140 部队即美韩等国正在筹建的网络战司令部的简称

世界网络战硝烟四起

文 / 满凯艳 狄 鑫

美国著名未来学家托夫勒在《权力的转移》一书中提到，世界已经离开了依靠暴力与金钱控制的时代，未来世界政治的魔方，将控制在拥有信息强权的人手里，他们会使用手中掌握的网络控制权、信息发布权，达到暴力与金钱无法征服的目的。

走在世界政治经济前沿的中国，自然无法避开这场新战役，且不仅要攘外，更要安内。商战在互联网商业化 20 年之后，进入了轰轰烈烈的战国时代。曾经为人类提供前所未有创业机会的互联网，成为巨大的新战场。

网络战争将带来什么

如果说工业时代的“战略战”是核战争，那么，信息时代的“战略战”就是网络战。

网络战争会是什么样？负责反恐和网络安全的白宫前幕僚理查德·克拉克在他的新书中设想了十五分钟之内造成的灾难性破坏：计算机病毒让军方的邮件系统瘫痪；造成炼油厂和输油管道爆炸；空中交通管制系统瘫痪；货运和城市铁路列车出轨；金融数据被涂改；美东电网断电；轨道卫星运转失控。随着食物紧缺，资金链断裂，整个社会很快分崩离析。最糟糕的是，攻击者的身份一直成谜。

IT 行业的安全专家布鲁斯·施奈尔则表示，在未来战争中，网络空间肯定是战场之一，但除非是在真正的战争环境中，否则要对美国施行毁灭性攻击从技术上来说困难重重，也不符合常理，而如果真正的战争爆发的话，攻击者可能是显而易见的。

对高层领导来说，计算机技术是一柄双刃剑。炸弹可以由 GPS 卫星导航；飞机可以通过远程遥控飞行全世界；当今的战斗机和军舰本身就是巨大的数据处理中心，即使是普通的步兵也在上网。但是不断增加的互联互通和不安全的互联网，让电子攻击的手段不断翻新；对计算机的日益依赖也增加了它们可能造成的损失。

网络武器的神秘面纱

网络武器和核炸弹一样，存在并不代表要使用。而且，攻击者不能确定攻击行为会对另一个国家造成怎样的影响，这就使得他们的攻击部署存在很高风险。对先进的军事力量（如美军）而言，这样的不确定性是网络攻击的一个缺陷，但恐怖分子和流氓国家的军队对此就无所谓了。网络攻击也带来了网上犯罪和间谍活动的危险。

所有这一切构成了危险的不稳定趋势。网络武器正被秘密研发，谁都绝口不谈将在何时，怎样使用它们。没人知道它们真正的力量，所以国家必须为最坏情况作打算。网络的匿名属性也增加了错

误、错认和失算导致军事力量在常规武器或太空武器上升级的风险。网络战发动很快，且偏好先发制人的攻击方式，几乎没有时间留给你冷静应对。即使计算机辅助武器系统和信息化步兵已经吹散了一些战场上的迷雾，网络武器依然给网络空间罩上了一层厚厚的危险的不确定性毯子。

网络武器在大国手中使用起来最为有效。但是它们因为价廉物美，对相对弱势的一方来说更有用，同时它们也很适合恐怖分子使用。幸运的是，类似于基地组织这样的恐怖团体看起来主要是用互联网进行宣传和通讯，可能是缺乏让炼油厂自爆的技术能力，或许他们更喜欢用自杀性炸弹制造血腥场面，而不喜欢电脑破坏这样的匿名行动——至少现在还是如此。

各国正组建网络战机构

奥巴马已经宣布，美国的数字化基础设施属于“国家战略资产”，并任命国家安全局局长基思·亚历山大将军担任新成立的网络司令部的领导。英国也建立起了一整套网络安全政策体系，和总部设在英国国家通讯总部（GCHQ）的“行动中心”，GCHQ相当于美国国家安全局。中国在讨论“如何到21世纪中期打赢信息化战争”。许多国家也在组建各自的网络战机构，包括俄罗斯、以色列和朝鲜。伊朗自称已拥有了全世界第二大的网军。

与传统军队相比，网军有什么不一样？全部由黑客组成吗？虽然中国国防部前不久刚刚公开确认，为提高部队的网络安全防护水平，解放军广州军区组建了专业的“网络蓝军”，但是关于网络部队的详情，并未有确凿详尽的信息。在这一方面，喜欢大张旗鼓吹网络战的美国或许倒可以成为我们的参考。

1995年，美军就有16名“第一代网络战士”。到目前为止，美国已拥有最大的网络战力量，三军都有网络部队。据防务专家乔尔·哈丁评估，美军共有3000-5000名信息战专家，5万~7万名官兵涉足网络战，规模相当于7个101空降师。

美军大张旗鼓地组建网络战司令部，实际上是承认美国已拥有越来越多的网络战武器，并为未来使用这些武器制造舆论。在软杀伤网络战武器方面，美国已经研制出2000多种计算机病毒武器，如“蠕虫”程序、“特洛伊木马”程序、“逻辑炸弹”、“陷阱门”等。在硬杀伤网络战武器方面，已研制成或正在发展电磁脉冲弹、次声波武器、激光反卫星武器、动能拦截弹和高功率微波武器，可对别国网络的物理载体进行攻击。

网络窃密是最大的情报灾难

传统的间谍人员冒着被捕或死刑的风险想方设法将文件副本偷运出境。但是那些网络空间中的间谍就没有这样的风险。“一名间谍一次可能拿走相当于几本书的材料，”一名高级美国军方人士说，“现在他们可以把整个图书馆偷走。而且如果你把书又重新上架了的话，他们还会再来偷一遍。”

“自从1940年代后期丢失过核机密以来，网络窃密是最大的情报灾难。”总部在华盛顿的智库战略与情报研究中心（CSIS）的吉米·路易斯说。间谍可能是西方面临的最直接的威胁：失去高科技技术可以让西方逐渐丧失经济领先优势，如果真的置身于战争之中，窃密可以削弱其军事优势。

西方的间谍认为中国部署了最勤恳的和最无耻的网络间谍。但是俄国间谍在技术上可能更熟练，也更狡诈。间谍们说，在这一军团中，首当其冲的还是美国的国家安全局和英国的GCHQ，这也解释了为什么西方国家直到最近都不愿意大声谴责计算机窃密。

网络犯罪就是网络战争

互联网的设计目标是方便和可靠，而不是安全。而通过全球网络化，鲜花和野草良莠不齐地同时出现了。网络空间无需护照。警察们被限于国界之内，罪犯却可以逍遥自在地四处漫游。

奥巴马称，去年因网络犯罪造成的损失接近1万亿美元，尽管这一数字存在争议，但却是一个比毒品交易的金额还要庞大的秘密世界。银行和其他公司不愿意承认丢失了多少数据。2008年，在为客户进行的调查中，区区一家电信公司Verizon就报告丢失2.85亿条个人信息记录，包括信用卡和银行帐号等细节。

更令人担忧的是，网络犯罪和网络战争间的界限现在是很模糊的，很大程度上是因为，一些国家将网络犯罪组织视为有用的联盟。一些国家已经表现出他们愿意容忍，支持甚至引导犯罪组织和市民去攻击敌对目标。

在格鲁吉亚的网络攻击案例中，就有这样的情况，市民在俄罗斯军队从陆地和空中入侵格鲁吉亚

的同时，发动了针对目标的网络攻击。专家认为，网络攻击事件与军方行动如此协调，显示出在市民网络攻击者中与俄罗斯军方之间存在着密切的联系。

“许多网络战争的挑战都在网络犯罪中体现出来，因为国家和网络帮派都使用同样的工具。”按照一名德国网络犯罪研究人员的说法，“比如说，任何人都可以去向犯罪组织租用一个僵尸网络，我们甚至可以做到，只要你有钱就可以产生破坏，而不需要知道如何做或者这其中有些什么需要被跟踪。”

网络军备竞赛已经开始

由网络安全公司 McAfee 发表的“虚拟犯罪报告”称，国际间军备竞赛已经移师互联网。

据白宫前顾问保罗·库尔兹（Paul Kurtz）称，法国、以色列和中国都拥有网络武器程序。他在采访了 20 多位专家后得出的结论与上述报告相同。

McAfee 公司总裁戴夫·戴尔特（Dave Dealt）说：“我们从两年多以前就开始预警全球性的网络军备竞赛，但现在我们找到很多证据表明，竞赛已经开始。”

除了美国，俄罗斯、日本、法国、德国、印度等国家，甚至台湾地区，都已经把网络战的部队建制化、编制化。北约正讨论网络战要达到何种程度才能被认定为是某种“武装攻击”的形式，从而责成其成员国提供作为盟友的帮助。

相比于二战之后苏联和美国之间的武器军备竞赛来说，状况有些不同，国家间正在进行着建立网络武器方面沉默的军备竞赛。如果将前者视为决斗，那么网络武器竞赛相对来说可能更加像自由竞赛。

战略和国家关系研究中心的前技术领导人吉姆斯·里维斯不认为已经见到了真正意义上的网络战争，但是他相信网络战争风险正在加大。他说：“网络战争现在不会爆发，但是国家间的竞赛已经毫无疑问地在运行，网络武器存在，而且我们可以预见到敌人也许会使用它们。”

相关链接

几场著名的网络战

“逻辑炸弹”初露端倪

1982 年 6 月，正值冷战高潮时，美国一颗预警卫星发现西伯利亚某地突然起火。人们后来发现，这是一起天然气管道爆炸事件，爆炸原因是控制天然气管道的电脑系统发生故障。可苏联人不知道的是，美国中央情报局的特工人员已经篡改了该电脑里的软件指令，设定了让该电脑在经过相当一段时间后就自动失灵的程序。30 年后的今天，据美国有关人士透露，这是从电脑问世以来最早出现的在软件中植入的“逻辑炸弹”。

7 月 4 日攻击

2009 年 7 月 4 日，当美国人庆祝国家独立日时，他们政府的网站遭到攻击，速度缓慢并且会间断地阻塞对这些网站的访问。这些拒绝服务攻击的目标，包括白宫、国土安全局、秘密服务局、国家安全局、联邦贸易委员会、财政部、国防部等，也包括纽约证券交易所、纳斯达克、亚马逊和雅虎。

随后，韩国政府的 11 个网站遭受相同电脑网络的攻击导致下线，该网络是位于美国境内的 50000 台电脑。互联网安全专家很快判断出有隐藏的敌人发动了针对美国和韩国的攻击事件，并且争论朝鲜是否隐藏在这起事件的背后。

爱沙尼亚信息洪流

2007 年，爱沙尼亚政府和商业站点成为一系列拒绝访问攻击（DDOS）的牺牲品。该攻击持续了数周，影响了爱沙尼亚的在线账号以及电子商务活动。技术分析显示这些攻击来自于俄罗斯国内，但是俄罗斯政府拒绝作出任何回应。这次事件之后，全球各国都开始越来越关注信息防御。北约已经在爱沙尼亚建立了一个“智能中心”以进行信息防御。

俄格冲突 第一场网络战

2008 年 7 月 20 日，一组诡异的信息数据流向了格鲁吉亚政府网站，其携带的信息为“win+love+in+Russia”。伴随而来的，是短时间内以百万计的访问请求汹涌而来，使得格鲁吉亚政府网站瞬间瘫痪。

随着俄军进入南奥塞梯，格鲁吉亚的网络 8 月 8 日再次受到大规模攻击。交通、通讯、媒体和银行的网站纷纷遇袭中招，政府网站系统更是全面瘫痪。甚至，在国家银行的网页上，格鲁吉亚总统萨卡什维利的照片和希特勒等 20 世纪独裁者的照片挂在了一起。