授权功能，实现攻击目的。

④逻辑炸弹。是由计算机系统开发者或程序员按一系列特定的条件设计，并蓄意埋置在系统内部的一段特定程序

↓ 美国海军陆战队在演习中进行通信联络。而战场通信网将愈来愈多地由战术互联网来承担。

或程序代码。

⑤截取程序（sniffer）。是攻击者在远程网络交换机或主机中有意插入的一种软件程序。该程序可监视信息分级包，并将其复制后返回攻击者，攻击者可以借此获悉用户名和密码而闯入系统。

⑥“黑客”手段。利用“黑客”技术，进入敌方计算机网络系统，对加密程序解密、窃取或对信息进行破坏，并攻击系统使其部分或全部瘫痪。

(2) “硬”破坏手段

①“芯片捣鬼”。是指蓄意修改、更动、设计或使用集成电路芯片的活动。在多达数百万个晶体管的集成电路芯片上，芯片制造者可以加入正常使用者料想不到的某些特殊功能。例如，在使用一段时间后使芯片失效，或者在接收到特定频率的信号后自毁，或者运行后发送可识别其准确位置的无线电信号等。而一个关键芯片的小故障足以引起整个系统停止运转。

②实体摧毁。是指对计算机网络的物理结构实施摧毁。可采取火力攻击，使敌局部信息网络所依赖的通信实体遭到彻底破坏。亦可采取电磁脉冲打击的方法，使敌网络中的计算机系统和信息传输系统阻断、过载或自毁。常见的武器还有微波炸弹、电磁脉冲炸弹和生物炸弹等。

计算机网络防御的手段主要有：

(1)网络安全设计。包括安全风险评估和分析工具、网络和信息环境的安全分析标准、安全策略设计辅助软件、安全策略实施方案与步骤等。

(2)网络的安全监控与告警。包括入侵检测工具、代理服务器与审计分析工具、实时告警与监控软件等。

(3)网络安全基础设施。如分布式计算环境、分布式证书系统、网络安全体系结构设计规范、专用网络安全协议的设计与实现等。

(4)网络“防火墙”。包括基于应用级和网络级的防火墙结构设计、安全网络拓扑结构设计等。

(5)开放网络环境安全。包括安全/开放的信息网络、移动计算机安全技术、防电磁屏蔽与干扰、防窃听技术等。

(6)其他防御技术：包括大型数据库的安全技术、病毒检测与消除、标准报文卡、访问控制、用户识别、审计跟踪、数据加密、安全密钥管理、智能卡、网络安全协议、多级安全、信息源伪装等。

计算机网络战的现状与趋势

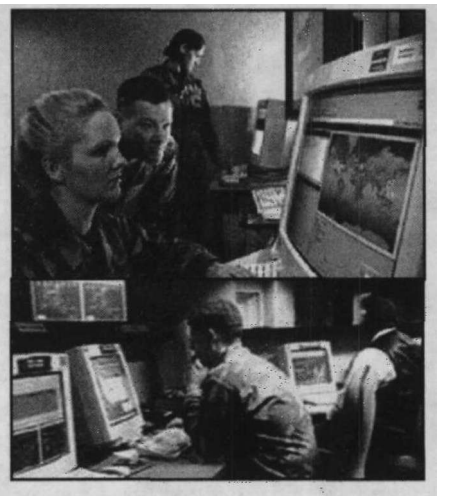
魏：刘教授，目前计算机网络战研究的现状如何？能否预测计算机网络战的发展趋势？

刘：为了在未来网络战中占据主动，世界各国已纷纷采取措施，积极开展网络战研究和准备。

(1)加强网络战理论研究。为了争夺网络战制高点，世界各国都极为重视网络战理论研究，并以此指导计算机网络战建设。目前，美军已将网络战的有关理论写入信息作战条令，同时积极研究网络战技术，研制网络战武器装备。2000年，俄罗斯讨论并通过了《国家信息安全学说》。该《学说》的基本宗旨是促进俄罗斯信息技术的发展，为国家信息活动提供安全保障。针对网络领域的激烈斗争，俄军就建立自己的信息防护范围等问题，展开系统的、有针对性的理论研究。

(2)组建网络战机构。美国防部现已设立了“国防信息系统局”，陆、海、空三军也相继成立了信息战中心。英国陆军已经建立一个40多人的网络作战单位，以对抗逐渐增加的网络战争威胁。印军拟组建一个联合的武装部队计算机应急小组，处理对军事设施的计算机非法入侵、电脑恐怖主义活动等。印度海军已准备成立印度海军计算机应急小组。此外，印军将加强与印度理工学院、印度科学院以及印度信息技术与管理学会等信息技术专业机构的合作。

(3)重视网络战人才培养。1995年美军第一代“网络战士”从美国国防大学信息资源管理学院毕业后，又有一定数量的网络战人才相继完成学业，其中还包括一部分信息战指挥军官。美军还组建了世界第一支面向实战的网络信息战部队——第609网络信息战中队。该部队有55名成员，由计算机、电子学、航天、通信工程、通信保密等专业的专家和技术人员组成。此外，日本、以色列、英国等国家通过培养“黑客”、召集计算机专家的方式，发展网络战人才。



↑ 美军网络攻防分队在进行演练。

(4)注重网络战演练。20世纪90年代以来，美军已经多次进行网络战的模拟演练。特别是美军举行的代号为“联合远征部队实验99”的演习，重点之一就是检验软破坏和硬摧毁等手段在信息战中的实际效果，探索对计算机网络实施信息攻击的基本方法与途径，同时也寻找可能遭到敌信息战攻击的薄弱环节，为提高信息网络的安全可靠性提供依据。与此同时，法国、德国等国家也在着手网络战的研发和模拟演练，以此来加强网络作战能力，确保其网络系统适应未来实战需要。

海湾战争和科索沃战争中，网络战已初露端倪。然而，从严格意义上讲，这种无组织、自发的“网络战”行动还不能算是真正意义上的计算机网络战。未来的计算机网络战必将是国家或军队之间的有组织、有目的的对抗。要实施真正意义上的网络战，一是要解决网络战可能引发的违反国际法准则、战争道德和战场指挥官权限的问题；二是要在网络战技术上取得重大突破，特别是在网络防御技术基础上，重点发展网络进攻技术；三是计算机网络战力量要作为一个新型的军种得到广泛的认可；四是计算机网络战理论研究需向深层次、条理化和可操作的方向发展。