# 网络战正向现实扑来（下）

奕 兵
（广州 30 卫士信息安全有限公司，广东 广州 510630）

**摘 要**：描述网络战争的威胁迫在眉睫，提醒人们早做准备，有备无患。

**关键词**：网络战争；网络武器；黑客；信息安全

**Abstract**：Extremely urgent threat of the cyberwar is described. Be constantly alert and vigilant, and go to prepare as early as possible. Where there is precaution, there is no danger.

**Key words**：Cyberwar；Netweapon；Hacker；Infosec

（接上期）

## 5 各国网络备战忙

美国著名军事预测学家詹姆斯·亚当斯在其所著的《下一场世界战争》中预言：在未来的战争中，计算机本身就是武器，前线无处不在，夺取作战空间控制权的不是炮弹和子弹，而是计算机网络里流动的“比特”和字节。未来派学者斯蒂芬·斯蒂尔指出：“多层次协调一致的网络袭击将能够同时进行大（国家安全系统）、中（当地电网）、小（汽车发动）规模的破坏。”

当前，各个军事大国都正在从网战的理论、网战部队编成一直到网战武器，在网战的法律根据、网战的条令、网战的方式／方法／手段、网军的编队、网战的武器／兵器、网战的指挥控制、网战与其他领域作战的衔接与转化艺术等方面，积极做着战前准备。

### 5.1 美军

美国国防部早在 2005 年 3 月公布的《国防战略报告》中就已明确将网络空间、陆、海、空和太空定义为同等重要的、需要美国维持决定性优势的五大空间。就战略威慑而言，要想维护五大空间的决定性优势，则必须对凡是威胁国家安全的战略方向，都实施程度不一的威慑，而且必须是全方位的、着眼未来的，从而对潜在的侵犯者形成有效的威慑。

美军惯于将其信息系统设想成时刻处于被攻击之中，实际上他们早就在准备网络战了。2003 年 2 月 7 日《华盛顿邮报》就透露，当时的总统小布什已于 2002 年 7 月签署了“第 16 号国家安全总统令”，责成国防部牵头，组织中央情报局、联邦调查局、国家安全局等政府部门制定美国国家网络战的战略，以便在必要时，在确保美国军、政、民、商网络安全的前提下，攻击和破坏任何敌方的网络信息系统。据说，美军已开发出能通过计算机破坏敌国军用信息网而不殃及自己和友好国家民用网的多种攻击算法，其原空 8 军的攻击算法能在 8 秒之内攻击世界任何地方。美军于 2003 年建立了军中情报部门共用的威胁数据库；2004 年底完成了无线技术脆弱性数据库的最终版本；2005 年完成了通用的全球网络防御操作图，并向其盟军／友军发布使用准则；他们原计划于 2007 年 1 月完成开发一套旨在保护军网免受软件攻击的原型系统。美国国防部则宣称，将把以突袭破坏敌军计算机网络为主的信息战纳入美军的常规作战战术之中，网络战武器也跟普通炸弹、巡航导弹、攻击型直升机一样，成为美军的“常备武器”。

美军已经把网战的潜在对手分为三类：第一类是普通的独干黑客，多数没有政治目的；第二类是拥有一定实力但还够不上国家级对手的一些实体；第三类是拥有网战资源和实力的国家，包括俄罗斯、中国、英国和欧洲的其他国家（2008 年 7 月 31 日美军发布的《国防战略报告》也声称，恐怖主义、“流氓国家”和“新兴大国”“使美国面临严峻的战略环境”）。

他们早把“网络信息作战状态级”分成五个等级，紧张程度从低到高分别叫 Normal、Alpha、Bravo、Charlie 和 Delta。

美军从国防部到各个军种、兵种原都有各自的信息战部队，只不过它们的管理关系以前还完全没有理顺。2009 年 6 月 23 日奥巴马正式批准成立国防部网络司令部，其各军兵种内设的信息战部队在业务上理应归属网络司令部领导，其司令亚历山大的将军军衔由三星升为四星，想来也有“镇住”各军兵种信息战部队一把手（多为三星将军）的用意。国防部副部长威廉姆·林恩说，网络司令部的主要任务是保护美军的 1.5 万个军用网络和 700 多万台电脑。战争期间，美军必须能以“网络速度”对于任何入侵或者攻击予以回应。美军国防部长罗伯特·盖茨则表示，网络司令部必须在全球安全背景之下协调网络战行为，另外还向美国民用机构和国外伙伴提供协助，能像完成传统军事行动那样“信心百倍”地展开网络攻防任务。网络司令部由此有望获得超过 50 亿美元的预算。

关于网军规模，有美军官透露，美军新成立的“网络司令部的规模不会很大，职员约有几百人，而不是几千人。”[注 2] 根据长期跟踪美军黑客项目的防务专家乔尔·哈丁的估计，目前美国全军共有 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 88700 人左右。

### 5.2 其他国家

#### (1) 德国

德国《明镜周刊》2009 年 2 月 11 日报道，德国国防部长弗朗茨·约瑟夫·荣格命令德国国防军在未来三年内组建一支网络黑客部队。该任务落在现年 60 岁的陆军准将弗雷德里希·威廉·克里塞尔头上，本是联邦国防军侦察部队负责人的他，将率领叫作“信息和网络技术管理部”的部队，总数 6000 人，总部设在波恩附近的小镇莱茵巴赫。其实在 2009 年年初，他已有 76 名部下在忙于测试最新的网络渗透、网络扫描和网络操纵技术并模拟网络攻击了。目前，该部队主要任务是应对网络突发情况，主要针对有关外部服务器和网络的攻击。该部队也已经在阿富汗执行过网络监控行动，现时是做好执行 2010 年任务的准备。

据报道，德国政府同样对未来世界范围内的网络战做好了准备。

#### (2) 日本

根据其 2005-2009 年《中期防卫力量发展计划》，日本防卫省已经组建了一支由大约 5000 名计算机专家组成的网络战部队，专门从事网络系统的攻防。该部队的主要任务是，进行反黑客、反病毒入侵的攻击，同时研制和开发可破坏其他国家网络系统的跨国性“网络武器”，必要时可对敌方重要网络实施“瘫痪战”。

#### (3) 南韩

中新社 2009 年 7 月 9 日北京报道，韩国国防部官员于当日透露，由于韩国的青瓦台、国会、国家情报院和国防部等国家机关，以及金融界、媒体和防火墙企业等 25 家网站遭受连续四天（7 月 7 日至 7 月 10 日）的猛烈攻击，分布式拒绝服务（DDoS）攻击使得韩国国会、国防部、外交通商部、《朝鲜日报》、国民银行和驻韩美军等机构的网站一度无法打开、打开速度极慢或连续不稳定，使韩国有 7.4 万部个人电脑感染病毒，电脑硬盘随后被黑，所存数据全部丢失等情况，因此原计划定于 2012 年组建的“信息安全司令部”提前于 2010 年元旦成立，以维护韩国的国家网络安全[注 3]。国防部负责该项目的官员金宰民（音译，Kim Jae-min）称，信息安全司令部将制定可操作的防卫计划，预计 2010 年 7 月就能全面运作，发挥完全作用。

“这（网络司令部）是一支独立部队，由 200 名专业技术人员构成，一名少将统管。”一个没有公开姓名的国防部官员告诉韩国联合通讯社。依照韩联社说法，韩国独立网络司令部不仅承担韩国的网络安全维护与防护任务，还具备国际互联网攻击能力，可扰乱别国重要机构的网络运行。

#### (4) 北朝鲜

据报道，北朝鲜军队于 1998 年组建了一支专门从事网络战的新队伍，代号为 121 部队。据说该部队在规模和能力方面的巨大努力，就算在发展网络战的前 10 个国家当中也是很突出的。有人对该 121 部队评估如下：

1) 规模与战略目标评估

部队规模：起初 1000 人，目前估计有 17000 人。

预算：北朝鲜网络战部队预算为 700 多万美元（北朝鲜全部军费总预算为 60 亿美元，位列世界第 25 位）。

经历：黑进了韩国网站并造成重大破坏，黑进了美国国防部系统。

威胁等级：北朝鲜 2007 年制定的间谍战（Spy-Ops）网络能力威胁矩阵被列为世界第 8 位。

战略：将网络战部队纳入整体的战斗战略，使之成为联合军事行动的一部分。另外他们希望利用网络战武器作为非战争时期有限地扩大实力和影响的方法。

目标：控制敌人的信息基础设施，制造社会动荡和金融损失。

目的：通过非对称战和网络战增强军队的能力。

2) 能力评估

网络情报／间谍：正向网络情报发展。

攻击性网络武器：具有较先进的一般分布式拒绝服务攻击能力，一般性的病毒和恶意代码工具；拥有建造和部署网络武器和蓄电池 EMP（电磁脉冲）装置的技术能力[注 4]，能在有限的范围内摧毁电子设备和计算机。

根据韩国国家情报院的情报，北朝鲜的 121 部队隶属于朝鲜军队总参谋部侦探局，目前的 100 多名黑客全部毕业于平壤自动化大学，位于平壤的“110 号实验室”是伪装成开发电脑软件公司的黑客部队。韩联社说，韩国国家情报院已经确认朝鲜军队扩编了网络战专业人才，命名为“技术侦探组”。2009 年 7 月 13 日，韩国《中央日报》甚至言之凿凿地说，中国丹东的星海酒店四层就是朝鲜网络战的一个据点，说是从 2004 年开始朝鲜就在这里建立了 115 平米的安全室，里面有十几台电脑 24 小时都在联网。而就在当天，中国《环球时报》记者在星海酒店并没有发现有一个“十几台电脑同时开机的、115 平米的办公室”。

2007 年，韩国联合参谋本部召开了朝鲜心理战非公开研讨会，确认朝鲜“人民军总参谋部侦察局下属 121 所黑客部队（300 人）和敌工局下属 204 所网络心理战部队（100 人）正在运作中。”此次 7 月的黑客攻击后，韩国情报部门猜测 110 实验室很可能就是 121 所和 204 所的另一个代名词，原因是朝鲜黑客组织经常变换名称。2008 年，韩国国会情报委员会称，朝鲜军方的黑客曾在 2006 年试图攻击美韩两国国防部，朝鲜的电脑黑客能力已达到美国中央情报局的水准，而且朝鲜的黑客部队已具备对美、韩、日发动网络战的能力云云。

## 6 关于网战武器

业内人士说，美国网络战武器库的完全程度已经成为密级最高的美国国家机密，防范程度比核武器还严。

从美国 Intelomics 等三个智库不久前联合公布的《网络武器威胁矩阵报告》可以看出，网战的攻击手段还真不少。阅读之余，笔者感到他们所列出的还不能通通都算

作“武器”，大多只能称为“技术”，而要将“技术”变为“武器”，还需走很长的路呢。例如利用网络的软件漏洞来攻击对方应算是技术而不能称作武器；产生高能量的电磁脉冲也是一种技术，仅当其变成电磁脉冲炸弹后，这炸弹就是武器了。由此，笔者把他们所说的网战武器改称为网战攻击手段。他们认为目前世界上有 18 种常见的网战攻击手段（见表 1），且一一赋予这些攻击手段不同的威胁指数值。其中，属于高风险的有 9 种，其威胁指数在 3.5 以上；中等风险的有 3 种，威胁指数在 3.2 至 3.4 之间；低风险的有 6 种，威胁指数在 3.0 以下。

表 1 18 种常见的网战攻击手段

| 序号 | 网战攻击手段 | 攻击手段描述 | 威胁指数 | 备注 |
|---|---|---|---|---|
| 1 | 软件漏洞 | 攻击对方软件的内在漏洞，是目前最常见也最危险的网络攻击手段。 | 3.9 | |
| 2 | 内部植入威胁 | 比较原始但威胁很大的手段，潜入对方基地的渗透人员，向物理隔离的对方网络注入恶意病毒或者代码。 | 3.7 | 据称，以色列为袭击伊朗核设施，计划派特工潜入伊朗，通过 U 盘向核设施网络植入病毒。 |
| 3 | 逻辑炸弹 | 在某种特定条件下触发恶意代码，破坏计算机存储数据或者妨碍计算机正常运行。 | 3.7 | |
| 4 | 特洛伊木马 | 通过网络植入，远程操纵计算机，偷窃计算机中的文件和数据。 | 3.7 | |
| 5 | 伪造硬件 | 通过伪造的硬件来发动攻击。 | 3.6 | 目前已不常用。 |
| 6 | 盗版软件 | 通过盗版软件发动攻击 | 3.6 | 目前已不常用。 |
| 7 | 隧道攻击 | 通过获取底层系统功能而在安全系统的更低层发动攻击，比如利用计算机防火墙本身的缺陷侵入系统。 | 3.5 | |
| 8 | 后门程序 | 在编制程序时事先留下可以自由进入系统的通道。 | 3.5 | |
| 9 | 连续扫描 | 在受感染计算机中植入蠕虫病毒，逐一扫描 IP 地址，确定主机是否在活动、主机正在使用哪些端口、提供哪些服务，以便制定相应的攻击方案。 | 3.5 | |
| 10 | 字典式扫描 | 利用目标客户端的缓冲溢出弱点，取得计算机的控制权。 | 3.4 | |
| 11 | 数字扫描 | 跟踪和刺探网络用户的行踪，以获取密码或者其它数据。 | 3.3 | 主要用于对无线局域网的攻击。 |
| 12 | 数据回收 | 搜集废弃的存储介质，还原大量未受保护的数据，获取相应系统的漏洞线索。 | 3.2 | 此手段肯定对信息安全有威胁，但威胁指数竟比僵尸网络、电磁脉冲炸弹等还高，让人费解。 |
| 13 | 僵尸网络 | 采用各种传播手段，用僵尸程序感染大量网络主机，从而控制网络用户群使之成为僵尸网络。众多的计算机在不知不觉中如同僵尸群一样被人驱赶和指挥，为虎作伥，成为被人利用的工具。 | 3.0 | |
| 14 | 电磁脉冲武器 | 通过将炸药的化学能转化为强大的电磁能并对外辐射，烧毁计算机或服务器的芯片，从而对网络实现物理上的破坏。 | 3.0 | 电磁脉冲炸弹和高功率微波炸弹同属于高能脉冲炸弹，见下图。可能因近来少用，故威胁指数仅被赋予 3.0。 |
| 15 | 细菌病毒 | 感染计算机操作系统，通过不断地自我复制使计算机中央处理器瘫痪。 | 3.0 | |
| 16 | 欺骗式攻击 | 指一个人或者程序通过伪造数据，成功地伪装成另外一个人或者程序，达到欺骗对方的目的。 | 3.0 | 美军在 1995 年举行了“网络勇士”演习，一名空军中尉用一台普通的电脑和调制解调器，不到几分钟就接管了美国海军大西洋舰队的指挥权，其中最关键的技术就是伪造数据，欺骗美军指挥系统。 |
| 17 | 分布式拒绝服务 | 简称 DDoS，短时间里洪水般向受害主机发送看似合法的服务请求，从而造成网络阻塞或服务器资源耗尽，最终导致拒绝服务。 | 2.9 | 这是目前应用最广的网络攻击手段。 |
| 18 | 野兔病毒 | 通过不断自我复制而耗尽目标计算机的有限资源。不会感染其他系统。 | 2.8 | 就现时技术而言，病毒恪守规矩不传染，奇怪；既然不会感染目标计算机之外的其他系统，咋能成为网战中病毒武器？ |

其实，在上表的 18 种网战攻击手段中，它们的威胁指数应当只是参考值，而且不应该是不变的。风险的高中低也应该不是固定的，它们会随环境和条件的不同而转化。

还应当明白，除了表中所列的这些攻击手段，还有不少已知与未知的网战手段、工具和武器。

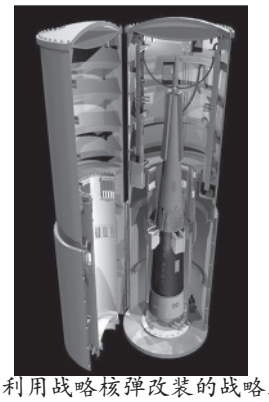

图 1 美国利用战略核弹改装的战略级电磁脉冲弹

核武器就是最早的电磁脉冲武器 EMP。电磁脉冲炸弹会瞬间产生非常强猛的电磁脉冲波，若它于 40 公里的高空爆炸，则可破坏 700 公里半径区域内暴露的通讯线路和电子设备，其破坏力仅次于核弹。有专家甚至说，电磁脉冲弹对高度现代化的城市破坏力尤甚，足以让整座城市倒退一个世纪。

## 7 后语

据《华尔街日报》2009 年 10 月 22 日报道，“美中经济安全审查委员会”日前正式发布题为《中国实施网络战和计算机网络应用能力》的评估报告，宣称中国正利用不断发展的信息技术能力，对美国展开“长期的、尖端的计算机攻击行动”，并搜集美国的情报。另有媒体称，为对付黑客，美国国防部每年要付出 300 多亿美元的代价，说是比当年制造原子弹的曼哈顿工程花费的还要多。这当然有夸大之嫌，也是找来的借口。

实际上，出于独霸的逻辑思维，世界上实力接近美国的任何国家都可能成为美国的敌人；所有存在霸权野心的国家都必会视中国为对手。中国只有在军事高技术上赶上美国，能够独立制造跟美国同样先进的武器，使美国无法打压、排斥中国时，中国才能获得战略主动权；美国之所以还能遏制中国，就是因为中国军事力量目前还不够强大。更有甚者，正如美国密歇根大学东亚问题专家 Josef Gregory Mahoney 教授所说，“9•11”之后美国出兵阿富汗、进驻中亚，在塔吉克斯坦和吉尔吉斯斯坦建立了军事基地；2003 年美国又出兵伊拉克并在那里驻军；美国在东南亚还有驻新加坡的军事基地，在日本和韩国也有驻军；此外，美国在台湾有大量军事“资产”，并持续向台湾出售战机和其他武器；美国还有太平洋舰队，美军的 F-16 战机遍布中亚，可以随时封锁波斯湾，美国已经

有效地将中国包围起来了。从军事上估计，美国只用常规武器就能够在 15 分钟之内袭击中国境内的任何目标（见美国 PoliticalAffairs2009 年 12 月 23 日报道）。美国视俄罗斯和中国为其最大的战略竞争对手，因而不断加紧对俄、中实施战略包围和战略遏制，其中最为阴险的战略牵制是东西对进——北约东扩和美日西进，目的就在于控制亚欧大陆。

这还不算，长久以来，美军一直在研制、试验“网络武器”，希望能用电脑代替炸弹，对敌发动远程袭击。那样，美军轻松敲打键盘，就能获得“斩首”效果——让敌国的首脑和军民丧失斗志，或置乱军队指挥和社会秩序。

目前国际形势总体上虽算稳定，但全球性挑战、新安全威胁因素日益增多，大大增加了形势变化的复杂性、关联性和不确定性。

奥巴马是靠网络媒体支持上台的总统。他在竞选期间就多次强调网络安全对于美国的重要性，就职后不久即要求对美国的网络安全状况展开为期 60 天的全面评估。2009 年 5 月 29 日，在他批准公布的国家网络安全评估报告中，提到来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁之一。美国国土安全部长纳波利塔诺 10 月 30 日就宣布，负责政府网络安全的机构“国家网络安全和通信综合中心”正式成立。

美国不仅在 IT 领域、信息技术方面占尽先机，在备战网络战方面也抢先起跑了十余年。自 20 世纪 90 年代以来，美军就频繁到“黑客”市场“招兵买马”了，例如在美国拉斯韦加斯最大的计算机展览上，美国前助理国防部长莫尼就曾在演讲中讨好“黑客”们：“如果你们考虑过余生要干些什么，请务必不要忘记国防部。”美军官员还经常在互联网上的“网络家园”游荡，目的是寻找天才“黑客”加入美军的行列。五角大楼曾经公开表示，在 2011 年前，要把军内熟悉互联网反黑客业务的专家数量从 80 名增加到 250 人。

国内外多数信息安全专家认为，对一个国家发动重大的网络攻击只是时间问题。

我们还有自知之明，发达国家通过对发展中国家所用的计算机芯片和关键软件技术的先天垄断，就实际控制了这些国家政治、经济、军事等要害部门的神经中枢，使这些国家的主权部分丧失。解放军报说，我国集成电路的 80%、软件的 60% 左右需要依靠进口解决，在安全方面存在许多漏洞和隐患。我们深知，网络攻击能否成功，关键就在于能否准确探知并巧妙利用对方网络漏洞这类信息“火力”的突破口；而网络防御能力强弱的关键，则在于能否及时发现并严密修补自己网络的安全漏洞。

有道是：生于忧患，死于安乐；又曰：凡事预则立，有备而无患。在应对可能的网络攻击中，应详尽估计到对网络的物理攻击（硬伤毁等）、电子攻击（断电、干扰、假冒、施毒等）以及信息攻击（侦收、破译、窃听、重放、删改、插入及信息流分析等）。我国和我军均需建立确实有效的四种体系——信息安全保障体系、信息安全管理体系、信息安全应急响应体系和信息安全威慑体系，以确保我国我军的信息网络能健康有序地为我国的和平建设服务。

献身于广州地区（含广州市政府）信息安全事业的广州 30 卫士信息安全有限公司全体员工，乐于和全国同仁一道，为确保祖国的网络安全而努力奋斗。（全文完）

**参考文献**：

[1] 徐周文 . 浅说信息时代的战略威慑 . 解放军报 ,2009-05-07 第 10 版 .
[2] 美国网络外交解读：扩宽外交理念、更具攻势特性 . 新华网 ,2009.07.09.
[3] 美高级官员称中国网络间谍已经深入美国的系统 . 环球时报 ,2009.04.20.
[4] 潘孟华 . 全球主要国家 2008 年国防白皮书概述 . 中国军网，2009.01.21.
[5]2020 预言：未来型战争恐爆发 美国还是那个美国？CCTV.com,2009.02.16.
[6] 戴旭 . 美国网军引发未来战争质变 .http://blog.sina.com.cn,2009.07.02.
[7] 知远 . 专家详解全球重点地区网络攻击与网络部队 .2008.07.11.
[8] 美防长下令成立网络司令部 十月份投入运作 ,2009.07.06.
[9] 林东，刘德瀚 . 美军将争夺网络控制权作为维持霸权重要部分 . 中国青年报，2009.6.13.
[10] 美请专家扮黑客演练网络战 发报告称中国威胁大，中青在线 - 青年参考，2009.10.28.
[11] 美报告披露网络战 18 种手段 .2009.07.13.
[12] 美国国土安全部招聘大量“有正义感的黑客”. 人民网 ,2009.04.19.

[注 2] 有资料称，美军战略司令部司令凯文 · 希尔顿曾公开承认，他们正在征召 2000-4000 名黑客，组建“特种部队”来承担网络防御的任务，还将对他国的电脑网络进行秘密攻击。在战略司令部里，又组建了网络战联合司令部，负责具体指挥美军的“黑客”部队。据悉，这支部队具备摧毁敌人网络、进入敌人计算机窃取或假造数据的作战能力，他们可以释放蠕虫病毒致瘫敌人的指挥和控制系统，使敌人无法指挥地面部队或发射地对空导弹。同时，该部队还能防护美国国防部的所有网络免受攻击（五角大楼发言人布赖恩 · 惠特曼说，美国防部新成立的网络司令部起初会隶属于战略司令部，今年 10 月开始运作，2010 年 10 月全面运作）。

[注 3] 新加坡《联合早报》爆料：就韩国主要网站 7 月上旬遭攻击事件，韩国国家情报院表态“我们接报，上个月初朝鲜军总参谋部侦察局领导的‘110 号实验室’，下达了‘破坏南朝鲜傀儡集团的通讯网’命令的情报。”但越南网络安全公司 Bkis 表示，他已经收集到证据，此次针对韩国网络发起的分布式拒绝服务攻击并非来自朝鲜，而是来自英国。韩国认为持续三天的黑客攻击由朝鲜军方操纵、锁定的 92 个 IP 地址却没有一个来自朝鲜。

[注 4] 早在 2002 年，当时的白宫技术顾问里查德克拉克在美国国会专家小组会上就说北朝鲜、伊拉克和伊朗正在训练 Internet 网战人员。2007 年春，北朝鲜又实施了一次网络武器试验；10 月北朝鲜试验了首个逻辑炸弹。北朝鲜的试验导致了联合国安理会通过决议禁止向东亚国家出售大型计算机和笔记本电脑。