□ 张海龙

黑客帝国

美国网络战部队揭密

今年9月3日，英国《金融时报》引述美国官员的话称，中国军方黑客6月侵入五角大楼计算机网络，对美国国防部实施了最为成功的网络攻击。针对外国媒体的肆意诬蔑，中国予以严正驳斥。在9月4日的外交部例行记者招待会上，我国外交部发言人姜瑜在答记者问时说："中国政府一贯坚决反对和依法严厉打击包括黑客行为在内的任何破坏网络的犯罪行为。在中美致力于发展建设性合作关系，中美两军关系呈现出良好发展势头的大背景下，有人对中国进行无端指责，妄称中国军方对美国国防部实施网络攻击，这是毫无根据的，也是冷战思维的体现。"

极具讽刺意味的是，美国一面在指责受到他国黑客的攻击，一面组建了一支世界最为强大的黑客部队，对世界的网络安全构成了严重的威胁。随着互联网的日益普及，网络战已经成为另外一个重要战场，对于美国的举动我们不能不有所警惕。

◎ 信息安全之忧

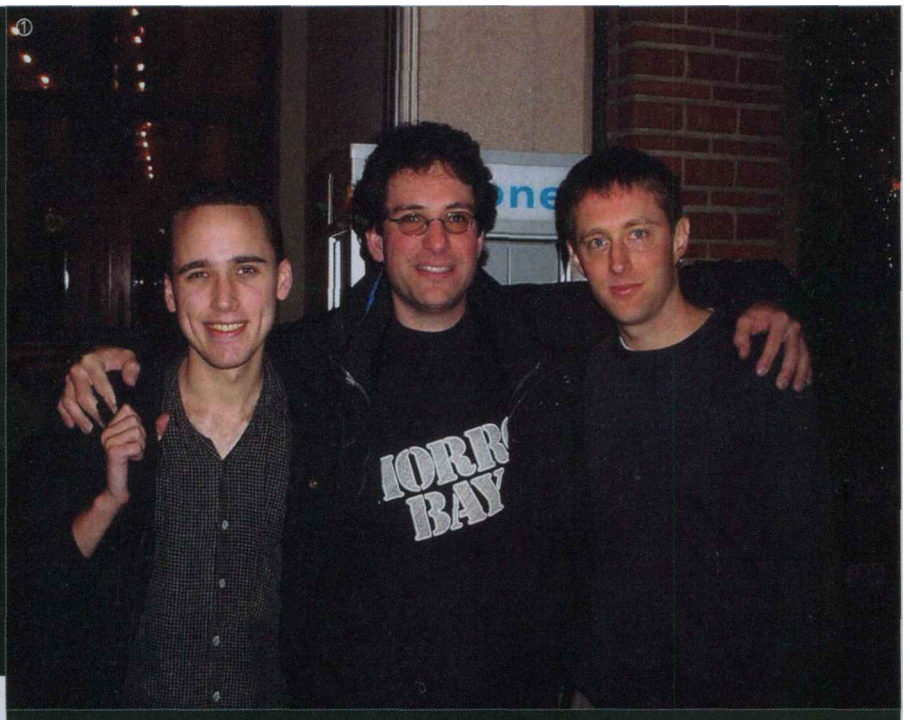
今年年初，美国联邦调查局的一份评估报告披露，最近频繁发生的针对美国政府部门和军用计算机网络的攻击事件，很可能是亲伊朗的"恐怖分子"黑客所为，这使得美国国家安全面临"潜在危机"。其实美国政府和军队网络遭黑客攻击早已不是什么新鲜事。据美国媒体报道，由于遭到黑客大量无休止的攻击，美国网络安全日益面临严重威胁，给美国的安全带来了巨大的危害。美军方也强调，来自黑客的网络袭击对美军方网络"威胁很大"。早在上世纪90年代初，曾被誉为"世界第一黑客"的米特尼克，15岁时就利用家中的电脑侵入了北美防空司令部指挥系统的网络系统。2005年2月，三名来自希腊不同大学的网络黑客成功地入侵了美国军方位于亚利桑那州的最高电子指挥系统，造成军方指挥系统因接获错误讯息而陷入紊乱。2006年11月，为窃取美海军演习的秘密资料，黑客对美国海军学院电脑系统进行攻击，最终导致该学院电脑系统瘫痪，被迫切断互联网服务数周之久。以上所列仅仅是美政府和军队网络系统遭到黑客攻击的"冰山一角"。被入侵的政府网站包括国防部、国务院、能源部、国土安全部等重要政府职能部门，其中以国防部最为严重，在2004年达到1300多次。

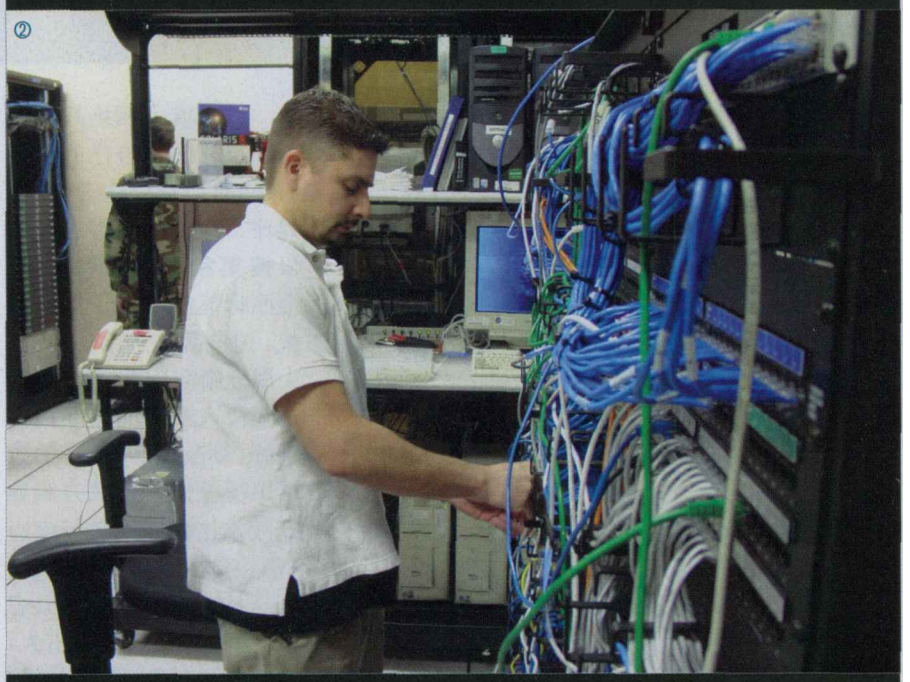
专家分析，随着互联网深入到社会的方方面面，军事和民用的界限越来越模糊，且相互依赖。据美国国防部国防信息系统局披露，目前美军95%的军用通信要依赖民用通信。因此，黑客要破坏其军队的通信网络，既可通过军用通信网络直接实施，也可从民用系统入手，从而给了其更大的发挥空间。

◎ 大力打造黑客部队

为了应付网络黑客的种种攻击，防止出现"网络9·11事件"，早在2002年，美国总统布什就签署了"国家安全第16号令"，要求由国防部牵头，组织中央情报局、联邦调查局、国家安全局等政府部门制定网络战战略。美军为了应对未来的信息战，首次提出了"网络中心战"的新型作战模式，美国战略司令部据此组建了美军网络黑客部队——网络战联合功能构成司令部（JFCCNW）。为统一指挥，更好地组织实施网络战，美军于2005年对战略司令部进行了重组，这个在冷战中以策划和统筹全球核打击为主的最高指挥机关，被赋予了统领全军网络战的重任。此举标志着此前由黑客们进行的"网络游击战"正逐步向未来由正规"网军"部队进行的"网络正规战"演变，美军网络战由此正式登上历史舞台。

前美国海军陆战队指挥官、从事网络恐怖情况调查的资深情报专家唐·维顿称，战略司令部所属的"网络战联合功能构成司令部"由世界顶级电脑专家和黑客组成，其人员组成包括美国中央情报局、国家安全局、





① 照片中间的人物就是有着“世界第一黑客”之称的凯文·米特尼克，他在15岁时就曾侵入北美防空司令部的主计算机，后来又侵入多家著名跨国公司和政府部门的计算机。1995年米特尼克终因网络犯罪而被判5年徒刑，2000年假释后被法庭禁止在3年内的监视期内接触计算机。他现在正运营着一家网络安全公司。
② 一名美军的技术人员正在检查，计算机的网络连接，互联网的应用使美军的作战能力大大增强，但同时也留下了脆弱的软肋。

联邦调查局以及其他部门的电脑专家，甚至还可能包括盟国的顶级电脑天才。由于其所有成员的平均智商都在140分以上，因此也被一些媒体戏称为“140部队”。2003年爆发的伊拉克战争中，美军网络战部队牛刀小试，进行了试验性作战，取得了显著战绩。同时，美军也意识到，在未来战场上，网络将成为战争和舆论宣传的发展方向，其胜负对战争结局有着至关重要影响。因此，美国国防部又在2006年底组建了网络媒体战部队。网络媒体战部队成员既是电脑高手又是出色“记者”。他们全天候24小时监控互联网，以便及时纠正错误信息，帮助美军对付“不准确信息”并积极引导利己报道的传播。

其实，除了组建JFCCNW、网络媒体战部队、重组战略司令部外，美军还在各军种配置网络作战力量和指挥机关。目前，美国陆、海、空三军都组建了各自的网络部队，执行战场战术行动。美国陆军建立了“计算机应急反应分队”，其职责是维护陆军各基地信息系统的安全，必要时可发起信息网络攻击，侵入别国军事网络，进行破坏、瘫痪甚至控制；美国海军也成立了“舰队信息战中心”及下属的“海军计算机应急反应分队”；美国空军则建立了专门负责实施网络进攻的航空队——第8航空队，其属下包括大名鼎鼎的第67网络战大队，其任务是保证美空军在战时和平时都能够实施网络战、攻击潜在对手。此处，美空军还成立了计算机应急反应分队即空军609信息战中队，空军情报局还成立了第92信息战入侵队。据英国《简氏防务周刊》报道，美国空军目前正以第8航空队为依托，组建空军网络战司令部。据称，网络战司令部将与空中作战司令部、空中机动司令部等同列为一级司令部。有专家指出，此次美空军成立网络战司令部的目的，在于进一步整合空军现有网络作战力量，提高网络一体打击效能。可以看出，美军对网络战的应用与空中打击有几分相似：美军陆、海、空部队都具有自己的空中打击力量，又在最高层次设一个统一协调部门，网络战部队的情况也是如此。

自20世纪90年代尤其是2002年美国国防部正式将“网络中心战”列为美军未来主要作战样式后，美国各军种都积极储备各自所需的网络战人才。1995年6月，美军16名“第一代网络战士”从美国国防大学信息资源管理学院毕业。他们的任务就是利用计算机在信息空间与敌人展开全面信息对抗。除了自己培养外，美军还一直以不公开的方式到“黑客市场”招兵买马。美军情报人员还经常深入黑客组织中间，组织有众多电脑专业人员参加的电脑黑客大会，其目标就是寻找天才黑客加入美军的行列。此外，美军还雇

用一些黑客专门从事计算机漏洞测试的工作。按照计划，整个美军的网络战部队将于2030年左右全面组建完毕。届时，它将担负起网络攻防任务，确保美军在未来战争中拥有全面的信息优势。有人预计，在信息化战场上，“黑客部队”将作为一个年轻的兵种而产生，并在信息作战中发挥巨大的作用。

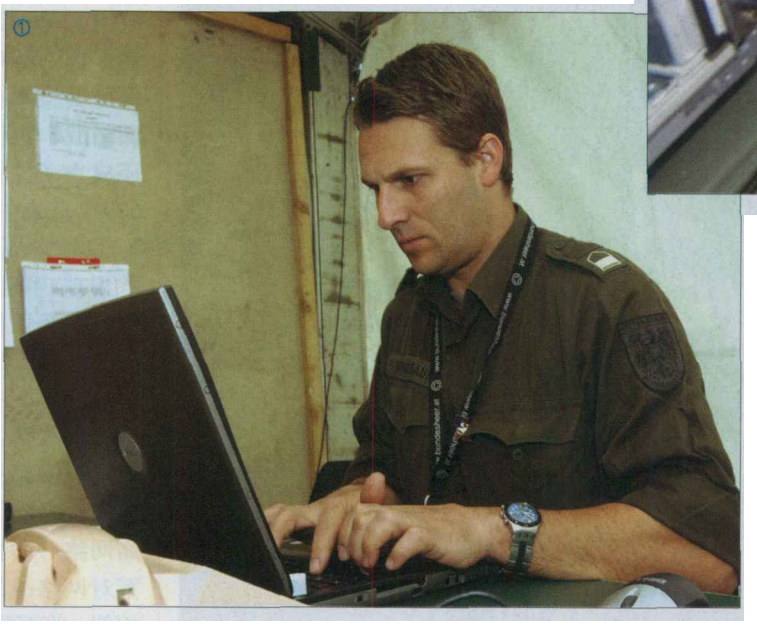
◎ 三大任务

据媒体报道，美军一直大力研究网络战，就是希望在不远的将来能用电脑代替炸弹、用网络代替枪炮对敌人发动更快速、更少流血的远程袭击。那时，美军士兵只要坐在电脑前轻松敲打键盘、点击鼠标，就能让敌方制导武器偏向、雷达系统失灵、通信、电力系统中断，甚至让对方无法调兵，不能发射导弹，只能被动挨打。JFCCNW正是这样的一支部队。据知情人士称，JFCCNW的成员掌握着世界上最先进的网络技术，能够轻松渗入敌国军事和民用信息网络系统窃取或假造数据，并可以释放病毒致瘫敌方的指挥和控制系统，使敌方无法指挥地面部队或发射导弹。同时，该部队还担负着防护美国国防部所有网络免遭攻击的任务。

据悉，五角大楼现在已经专门委派了一名将军来指挥这支“超级黑客”特种部队。这支部队当前主要有3方面任务：一是试验各种现有网络武器的效果；二是制定美国使用网络武器的详细条例；三是培训出一支过硬的网上攻击队伍。JFCCNW平时通过攻击自身的信息系统发现结构隐患和弱点，一旦爆发战争，将承担渗透、监控、摧毁敌网络系统以及窃取情报的任务。据五角大楼官员透露，美军发动“黑客大战”需要“得到最高层的批准”。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。

◎ 作战方式

对于网络战这样一种重要性日益凸现的作战样式，美国军方十分重视，现已将网络战纳入各种重要作战条令。早在1998年10月，参谋长联席会议颁发的《联合信息行动条令》中，就对“如何实施信息战中的计算机网络攻击”进行了详细论述。在2001年6月发布的美国陆军部新版《作战纲要》中，对“陆军部队如何实施‘信息行动’中的计算机网络防护”进行了重点规范。从2002年开始，美国国防部已正式将“网络中心战”列为美军未来主要作战样式。



近年来，美军为了加强网络黑客部队的实战水平，提高网络“反黑”能力，不断创新网络攻击技术手段进行了大量的网络战演习。当前，美军已初步建起了以各军种信息战中心的“红军”、计算机应急分队等为主的“网络勇士”，并多次与著名的智囊团兰德公司进行计算机网络安全模拟演习。2006年2月6日至10日，华盛顿上演了最大规模的网络战演习——“网络风暴”行动。美国所有的重要部门包括白宫国家安全委员会、国防部、国务院、司法部甚至英国的官员也前来观摩。

专家指出，美军未来的网络战将是融黑客式网络打击、实体打击、心理打击于一体的综合作战：

1.黑客式网络战。美军在严密防护自己的网络系统同时，通过病毒、木马程序、逻辑炸弹等进行情报搜集和网络阻塞攻击，全面瘫痪敌方电子信息系统，迫使敌信息系统关闭，大规模偷窃敌方信息数据，甚至侵入敌军的作战指挥系统，篡改控制信号，使数据出现差错，使敌方制导武器偏向，让敌军指挥系统接受虚假信息、对战场形势作出错误判断，甚至调动对方军队。据美国《C⁴ISR》杂志披露，2003年伊拉克战争爆发前不久，美国获悉伊拉克从法国购买了用于防空系统的新型电脑打印机，准备通过约旦首都安曼偷偷运到巴格达。美派特工在安曼机场偷梁换柱，将带有病毒的芯片置入打印机内。战争爆发后，美军用指令激活病毒，病毒通过打印机侵入伊防空系统电脑，使整个系统瘫痪。这是世界上首次将计算机病毒用于实战，并且取得极佳的作战效果的案例。

2.实体打击。美军将运用空袭和地面部队渗透破坏等方式攻击敌信息系统破坏敌指挥控制能力，瘫痪敌方

域、网络空间的优势。从美军近来在网络进攻与防护多方面的动作可以看出，美军对未来信息化战争的“网络空间主导权”志在必得。正如美国空军网络空间任务负责人兰里卡斯所说“如果不能在网络空间占据主导地位，就不能在空中和太空占据主导地位。”美军建立JFCCNW这样一支特种部队，就是为了顺应信息化战争的需要。据美国《华盛顿邮报》披露，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，也有美国网络安全专家指出，美国虽号称在信息战方面实力过人，但要在技术上完全拦截黑客的攻击，几乎不可能，谁也不能保证自己的网络系统不存在任何安全漏洞，正所谓“道高一尺，魔高一丈”。据美国军方官员透露，当前，美军在保障网络安全方面每年至少要阻止7.5万次的网络攻击，而美国安全机构最后能成功抓获的黑客只是极少数。美国网络安全专家表示，那些真正称得上高手的黑客很难被追踪到，能够被送进监狱的更是少之又少，而追踪网上罪犯却要耗费大量的时间和精力。而且，美军已经组建的大型军事网络就多达二十余种，涉及面宽，覆盖范围广，这些网络系统在发挥着巨大威力的同时，也存在着致命的弱点，一旦这些网络遭到破坏，再强大的火力杀伤武器也难以发挥作用，整个军事系统将处于全面瘫痪的状态。因此美国有不少军事专家担心，对付黑客尚且如此费力，如果是敌对国发起有组织的大规模网上袭击，五角大楼将如何处置？并且，在网络信息战中，强弱判断不像常规战争中那样明显。处于弱势的一方一次得手，进入到对手的“神经中枢”，就可能在顷刻间扭转战争局势。因此，如果美军贸然发动“黑客战”，很可能引火烧身，导致自己的网络体系也同时遭到来自敌人的毁灭性袭击。正如第8航空队司令罗伯特·埃尔德空军中将说的那样，“美军在网络战领域遭到攻击的风险，正如我们允许本·拉登驾驶战机飞越美国领空一样让人无法安心。”

① 现在互联网已经渗透到美军的各个角落，如何维护信息安全已经成为美军的一道难题。② 一位美国空军的技术人员正在用计算机检查基地设备的运行情况。③ 在作战平台逐渐进入无人化、信息化的时代，保障网络安全变得更为迫切。在未来的战争中，网络战一旦失败，各种无人作战平台，乃至整个国防系统的的控制权便很可能落入敌军的手中，出现上世纪80年代的好莱坞大片《战争游戏》中的情景。

情报、指挥网络系统，使敌指挥官无法了解战场情况，最终夺取“制信息权”，或通过实体打击寻找网络接入的突破口，给“黑客”部队创造侵袭条件；

3.心理打击。美军将借助美国在传媒界既有的超强影响，辅以计算机、虚拟成像等多媒体技术对敌国官兵施加心理攻击，利用“虚拟现实”技术创造的逼真作战环境与敌方进行模拟演习式的作战行动，扰乱军心，摧毁敌人的战斗意志，使其陷于真假难辨的消息和令人绝望的纷乱气氛之中，大大丧失抵抗意志，从而达到“不战而屈人之兵”之目的。

◎ 软肋突出

未来信息化条件下陆、海、空、太空、网络空间五维战场中，制太空权、制空权、制海权、制陆权，已从依靠对空天兵器、作战飞机、坦克等“硬武器”系统优势，逐步转为依靠电磁领