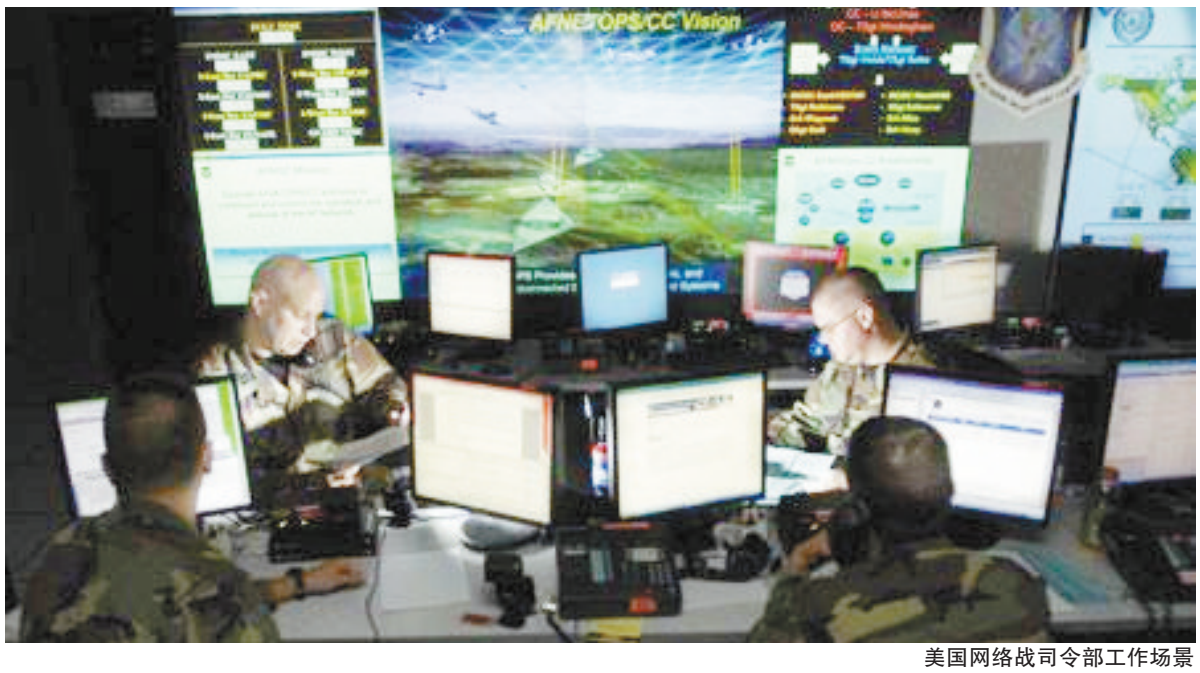
中国网军“网开一面”露真容

国防部新闻事务局局长耿雁生大校5月25日透露：中国解放军建立了一支“网络蓝军”。此消息一出立即吸引了广大军迷的视线，也迅速引起西方媒体的关注。有外媒报道，中国称培养“网军”是自卫，但中国黑客被看做是全球最大的网络攻击力量。对此，我国防部回应称，“网络蓝军”由部队已有人员构成，是常规部队的训练科目之一。那么，何谓“网络蓝军”？我国为何要建立这样一支队伍？其他国家的“网军”规模究竟有多大？ 据《北京晚报》



美国网络战司令部工作场景

名词解读 何谓“蓝军”？

军事评论员宋忠平解释说：“蓝军”是国际军事管理的一个术语，也就是我们常说的“红蓝军对抗”，其中“蓝军”主要扮演对手，如美军的“红旗演习”，通过“蓝军”逼真模拟对手的军事实力和战术战法，达到真实训练部队的目的。一般而言，国内部队都会到“蓝军”轮训，以达到全员训练的主要目标。为了打造完全强势的“蓝军”，很多国家不惜重金装备或采购先进武器武装“蓝军”，将其按照对手的真实实力武装，因而“蓝军”一般而言都是比较强的军事对手。

而“网络蓝军”顾名思义就是打造基于西方网络实力的“网络军队”，以此来训练中国的“网络红军”。既然我们已经组建了“网络蓝军”，这本身说明“网络红军”已存在。

零点接触 中国“蓝军”并非黑客

中国军方组建“网军”的消息传出后，迅速引起西方媒体的关注。英国《泰晤士报》报道，中国自称培养“网军”是自卫，但中国黑客被看做是全球最大的网络攻击力量。我国防部回应称，“网络蓝军”由部队已有人员构成，而他们既不是专门招聘的专业人员，也没有被专门编制，是常规部队的训练科目之一。

今年4月下旬，广州军区组织了一场网上异地同步演练，“网上蓝军”四面出击，一改过去“一对一”对抗模式，在“以一对多”的无形战场上，从容使用网络新战法，使网上对抗更加精彩激烈。“网上蓝军”发挥专业优势，同时向4支“红军”发起凌厉进攻，时而实施“病毒攻击”，时而发布大量“垃圾文电”，时而渗透进入“红军”内部网络，窃取兵力部署和行军路线图等信息，逼着“红军”指挥员不断出新招。这种“网络红蓝对抗”，其实就是实战中“红蓝对抗”演练的延伸。

据悉，为提升网上训练效益，广州军区投入数千万元，联通军区、军级单位、作战师旅团和训练基地之间的网络，建成全军首个军区级训练专网，并从军区范围内挑选30多名网络人才，建成首支专业化“网上蓝军”。

某基地李副司令员介绍说：“如今实行网上对抗，从方案设置到设备调试，不到10天就能完成。‘网上蓝军’的诞生，节约了训练成本80%以上，提高了训练效益。”

军迷发言 中国“网军”两大困难

中国网军相比美国网军，面临着两大困难。其一，有数据显示，我国集成电路芯片的自给率不足10%。要做到网络安全，首先就是硬件安全，而芯片安全是硬件安全核心内容之一。其二，微软的各版本操作系统在中国市场的占有率达到98%。软件安全是网络安全的另一个核心内容，最基本的操作系统不是自己编写的，同样留有安全隐患。

这两个问题，我国已经意识到了。我国进口的所有芯片都经过显微分析，目的就是为了在无法进口时予以仿制。作为军用芯片，这一步骤更是必不可少。至于操作系统软件经过如何的分析，我并不知晓，不过我相信我们的软件专家一定仔细分析过来自境外操作系统的汇编码。

尽管如此，军迷们仍担心百密一疏，如果对手就是要刻意安插进特殊用途的东西，必然是经过伪装，我们很难逐一检验。打网络战，核心软件、核心硬件都掌握在对手那边，我们的网军自然就会面临着很大困难。因此，我国防部发言人称“中国的网络安全防护还比较薄弱”，这的确不是自谦而是现实。

延伸阅读 没有硝烟的战场

美国网络战司令部：借口境外黑客威胁 早将网络用到实战

在美国媒体的报道中，“中国黑客”向来无所不能，往往能轻而易举地突破白宫和五角大楼网络的防护系统，“窃取”机密情报。在美国国防部长盖茨于2009年6月23日宣布建立网络战司令部后，外界似乎立刻明白了美国频频炒作“中国黑客威胁”的真实意图。

渲染“中国黑客”威胁，只不过是美国强化网络战力系列图谋中的一环。事实上美国构建网络攻击力量的历史远远超过外界的想象，甚至在“中国黑客”这个词语出现之前，美国就将网络战运用到实战中了。1991年海湾战争中，美国通过情报系统，在伊拉克从法国购买的防空系统中植入电脑病毒，在美军空袭前用遥控手段激活这些病毒，导致美空军飞临巴格达上空时，伊拉克防空系统已经瘫痪。

作为互联网的诞生地，美国有着“先天优势”。在1999年的科索沃战争以及2003年的伊拉克战争中，人们可以更加清晰地看到网络战的影子。根据美国防务专家乔尔的评估，目前美军共有3000至5000名信息战专家，5万至7万名士兵涉足网络战。如果加上原有的电子战人员，美军的网战部队人数应该在9万人左右。

尤其值得注意的是，在奥巴马政府大幅削减导弹防御系统、F-22战机采购费用的同时，却加大了对网络安全的投入，加速推进网络战部队建设。英国《卫报》分析称，美国这么做就是为了整合分散在全国各地的高科技军事单位，以便在必要时对敌对国家发动网络战争。

在军事专家看来，美国打造“网军”还有着更为深远的意义，那就是将人类战争形态带入新的历史阶段。一位军事专家表示，美国建立网络战司令部，意味着网络战以后很可能作为一种国家战争新方式走入人类历史。今后美国如再遭受网络袭击，美国可以宣布其为战争行为，进行还击。

韩军网络部队：从民间招募黑客 主要应对朝鲜

韩国防部近日决定将现有网络司令部提升为独立部队，以便在应对来自黑客攻击的同时，进行攻击性网络战。

此外，韩国防部还计划将目前500多名的网络司令部人员增加一倍，并加强其功能。另有韩媒体指出，韩军方还计划在未来3年内将网络司令部的兵力再翻一到两番，而长远计划更是要打造成一支兵力数万的网络战部队。

对于此次网战司令部的大幅扩军，韩国军方表示是为了应对来自朝鲜黑客的攻击。韩军方消息人士称，朝鲜军方正在大规模培养专业黑客，提升网络战能力。韩国《每日经济》网站援引军方消息人士的话说，韩国军方要努力达到美国网络部队作战的水平。

韩军网络司令部是在2010年1月创建的。自成立以来，韩军网络司令部从民间招募了一大批拥有很强实战经验的黑客。除了培养和招募网军，韩军网络司令部还在韩美“关键决心”联合军演和“乙支自由卫士”演习期间，进行网络攻防演习。对于网络司令部的升级，韩国《中央日报》曾发表文章认为，目前网络战争被认为是最具杀伤力的战争形式，因为网络战争能够盗取整个军队的作战计划。

伊朗网络警察：启动“网络巡逻” 迎击美国网络战

伊朗新成立的网络警察部门今年1月份已开始正式运转，该部门的职责是阻止有人利用互联网从事针对伊朗的间谍及破坏活动。

伊朗高级警官卡迈勒·哈迪安法尔说，信息工具在政治、安全、经贸以及宗教领域的相互对抗方面有着不容否认的作用，“网络警察可以阻止信息领域的间谍及破坏活动”。首批互联网警察本月在首都德黑兰展开“网络巡逻”。到2012年初，伊朗全国所有警察局将配设网络警察。

日本网络空间防卫队：防备黑客攻击 保护机密信息

日本防卫省决定，在2011年度建立起一支专门的“网络空间防卫队”，以防备黑客攻击，加强保护机密信息的能力。

“网络空间防卫队”初期人数约60人。这支“网络部队”负责收集和分析研究最新的病毒信息，并进行反黑客攻击训练。防卫省2010年度预算中已包含总额约70亿日元(约合7525万美元)的“应对网络攻击”项目。

本报地址：合肥市永红路10号 邮政编码：230063 新闻热线：2620110 2639564 广告垂询电话：2815807 订报热线：7136993 发行部：2813115 总编办：2636366 采编中心：2623752 新闻传真：2615582
信息传真：2615007 Email：ahscb@mail.hf.ah.cn 零售价每份：0.50元 今日合肥、蚌埠、铜陵、宿州、阜阳同时开印 全年订价：180元 月价：15元 安徽新华印刷股份有限公司承印