窥视三场局部战争

计算机网络战

□ 魏岳江 黄铁成

计算机网络战是指敌对双方在计算机网络领域为争夺制网络权，通过削弱、破坏敌方计算机网络系统的信息和使用效能，保障己方计算机网络系统的信息和安全运行而展开的信息作战行动。由此可见，计算机网络战属于信息作战范畴，其作战目的是夺取制网络权，作战对象是敌方的计算机网络，作战主体是用信息技术和装备武装起来的网络战士，作战区域是广阔的计算机网络空间，作战手段是根据计算机技术研制的各种病毒、逻辑炸弹和芯片武器等。

计算机网络战分为平时和战时计算机网络战、全球与战场计算机网络战、计算机网络侦察、进攻与防御作战。其特点：以夺取和控制制网络权为首要目的；作战行动不受时空阻隔，更加主动、突然；作战力量构成军民一体，既军也民；作战手段具有高技术性和多元性；作战行动一体化，效费比高。

计算机网络战的出现既有时代的背景、技术的牵引，也有其历史的渊源。20世纪90年代，世界上爆发了以海湾战争、科索沃战争、伊拉克战争为代表的高技术局部战争，在这三场战争中最引人注目的是计算机网络战。

海湾战争—计算机网络战初露锋芒

1991年的海湾战争，网络战被第一次搬上了战场。在这场战争中，美国五角大楼的网络系统遭到极其猛烈的攻击，数百件美国的军事机密文件被黑客们从计算机中窃取出来，提供给了美国的战争对手伊拉克。荷兰一个叫哈卡的10岁男孩通过因特网侵入美国国防部的电子计算机系统，盗走了部分机密资料，改动、复印了部分资料，并把一部分美军兵员、装备和武器系统的绝密情报公之于众。除此之外，还发生了多起针对美国军用计算机网络系统的“黑客”行为，使美军饱受惊吓。海湾战争“沙漠风暴”行动前夕，做好了临战准备的多国部队建立有史以来规模最大的C^4I系统，该系统保证了多国部队的指挥控制、情报分发、作战支援等能力，成为多国部队的神经中枢。在这个神经中枢指挥下，多国部队以“白雪”电子战行动为序幕，拉开了一场大规模信息作战实验。在这场信息作战中，计算机网络战开始崭露头角，首次登上人类战争的舞台。据报道，战争爆发前，美国向伊拉克准备从法国订购的防空指挥系统的计算机中心的电脑打印机内，预先植入计算机病毒。战争中，美军用无线电遥控装置将隐藏在计算机中的病毒激活，当伊军实施电脑打印时，病毒开始发作，致使伊军防空系统处于瘫痪。美军虽然成功地使用计算机网络战攻击了伊拉克，但其计算机网络系统也受到了网络攻击。战争中，美军20%的情报在互联网上都未加密，很容易受操纵或者干扰。

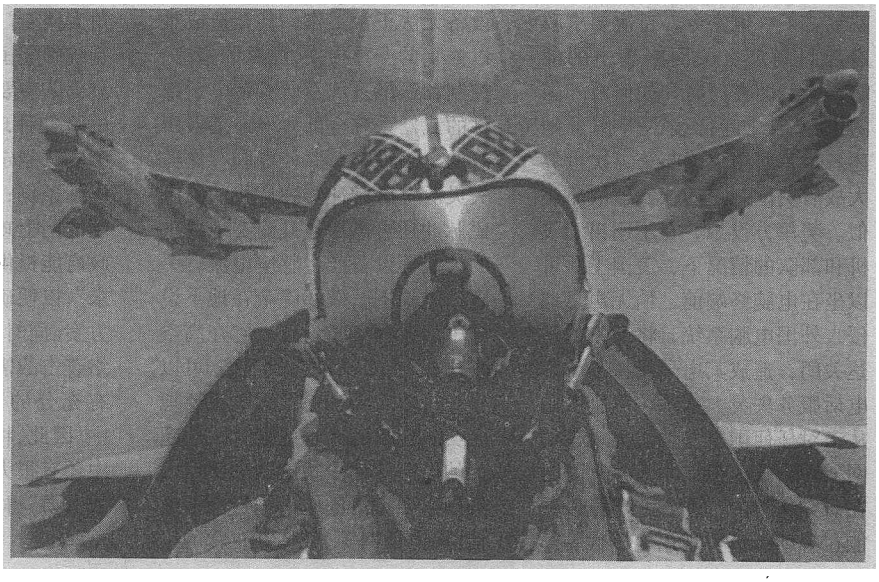
科索沃战争—计算机网络战大显身手

在科索沃战争中，以美国为首的北约遭到来自全球范围反战黑客攻击。1999年3月28日，北约某站点因受到攻击而被迫对公众关闭；3月31日，北约互联网址及电子邮件系统受到南

联盟黑客攻击，使其电子邮件服务器阻塞。一段时间内，北约某站点每天都收到2000封发自南联盟的电子邮件，使北约负责电脑网络的官员大伤脑筋，惊呼这是北约有史以来所遭到的非武力所能解决的最大难题；3月29日，俄罗斯黑客入侵美国白宫网站，致使该网站服务器瘫痪半小时，并对英国网站实施攻击，使北约空袭中最需要的英国气象局网站损失惨重；美空袭我国驻南联盟使馆时，中美黑客也展开网上较量。中国黑客攻击了美国白宫和驻华使馆等站点，并在网上公布了美国200多个网站的密码。空袭开始后，英国和美国新闻媒体分别在因特网上设置了“北约空袭”、“科索沃危机网站欢迎来信发表见解”、“南斯拉夫最新发展”等常设链接，大量歪曲报道战争事实真相。南联盟也积极实施网络攻击。其主要报纸、电台和一些政府部门都在网上设立了自己的主页，如“塞尔维亚信息”等，宣传南联盟政策，揭露北约的暴行。此外，南联盟民间网络战士也直接参人了网上对抗。

伊拉克战争—计算机网络战紧擂战鼓

伊拉克战争中，人们从电视画面上看到了飞机的轰鸣、导弹的轰炸、防空的火舌和地面的激烈交战场面，而没有看到一场没有硝烟的战争——计算机网络战。来自世界各地的电脑黑客纷纷施展绝技，从远隔千里的键盘上操作战场鼠标，定下攻击决心，导演了一场没有硝烟的战争话剧。早在2002年12月，美军在海湾地区举行了一个代号为“内部观察”的军事演习中，就建立了“漂移的军事指挥所”即“网络指挥部”。它将指挥中心与陆、海、空三军的战场信息系统，甚至单兵联为一体，实现了信息共享，随时能了解战场动态、定下决心、发布命令。战争中，美军“网络指挥部”指挥“网络特种部队”，使用2000多种计算机病毒，向伊拉克发起网络攻击，摧毁伊拉克军事通信系统，使伊拉克军队得到错误信息或者得不到任何信息。伊拉克战争前几天，数千名伊拉克人在他们的电子信箱里发现了一封封类似于发信人被掩盖的邮件。“放弃吧。起义并倒戈。到另一方来，否则美国人就开战了。”正当美军士兵被派往海湾地区，与此同时，在美国，网络攻击也在高速运转。3月20日，随着巨大的爆炸声震碎了巴格达凌晨的宁静，美国对伊拉战争宣布打响。在因特网上，一场针对美国的战争早已无声无息地开始，也进行得如火如荼，平均每天发生2500起攻击美国网络事件。一个黑客组织立即对近400家美国网站进行了攻击，此后越来越多的电脑黑客针对美国公司网站的攻击频率明显上升，其中多数攻击是为抗议美国发动对伊拉克战争。战争中，全球电脑黑客们改变了关注的对象，专打北美网络目标，特别是阻塞商业入口网站，干扰企业的计算机，使企业活动受到很大影响，给全世界计算机系统造成20亿欧元的损失。电脑黑客本是一群游戏在网络不大关心政治的人，而在战争中他们攻击过的网站，都保守清晰的政治问题，指责美国，使美国农产品应用国家中心和美国海军在内的数家网站被黑，其中包括英国首相布莱尔的官方主页“唐宁街10号”，出现短时间的瘫痪。战争中，黑客的主要攻击目标是美英两国中小企业和非赢利机构的网站。由于这些网站的防黑客措施相对简单，黑客们可以比较容易地把反战图画或者标语插在这些网站的网页上。此外，黑客们还大量地采用了拒绝访问攻击手段，向一些网站的服务器发送大量请求信息，导致这些服务器因为数据堵塞而陷入瘫痪。战争中，为了及时报道美伊战争的情况，半岛电视台在3月24日推出英文网站，但是第二天就受到黑客袭击，网站出现技术故障，同时半岛电视台的阿拉伯文网站也遭到黑客袭击。这些网站有4小时无法更新网站资料。战争中，美国最厉害的一招就是利用黑客及大量的“倒萨”电子邮件攻击伊拉克的互联网，给伊拉克军官发送电子邮件，鼓励他们背叛萨达姆。同



时，每日还有数千名伊拉克人会收到诸如“离开吧！”，“如果你们不行动，停留在你们驻扎的地方，我们将不攻打你们，如果你们一参战，将会受到致命打击！”等内容的电子邮件。这样的电子邮件对伊拉克部队的官兵是一种强烈的攻心战。这一做法，一方面使伊拉克的互联网难以正常工作；另一方面使伊拉克人一打开电子邮箱，看到的全是“倒萨”的邮件。在这种情况下，伊拉克不得不全面关闭了本国的互联网。这虽然对美军的信息战起了抑制作用，但是也给伊拉克造成了巨大损失。美军通过电子邮件与伊国内反对派及伊军中有叛国动向的军官联系，用网络传输信息这一秘密的方式获取伊拉克军事情报，特别是刺探萨达姆的行踪。据报道，美军3月20日凌晨对巴格达的第一次空袭就是在接获伊拉克内线人的所谓确切情报后发动的。情报透露萨达姆当时正住在位于巴格达杜拉区的一所民宅内，所以美军才发射了“战斧”巡航导弹。

未来高技术局部战争—计算机网络战招法翻新

2003年1月，美国总统布什下令制定一个网络战略，以便在必要的情况下对敌人的电脑系统发动袭击。报道说，布什去年7月就签署了一道密令，首次要求政府部门制定有关网络袭击的战略，就美国在何时和如何对外国的电脑系统进行袭击等作了阐述。这一网络战略与第二次世界大战后美国制定的核武器战略类似。美军方设想，在不用出动飞机和部队的情况下，美国士兵可以坐在电脑终端前，悄无声息地侵入外国电脑系统，将敌人的雷达关闭，造成其电子指挥系统和电话服务失灵。据悉，尽管美国从未对任何国家发动过大规模的网上袭击战，但五角大楼却一直在研究所谓的“网络武器”，以便能在有朝一日实现用电子代替炸弹，对敌人发动更快速、“少流血”的远程袭击行动。那样，美军通过在电脑终端前轻松敲打键盘，就实现了让敌国雷达系统失灵、电力供应彻底中断、通信全部紊乱之目的。《华盛顿邮报》报道，布什政府一直对获取各类“可改变战争方式”的武器系统非常感兴趣。白宫官员表示，美国现在完全有能力对敌人发动“网上破袭战”。不过，由于美国自身也大量依靠电脑网络体系，如果在时机尚未成熟时贸然对敌人发动黑客战，很可能导致自己的电脑体系也同时遭到来自敌人的毁灭性袭击。此外，由于破坏敌人的电脑体系将会把“军民系统”一网打尽，因此白宫在此事上的做法显得“异常谨慎”。比如，通过网上打击，可让负责向军方供电的电厂瘫痪，但最后结果却很可能同时导致旁边的医院也给“黑”了。为了防止这种“伤害无辜”的事情发生，美国宣称，不会采取向网络上散步“蠕虫病毒”之类的做法。伊拉克战争中，美军使用一种电磁脉冲炸弹，是一种介于常规武器和核武器之间的新式大规模杀伤性炸弹，在目标上空爆炸后，会辐射出高强度的电磁脉冲，覆盖面积大，能够使半径数十公里内的飞机、雷达、电子计算机、电视机、电话、手机等几乎所有的电子设备无法正常工作，甚至造成难以修复的严重损伤，那里的指挥、控制和通讯系统及所有带电子部件的武器系统全部瘫痪，摧毁所有的电子设备，并使电脑存储器失灵。电磁脉冲炸弹产生的强电磁脉冲还可能通过暴露在地面上的天线等设备产生感应电流，一直钻进地下，破坏隐蔽在地下设施中的各种电子设备。它在高空爆炸，不会对平民造成损伤，可以作为进攻武器，对敌国的重要地区实施连续的高程度轰炸，用超强的电磁脉冲干扰甚至彻底瘫痪敌国重要地区的电力输送网、通信网、电视网等，破坏其正常的生产和生活，给民众带来巨大的心理压力。在1999年北约对南联盟的轰炸中，美国使用了尚在试验的微波武器，这使南联盟部分地区的各种通信设施瘫痪了3个多小时。面对网络时代的新挑战，美军把培养计算机勇士纳入了训练重点，专门开设了计算机勇士培训班，普及有关的软件和硬件知识，着力于建设相应的“网络部队”来争锋网络战场，“计算机勇士”成为其致力发展的新兵种。目前，美空军成立了计算机应急反应分队即空军609信息战中队。该中队于1996年8月在南卡罗来纳州的空军基地成立，共有55名成员，从受到特殊训练的计算机操作人员和监控人员中择优录取；美陆军计算机应急反应分队的职责是与自动系统安全应急支援分队一起维护各陆军基地的信息系统安全，但其重点是对付战术层次的计算机威胁，特别是自动化指挥控制系统；美海军计算机应急反应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，并且成为美海军在安全机构中集成监视、侦察和反应能力的基础。它可识别未授权人员闯入美海军网络的企图，并向有关人员报警和对入侵者进行自动记录。目前，五角大楼专门委派了一名将军来负责统帅美国的“网上特种兵”。这只部队主要有三方面任务：第一，试验各种现有网络武器的效果；第二，制定美国使用网络武器的详细条例；第三，培训出一支“过硬的网上攻击队伍”。美军希望，政府能提供“确切的网上打击要求”，以便确定自己的作战手段和方案。同时，发动有效的计算机网络袭击战需要对敌人的电脑系统有充分的了解并能有效进入其中。因此，将现有技术应用到实际中还有很大距离，美军发动电脑战需要“得到最高层的批准”。