2003年3月20日北京时间10点半左右，以美英发动第一轮空袭为标志，伊拉克战争正式打响。

其实，在网络世界里，烽火硝烟早在一个月前就已燃起。美军在2月底就发动了对伊拉克的第一轮网络攻击。短短几天内，数千名伊拉克人在他们的电子信箱里发现了一封发信人被掩盖的邮件。“放弃吧，起义并倒戈。到另一方来，否则美国就开战了。”同时在美国联邦调查局公布的一份评估报告中披露，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，可能是亲伊拉克的黑客所为。

从20世纪80年代以后的几场局部战争，特别是90年代的海湾战争、美英对伊拉克实施的“沙漠之狐”空袭以及科索沃战争，信息化的网络战在战争中都起到了极大作用。在去年阿富汗的反恐战争结束后，“基地”恐怖组织开始在互联网上寻找他们新的“基地”，并且互联网也成为他们新的恐怖袭击目标。

所有这些都在向我们证明：网络战争已经走上了历史的舞台。网络战争是近年来伴随着信息技术的发展而出现的一个新名词。它是指以计算机网络为主要目标，以先进的信息技术为基本手段，在整个网络空间所进行的各类攻防作战的总称。目的是获取和保持信息网络优势，掌握并确保网络空间的“制信息权”。

总体而言，网络战争分为两条战线：基于因特网的战略网络战和基于战场网络的战场网络战。战略网络战的攻击目标主要是国家的要害部分，如通信网络、金融系统、交通枢纽、国家的政府网站和商业网络。其目的是使对方国家的政治经济陷入混乱，甚至瘫痪崩溃。采取的攻击方式有几个：利用逻辑炸弹、病毒程序等摧毁由电脑网络控制的政治经济系统；利用垄断的硬件、软件技术，偷窃军事、经济、行政机密，切断因特网的人口、中断与其它国家的联系，造成网络瘫痪。战场网络战则是网络战中的另一条重要战线。攻击目标着重是敌方的军事指挥、控制、通讯和计算机系统，主要攻击战术局域网。采用的攻击方式有下面几个：采用网络侦察设备截获信息，利用强烈的干扰信号压制战场网络的无线信道；给战场网络系统预埋病毒，在战争中触发病毒；采取火力打击、兵力袭击等传统手段。

作为目前新军事革命的重要组成部分，网络战争以其独特的特点，吸引了各国军事领域的注意。下面简要的分析一下网络战争的六个特点。

1、网络战争破坏性极大：网络攻击的威力不亚于核袭击，因为一旦受到网络攻击，一切活动都将陷于瘫痪，如电力供应中断，通讯失效，股票交易停顿，交通系统瘫痪等。

2、网络战具有广泛性，未来的网络作战并非单靠职业军人利用计算机对敌军事信息系统进行攻击，网络高手甚至普通人员都可以通过键盘、鼠标和调制解调器等，入侵网络所能达到的任何范围。

3、网络可将各种作战力量高度聚合。现代军用网络系统，可把遍布于战场每个角落的侦察系统、火力系统、指挥系统、支援保障系统等诸多作战单元，整合成“一体化”的战争网络。

4、网络战表现出较强的不规则对抗：作战系统网络由若干分散的作战单元相互联接而成，其功能的发挥离不开节点的中继和转换。这些面广量多的节点，自身防护薄弱，易被对方楔入或实施“一点瘫痪”，进而影响整个作战系统功能的发挥。因此，围绕网络节点的打击、破坏与渗透，将成为作战双方斗争的焦点。

5、网络战具有明显的脆弱性：保持网络的完整性和纯洁性极为困难，因此未来作战必将围绕网络的破坏与反破坏展开搏杀。

6、网络战具有“隐蔽”性。网络战一般是利用各种手段，骗过敌方网络的防火墙或找到网络漏洞，隐蔽进入敌方网络，然后实施攻击。或者在和平时期卖给对方留有秘密“后门”或设立“芯片陷阱”的计算机，为战时使用。

正是因为网络战的以上特点，以及人类对网络技术依赖性的逐渐增强，预计网络战争在未来战争中将会扮演着越来越重要的角色。

在许多人看来，网络战是很遥远的事，其实从2001年5月爆发的中美黑客大战，到目前大陆和台湾在网络战争技术上的竞争，这些事件都在向

键盘：象人一样，没有压力就没有工作的动力，同时，哪里有压迫，哪里就有反抗。

未来的网络战

□徐 勉

我们证明，网络战争就在我们身边。未来发生在我们身边的战争，最大可能是首先以网络战争方式向敌方的经济、政治和军事网络的“神经中枢”——计算机网络发动进攻。

凡事预则立，不预则废。落后就要挨打的历史教训恍如昨日。我们必须冷静地审视目前网络战争带给我们的挑战，从现在做起。笔者认为，从保卫国家和平的大计出发，为了在未来的网络战争中占领战略制高点，我们需要从如下几个方面作出努力。

一是建立国家网络安全防御体系，完善网络安全应对系统。国家网络安全防御体系的建立关系到国家安危，因此国家需要对这一体系的建立、管理和运行进行统一的组织，系统的设计，并最终有机组成一个坚固的系统。目前我国在这一个方面还比较薄弱，主要原因是技术力量欠缺、资金紧张和网络安全人才匮乏等。

二是培养大批网络安全领域的高素质专业人才。据介绍：“我国现有信息安全专业人才仅3000人左右”，显然，这样的人数与我国的迅速发展是不相适应的。除了军队、公安部门等对高级网络安全人才的需要外，政府、企业也需要信息安全方面的人才；中国互联网本身的漏洞，也急需网络安全人才来解决。同时我国需要建立一套科学的培养模式，保证系统培养出大批的网络安全人才。

三是增强安全意识，加强安全培训。目前国内企业对于网络安全的了解与熟知程度令人担忧，包括政府、银行、证券及ISP/ICP等在内的诸多企业的安全意识普遍薄弱，据有关调查显示，国内90%以上的电子商务站点都有着严重的安全漏洞，大多数企业内部网络（尤其是企业局域网）存在着不同程度的安全隐患。因此，在全国范围内加强政府、企业和军事部门的网络安全意识教育是非常重要的。主要的手段是网络安全的培训。安全培训的内容应该包括：安全常识介绍，密码使用规范，病毒防护介绍，安全使用电子邮件，Intranet网络合理使用规范，常见安全陷阱防护措施，网络受到攻击后的防护技术等。

四是成立国家信息网络安全机构。在和平时期该机构的职责是具体规划国家的计算机网络建设工作；统筹协调全国的信息安全工作；评测审计我国的基础信息网络系统，监督我国的基础设施网络系统。在战争情况下，主要职责是严防在战争条件下基础网络设施的瘫痪和被损坏。笔者认为，在目前情况下，国家信息网络安全机构的主要任务是审计评测现阶段我国基础网络系统的安全性，制定和实施网络安全的具体防护措施，以尽快提升我国基础网络系统的安全级别。

五是建立我们自己的民族信息产业体系，这是最为核心和基础的。国家安全和信息系统安全必须立足于民族产业的支撑和技术保障。试想一下，如果网络大厦建立在敌方的硬件地基和软件平台之上，那么一旦网络对抗发生，平时友好温柔的芯片和操作系统也许就成了“潘多拉的盒子”，谁也无法想象将会发生什么事情，会有什么样的结局。因此我们必须自力更生发展我国信息产业，发展和壮大中国的信息安全体系建设。研究我国的计算机安全防御体系，开发具有自主知识产权的计算机安全产品和技术。最安全的作法是尽可能地建设有我们自主知识产权的信息网络，并对事关国家政治、经济、军事安全的重要骨干信息网络，由国家统一规划，统一建设，形成一定范围的局域网，以提高网络的安全性。

最后，是要大力发展我们自己的网络战技术。仅仅拥有“盾”——建立网络安全防御体系，并不足以保护国家的主权和网络安全，在战争中进攻才是最好的防守，只有拥有了进攻的手段才能在战争中掌握主动权。因此我们需要充分运用网络安全技术，建立起自己的“矛”——网络战进攻武器和实施网络战争的部队，最终建立一个攻防兼备的网络战战略。网络战进攻部队在发生战争的时候，一方面通过网络向敌方发动攻击，另一方面担负起保护己方网络安全的责任。同时由于网络战争具有不规则对抗和不对称的特点，我国完全可以利用这一特征，在网络战争中发展出自己的不对称作战技术手段，做到拥有“撒手锏”，使敌人望而生畏，不敢轻举妄动，从而为国家的发展创造有利的和平环境。

磁盘：树木的年轮记录着岁月流逝的苍茫，智慧的年轮记载着人类成长的脚步