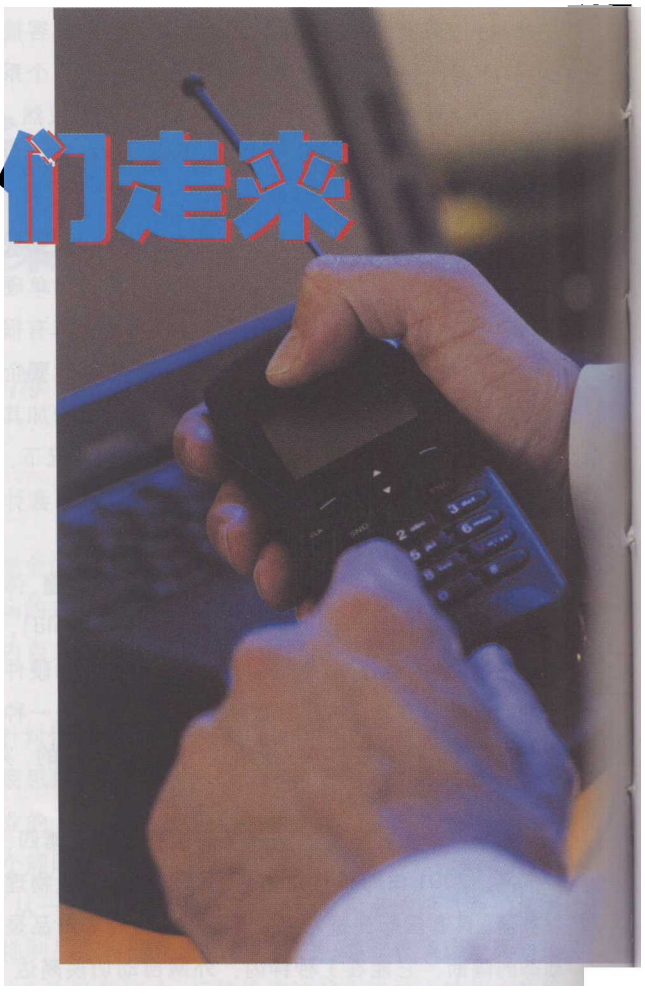
网络战正向我们走来

北京系统工程研究所 **黄志澄**



提起网络战，多数人都会联想到黑客，但网络战远远不止于此。一位在美国核心军事部门工作的军官说："当我听到有人谈起搞坏硬盘和散播病毒时，我就知道他们是业余的。"实际上，网络战是"全方位信息战"的一部分。美国国防部的有关文件指出：这种全方位信息战必须融入总体军事战略，并与相关的外交行动和国际公共信息活动互相配合。在这个新的作战领域，关键是获得网络信息信号。美国国家安全局迈克尔·海登说："我们正在遵从新的通信环境，彻底改变国家信号情报系统。"他说："过去在空中截获的信号，如今却在地面；过去在地面截获的信号，如今却在空中。"

从EP－3E侦察机看网络战

7月3日下午8:00，在4月1日抵近我沿海侦察，并撞毁我战机的美国EP—3E型电子侦察机，在卸成几块后，由俄罗斯安－124运输机从我国海南陵水机场，将其运回美国佐治亚州该机的制造商洛克希德·马丁公司的工厂。我国终于送走了这个瘟神。

对EP－3E侵入中国南海上空侦察，美国五角大楼的解释是，它只是在执行一次例行的飞行任务。不过，微软的全国广播公司（MSNBS）最近报道说，对几十名高级政府官员和军官的采访表明，EP－3E的任务远不止于"例行侦察"。它实际上是美国网络战的尖兵。正如美国五角大楼描述的那样，EP－3E能对语音通信和雷达信号进行监视。但五角大楼没有说出来的是，这种飞机的接收器还

能接收一种新形式的数据代码——"PROFORMA"。这也是一种电子情报的来源。

微软全国广播公司解释说，现代计算机网络传送数据时都夹带着网络协议的拨号音和连接信号，以确定传输的路径与速度。这种拨号音是所有计算机通信固有的一部分，称作"PROFORMA"。通过它可以操纵、欺骗甚至搞垮现代军队依赖的复杂的网络系统。从本质上说，这就是"机对机"战的开始。在这类战争中，每一方都可以通过对数据做手脚，而深入对方的核心指挥系统和控制系统。

在科学技术日新月异的时代，"PROFORMA"只是网络战的"冰山一角"。据称EP－3E就可在某些目标国家的无线通道处，截获空中传播的微波和其它信号，并进行融合和处理。总之，从这次EP－3E侵入中国南海上空侦察的事件，可以清楚地看到，网络战正向我们悄然走来。

网络在现代战争中的作用

美国著名的未来学家托夫勒在他和他夫人合著的《战争与反战争》一书中写道："一个国家创造财富的手段就是它制造战争的手段。"网络技术既为人类提供新的资源，又为人类提供了新的战争手段。

广义地讲，网络战就是在计算机网络领域进行的斗争，可分为全球网络战和战场网络战。全球网络战是指国家或集团围绕和运用国际计算机网络进行的政治、经济、文化、科技、军事等斗争。它是以争夺21世纪经济制高点为直接目的，集政治、经济、文化、科技、军事为一体的总体战。狭义的网络战，则专指战场网络战，即指战争中交战双方围绕和运用战场信息网络进行的对抗。战场网络，则是指利用网络技术，把上至高级指挥部，下至单个士兵以及各种武器系统的所有信息，通过网络联结成一个整体，实现军队作战信息共享，以满足军队的实时战斗要求。

互联网技术的发展，将使战场信息网络成为交战双方对抗的核心和焦点。网络在未来战争中的作用，不仅体现在网络攻防这种简单的作战样式上，更重要的是，网络在军事上的综合运用，将给未来战争带来的一系列深刻的变革。

无缝联接提高作战效率

今天，纵横交错的计算机网络正在加速将社会各领域，包括国防与军事系统，紧密联成一个巨大无比的无缝连接的网络系统。网络经济将是直接经济，即生产者和消费者直接见面的经济。与此相对应，军队作战也将因无缝联结的网络而引发直接作战。即在作战指挥中，不再需要走大量的迂回路径，而是变得更加直接、更加便捷。在直接作战中，通过网络的横向联结，一方面结束了发现和摧毁的分离现象，大大提高了作战效率。另一方面由于网络的作用，降低了作战中的物质消耗和人员损失。在未来的战争中，可以通过重点的精确打击，以及采用瘫痪敌人网络系统的方式，使对方丧失战斗力，进而迫使敌人放弃抵抗。

信息共享促进实时指挥

无疑，网络在现代战争中，将成为军队战斗力的倍增器。利用网络，将会大大提高指挥员的指挥效能。在大多数情况下，网络中的指挥，将改变机械化战争时代高度集中的指挥方式，转而实施高度分散的指挥。不仅各级指挥人员会享有前所未有的自主权，而且分布式无缝指挥网络，在需要时将使每一个战士都有可能了解某些全局情况，执行发现敌人并引导其他部队攻击的任务。同时，在某些事关全局的行动中，战略决策也可能由决策层直接下达到战斗小组一级，从而可将指挥员的意图实时地付诸行动。

扩大时空展现高度协同

机械化战争扩大了作战的空间，整个战争的时间延长，且部队的兵种构成复杂，协同变得越来越困难。因此，

在机械化战争中，随处可见部队协同失调的现象。网络克服了机械化战争难以跨越的地理上和时间上的障碍。战场指挥员和战斗员，可以利用手中的计算机终端设备，通过战场信息网络，实时了解自己和友邻的所有情报信息。各种命令、指示、情况通报将以文本、图表、静态或者动态图像的形式，在事件发生的同时，立即展现在指战员面前。

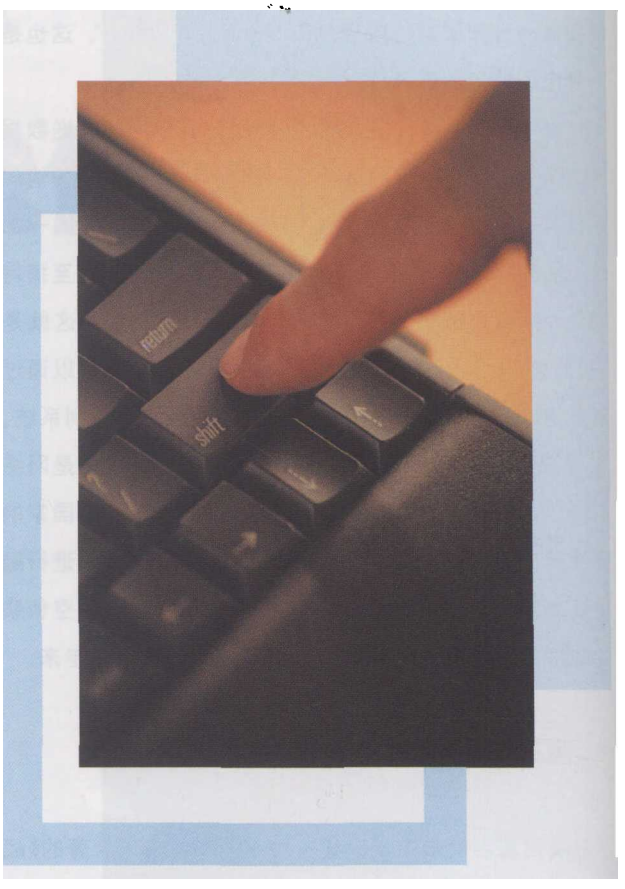
网络补给实现精确保障

在未来战争中，可以利用自动化补给网络系统，跟踪监测作战部队对各种物资的动态要求，并将所需物资和勤务，及时、准确地送到各战略、战役和战术单位。精确保障的目标，是要做到在适当的时间，输送适当的物资到适当的地点，这将彻底改变机械化战争时代大规模集结保障的传统方式。实现信息、后勤、运输技术的网络一体化。通过网络，后勤部门不但可以了解前方的物资消耗情况，而且可以找出最短的运输路线和最快的运输手段。由于在物资中嵌入了信息装置，使得对物流进行全程监控成为可能。

网络战正向我们走来

正由于上述网络在现代战争中的重要作用，各国已经高度重视对网络的攻击和防御，并加紧研究保证网络安全的对策。美国军方作为全球网络化水平最高的军队，未来几年将投入17亿美元专项巨资，积极准备21世纪的网络战。美国军方一方面积极发展网络防护技术，另一方面也注重发展网络攻击技术，以增强自身的网络攻击能力。实施网络攻击，是干扰、阻止、削弱或破坏敌方计算机和网络上的信息流，或破坏敌计算机和网络本身的作战行动。从而，它可为美国军事力量带来巨大的利益。

美国网络战的中心－美国国防信息系统研究所相信，未来的战争绝不只是战场上的较量，所谓"无接触战争"的胜败，将成为决定整个战争命运的关键。目前，供职于



该机构的电脑工程师们的主要职责，是维护美国军方使用的250万台电脑，主要任务是防止黑客袭击。然而，从某种角度说，这里本身就是个"黑客帝国"，因为这些电脑工程师，在防止黑客袭击的同时也充当黑客的角色：在看不见的网络后面，凭借雄厚的技术优势和创新的信息技术，研究如何提高电脑的攻击能力，制造破坏敌对国家的通信网络、金融系统、电力系统的入侵病毒。

其实，网络战已大大超出了黑客袭击的含义。实际上，美国在网络战领域的研究已取得了重要成果，并已拥有一系列强大的攻击性的网络武器，其中包括：

(1)计算机及网络病毒 目前美军军用计算机病毒技术，远远超过别国的病毒监测技术，美军已研制出具有超强破坏能力的军用计算机病毒，计算机芯片固化病毒，及计算机病毒无线输送装备等。

(2)计算机及网络探测器 为了进入敌计算机网络系统，并成功地实施信息攻击，美国正在研究网络系统分析

器、软件驱动探测器和硬件磁感应探测器等网络系统探测武器，以及服务否认、信息篡改、中途窃取和欺骗等技术装备，部分技术已日趋成熟。

(3)计算机及网络"肌体"破坏武器 美国国防高级研究计划局(DARPA)正在研究用于破坏电子电路的微米／纳米机器人、能嗜食硅集成电路芯片的微生物等网络攻击武器，这些技术有的已经取得阶段性成果。

这些网络武器可以通过无线电发送系统进入敌方网络系统。使用战术或战略无线电系统发送带有计算机病毒、逻辑炸弹等信息，当对方接收系统接收后，可以激活信息中潜伏的病毒，进行大量的繁殖，并进行数据的删除和涂改。也可利用各种后门，采用无线输入或提前植入目标系统等方法，将病毒、逻辑炸弹等送入目标计算机系统中去。除此以外，黑客们利用当前计算机采用开放结构的特点，在军队普遍使用与民用相同的编程语言的情况下，可从计算机操作程序的缺陷中找出漏洞，再使用专门的破译软件，在系统内部破译超级用户的口令。为此，美国国防部专门成立"红色小组"，使用网上黑客们常用的解密技术对国防部计算机系统进行解密试验，以便找出计算机系统的缺陷，同时演练网络攻击战术。最后，美国是计算机的核心模块－"中央处理器"的生产大国，也是其他组件如主板、内置式调制解调器的生产大国。全球销售的约90%的计算机使用了美制芯片，这将为美国将带有病毒的计算机系统直接或间接卖给目标国家，创造了有利条件。

网络战催生了"网络兵"或"计算机防护兵"这一新兵种。目前，美国陆、海、空三军中都设有计算机应急反应部队。例如，美国空军于1996年8月在南卡罗来纳州的空军基地成立了609信息战中队。其55名成员，是从受到特殊训练的计算机操作和监控人员中择优录取而来。其主要任务是通过下载过去24小时内访问计算机网络的情况，来掌握非法入侵网络的活动，并采取有针对性的防御性措施。目前，该中队正在开发一种自动化管理系统，以具备适时发现非法侵入信息网络的活动并自动采取相应防护措施的能力，提高信息防护的主动性。美国陆军计算机应急反应分队的职责，是与陆军自动系统安全应急支援分队一起，维护各陆军基地的信息网络系统的安全，其重点是对付战术层次的计算机，特别是自动化指挥控制系统的威胁。美国陆军正计划在欧洲和太平洋战区建立类似的应急分队。美国海军的计算机应急分队，隶属于大西洋舰队的"舰队信息战中心"。该分队研制的自动安全事故检测系统，能够改进信息系统的监控能力，并成为美国海军在网络安全方面，集成监视、侦察和反应能力的基础。它可识破未授权人员闯入海军网络的企图，并向有关人员报警和对"入侵事件"进行自动记录。

除美国外，其他国家在网络战方面也有很大进展。俄军对网络战的理论研究起步较早，并且在实战中进行了试验。在未来战争中，网络战"实际上已成为一种变相的突击样式，起到了与火力突击效果相同的作用"。众所周知，俄军击毙车臣分裂分子杜达耶夫，就是一次小小的网络战的演练，从中可以看出他们打网络战的水平。

今年5月5日，在印度西部拉贾斯坦浩瀚大漠中，印军开始了13年来规模最大的"全胜"联合演习。演习中印军大量使用被称为"力量倍增器"的信息装备，诸如监测与探测雷达、通信加密装置以及传输数据、图像和传真等信息的数字化侦察与通信设备等。据报道，印度三军目前正力争实现全军各网络系统联网，最终形成国家、战略、战役和战术层次上的联网。为了能够及时处理敌方对印军网络的攻击和非法入侵，印军组建了陆海军三军联合计算机应急分队。在加强网络的安全防护方面，印军采取的主要措施包括对指挥控制系统的各个信息单元，如武器制导系统和监视系统定时更换内置密码，以防止敌人识别并利用诱导控制信号操纵己方网络；杜绝高级平台用主动方式收集和传递信息，以避免暴露己方平台；在信号编制和线路设计时，采取抗干扰措施，以避免敌方刺探己方网络。其他措施还包括引进防火墙技术以保护网络和系统，建议使用印度古代梵文设计密码等。

目前美国军队内部对网络战的认识，在总体一致的前提下，还存在一些分歧。激进者认为，必须改变那种认为军事力量主要是飞机、军舰和坦克的概念，而应把注意力

更多地放在信息技术所能提供的军事力量上。保守者则认为，网络战攻击成功靠的是运气，其威慑价值值得怀疑。他们认为，网络战倡导者所面临的最大风险，是过分吹嘘网络战的功效和潜力。实际上，任何战争手段都有风险。在进攻的同时都必须进行防御。一般来说，易攻难守，网络战也不例外。而且，在网络战中，强弱不像常规战争中那样明显。常规意义上处于弱势的一方，只要一次得手，进入到对方的"神经中枢"，就可能在顷刻间扭转战争局势。美国虽号称在网络战方面实力过人，但也常在小河里翻船。由于美国军方近95%的信息，是通过未加密的商用网络传播的，网络的开放性使得五角大楼像一般商业网站一样，容易受到袭击。早在1997年，来自美国的一群专家就曾利用互联网上的黑客程序同时侵入了 9座城市的电网控制系统和911报警系统，并侵入了五角大楼的36个电脑网络系统。这些侵袭行动只有两例被查出。 1998年，五角大楼的约500台电脑再次被袭击。后来发现，肇事者竟是两名加州少年，他们的"师傅"不过是一名18岁的以色列青年。仅去年一年，黑客侵入美国军方电脑网络的次数就高达413次。不少美国军事专家担心，对付黑客尚且如此费力，如果是敌对国家或恐怖组织有组织的大规模网上袭击，五角大楼将如何处置？另一方面，网络系统也肯定会存在薄弱环节，例如在这次美国9月11日 飞机撞楼爆炸的恐怖袭击事件中，它的先进军事网络系统竟来不及反应，正说明了这个系统还有一定的脆弱性。但不论保守还是偏激，无可否认的是：网络战在现代战争中将起愈来愈重要的作用。

结束语

在信息时代，信息已成为现代战争的重要资源。军队为打赢战争，不仅要广泛地运用信息资源，而且还要采取相应的措施，确保军事网络系统的安全。此时，主要军事威胁之一是来自敌方对国家和军队的"中枢神经"－网络系统的突然袭击。军事信息在存储和传输过程中，如何不被修改，不被破坏和不丢失，不被敌方侦察和获取；网络系统如何能够始终保持正常运行；作战中如何保证随时存储和调用所需要的信息，就成为现代战争所面临的突出问题。为确保信息化战争中，始终掌握战场上信息斗争的主动权，当前需要认识军事网络系统安全对作战胜负的巨大影响，并采取积极的措施，作好进行网络战的准备。为保护己方军事网络系统的安全创造有利的条件，还必须采用有效的网络安全的技术手段，使信息处于严密的封锁状态，以便有效地防止敌方的信息侦察的信息防泄露技术等。

世界其他国家，包括我国在内，在网络战的能力方面，与美国存在较大差距。特别是其它国家的计算机网络大都依赖美国制造的软件和芯片。但前述的网络战的这种不对称性，在一定程度上，是否会更有利于常规意义上处于弱势的国家？更重要的是，战争的胜败从来不仅仅取决于技术和装备的优劣。最近，北约指挥科索沃战争的盟军司令克拉克，在《时代》周刊发表的《我们将如何作战？》一文的最后指出："我们的武装力量必须拥有最新的技术和充分的灵活性，以在政治上的制约的限度内实现既定目标。但最重要的是，我们仍将需要有才能的、足智多谋和勇敢的男女战士，以实施和指挥我们的军事行动。"历史证明，不管是在冷兵器时代还是网络时代，人仍然是决定战争成败的关键。