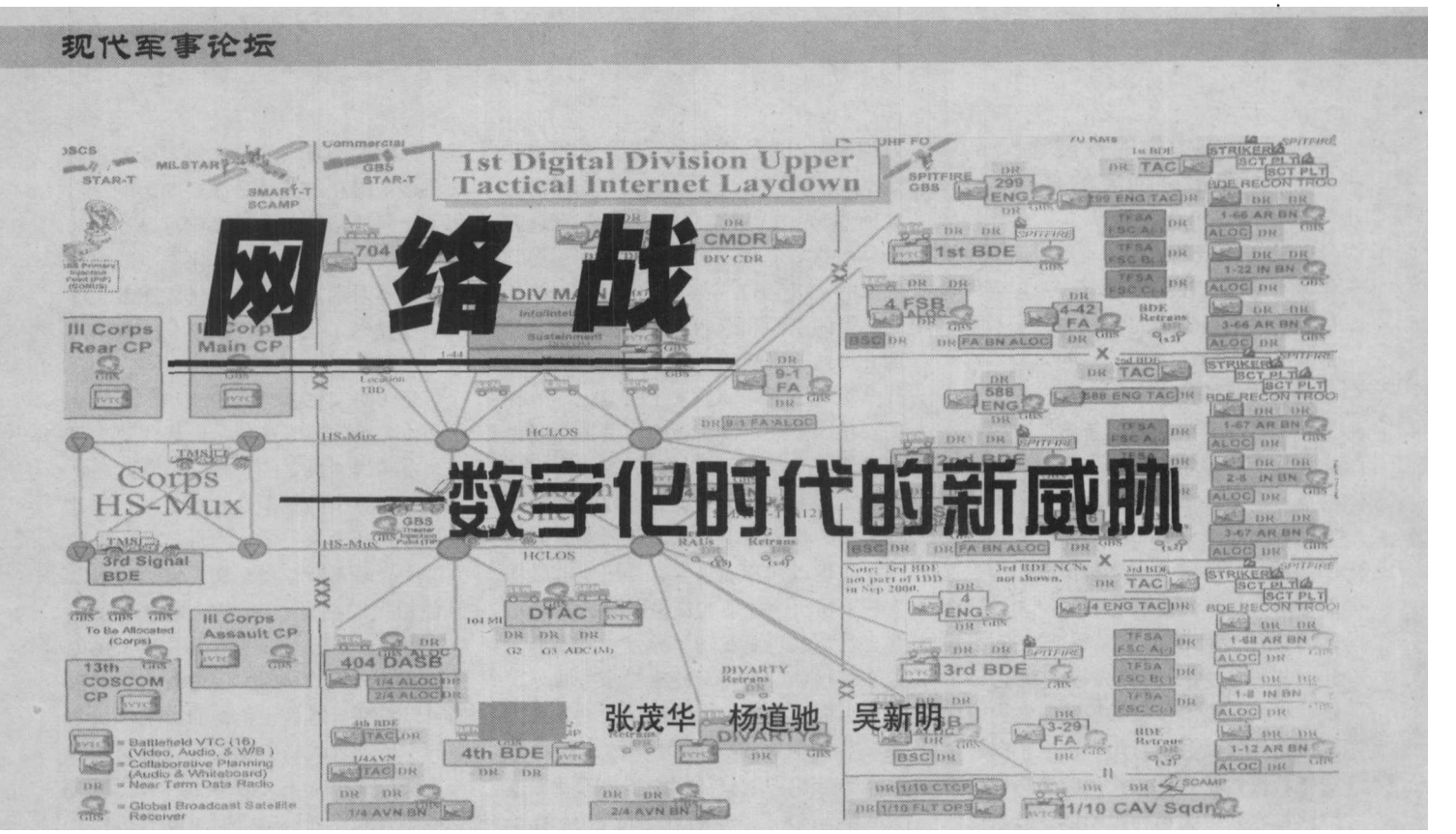

网络战

——数字化时代的新威胁

张茂华　杨道驰　吴新明

主题词　网络战

网络作战初露端倪

在人类历史上技术发展的不同时代，战争具有不同的特征。冷兵器时代军队主要依靠肉搏，特征是刀光剑影；热兵器时代依靠的是坦克、飞机、大炮的强大火力和快速机动，特征是火光硝烟；在数字化战场上，除了热兵器时代的基本特征外，包括悄无声息的网络战在内的信息战将成为越来越重要的作战样式。

网络战（Netwar）是指在国际互联网及其他网络上，利用计算机技术侦察、获取、干扰、破坏对方指挥系统、武器系统及人事、组织、后勤等系统中的重要信息，进行思想、文化渗透，从而达到影响、加速甚至决定战争进程的高技术行为。它以信息技术为支撑、以网络为载体，可使作战双方在互不见面的条件下遂行作战。网络战是信息战（Information Warfare）中一种极为重要的作战方式。

在北约发动的科索沃战争中，就已经发生了互联网上的战争。计算机“黑客”对美国、英国及北约的网站实施了攻击，使得白宫和五角大楼的计算机系统一度被迫停止运行；英国气象局的计算机网络也曾处于瘫痪状态，无法为北约空袭提供必要的气象服务，从而使北约的一些空袭计划被迫撤销；南联盟还利用互联网成功地反击了北约的信息封锁和宣传战……网络作战初露端倪。

网络战的主要作战模式

通过计算机网络开展信息攻势

通过计算机网络以文字、图像、音像等形式向敌对国展开心理战，具有速度快、范围广、不易察觉和防范、节省财力物力等特点，可以达到“不战而屈人之兵”的目的。

通过计算机网络还可以散布虚假信息，进行军事欺骗和诱导。例如，在网络的核心部位设置一系列不对世人公开的结构，在其中存放虚假情报，并且标以秘密等级，专门引诱那些手段高明的攻击者上钩。

通过计算机网络非法获取信息

一般地说，互联网上的军事网站对访问者的级别及范围都有限制。但对于精通计算机的“黑客”来说，所谓访问级别和权限是形不成障碍的。例如在1998年2月26日至3月21日，一名计算机“黑客”大闹美国国防部，先后侵入4个海军系统、7个空军系统的计算机网络，且在已被察觉并采取防范措施的情况下继续“骚扰”了一个星期，使得美国国防部陷入惊慌和尴尬的境地，以致美国总统克林顿亲自下令专门组织机构，以防止“电子珍珠港”事件的发生。

破坏敌方的计算机网络

在借助互联网发送的电子邮件中，可以携带计算机病毒。当网站的主人收到电子邮件并观看其内容时，隐藏的程序就自动运行，在被攻击的计算机中寻找关键性的密码、口令或者其它进入计算机系统所必需的信息，并自动把这些信息反馈给电子邮件的发送者。而军事计算机系统一旦被敌方的黑客非法进入，指挥系统就很有可能陷入瘫痪，军事指挥人员也可能因假情报的混入而做出错误的判断。这种秘密程序有时直接在敌方的计算机系统内兴风作浪，封锁或者删除其硬盘上的数据信息；或者作为“特洛伊木马”，暂时不动声色地潜伏在敌方计算机网络中，自主判断形势，等关键时刻再给对方计算机中枢神经以致命打击。此外，通过大量、集中快速地访问敌方网站，使得网站堵塞以致瘫痪，也

是一种有效的网络攻击方式。

网络战的特点

作战灵活，成本低廉

网络战所需要的硬件设备很简单：1台配备调制解调器的计算机和1条普通电话线，再加上必要的上网软件足已。有了这些基本设备，无论是国家、地区、组织还是个人，不论是军人还是平民，只要具备相应的计算机知识，掌握一定的网络攻击手段，都有可能介入战争，实施网络攻击作战。

手段专业、智能性高

与传统作战不同，网络战的主要作战手段是通过计算机键盘和鼠标，利用丰富的信息技术知识和有效入侵计算机网络、传播计算机病毒等方面的高超技能来实施作战，这就使作战手段具有高智能性和极强的专业性。

战场广阔，方式隐蔽

网络战是在网络空间实施的作战，不同于有形的现实空间，很难确定网络攻击是来自于国内还是国外，是个人犯罪还是国家作战；空间的距离对于网络作战将失去作用，不论是战区还是本土，只要联网就可能遭受攻击；而且网络战几乎不受任何自然条件的影响，可以说是真正的全天候、全方位作战。因此，相对于传统战争的时间、空间概念来说，网络战具有极强的隐蔽性。

效能显著，威力巨大

目前工业发达国家，尤其是美国，日益依赖计算机网络系统控制电力、航空、电信、交通及金融等重要行业和部门、军队的作战、指挥也日益依赖各种计算机网络系统，高精度的武器系统更是必须在网络系统的支持下才能充分发挥作用。对计算机网络的有效攻击，威力不亚于核袭击，往往在很短的时间内就会对被攻击一方的政治、经济、军事、文化系统造成巨大破坏、所造成的损失不亚于一场核战争。

网络战的现状与展望

网络战的研究现状

美军认为，在21世纪数字化战场将发生典型的网络战。为了迎接这一挑战，美军的准备目前主要集中在两个方向上：一是训练能熟练使用计算机和运用网络技术的“网络战士”。这些“网络战士”不但知晓如何保护己方的网络系统，而且还会利用计算机病毒等手段攻击敌方网络。二是根据信息战的要求，改进和完善单兵在战场上的网络应用能力，使普通士兵成为“准网络战士”。美军已经成立了专司计算机网络防护与攻击的分队，并进行了多次网络攻防演习。

日本防卫厅在2000年10月开始制订计划，研究开发“网络武器”。据日本陆上自卫队和防卫厅技术研究总部人士宣称，今后在构建防御体系的过程中，有必要认真模拟系统被黑客入侵的后果，并进行排除病毒的训练。

以色列军方已经为其计算机配备了“计算机攻击防御系统”，这一系统能有效的防止陌生邮件和病毒的入侵。此外，以色列最近研制成功一种“负荷平衡系统”，可吸收计算机额外的负荷，增强安全性。

我军目前也已开始探讨网络部队的建设。据解放军报报道，1998年初山西大同军分区预备役网络分队正式组建，编有程序班、操作班、保障班和培训中心等。他们的宗旨是：“坚持积极防御，通过模拟来自敌方对我指挥系统可能实施的网络破坏、情报窃取与修改等一系列网络战行动，探索提高我信息安全防护的战术技术”。

世界上许多国家已经在积极研究对策，防范网络入侵和攻击。比如只让值得信赖的信息通过的“防火墙”已付诸实用；在特定条件下破坏入侵信息（如电子邮件的涌堵）的“逻辑炸弹”正逐渐流行；模仿生物体免疫系统的防火墙、感应器和杀毒系统“三合一”防护措施也应运而生。但是，由于网络的迅速普及，掌握“黑客”技术的人日益增多，加上“战线”太长，所以防范网络入侵和攻击仍然任重而道远。

网络作战的发展前景

美国国家安全局局长最近在一次大型计算机安全会议上说，“现在网络空间已成为确保美国安全的新战场，就像海上、空中和陆地战场一样”。从发展的前景看，未来战争必将是陆、海、空、天、电、网一体化的作战，“网军”极有可能成为继陆军、海军、空军、天军、电子战部队之后的又一新军种，担负起保卫网络主权和从事网络作战的艰巨任务。有关专家认为，鉴于世界对互联网络的依赖程度日益增大，任何对网络攻击的后果都将是灾难性的。如果网络攻击与其它作战行动结成一体、必将使网络战在战争中发挥更大的作用。现代高技术战争将“无网”不胜。

↓ 现代武器系统高度依赖网络系统。因此，网络攻击的后果将是致命的。