

本	18 各国跳蚤市场人气旺盛
期	19 14岁少女扭转政府预算
导	20 “韩式整容风”吹到美国
读	

新民环球

本报国际新闻部主编 | 第 522 期 | 2013 年 10 月 3 日 星期四 责编:丁珏华

热点锁定



由于国会未通过新财年临时拨款预算案,美国联邦政府非核心部门1日起关闭。这是继1996年后美国联邦政府再次“停摆”。

反恐视点转向互联网 巨大花费堪比无底洞 网络战:来自承包商牟利游说?

文 / 袁原

随着电子技术日益普及,互联网正成为保卫国土安全的前沿阵地。美国国防部担心,未来恐怖分子会利用网络技术攻击美国,为此大手笔招兵买马增强网络战斗力。然而与有限的国防预算相比,网络战争的巨大需求堪比无底洞。

另一方面,网络战争究竟是现实威胁还是商家噱头,仍然存在争议。一些学者质疑,美国军方如此看重网络战斗力的升级换代,与承包商的强势游说不无关系。



美军网络司令部战士在上电脑课

图 G7

模拟“网络版珍珠港”

五角大楼“网络战士”最近的一项任务是利用网络技术更改电脑程序,令一列高速行驶的火车出轨。

这是一列满载放射性物质的火车,正驶往美国东部新泽西州郊区一个小镇。这是一座典型的美国乡村小镇,当地居民闲暇时在一家咖啡馆打发时光,借用那里的免费Wi-Fi在“脸谱”等社交网站闲逛。

然而,平静的表象之下危机四伏。利用同一家咖啡馆的免费Wi-Fi,恐怖分子“黑”入一位顾客的个人电脑。此人在当地一家医院工作,只要盗取他存在电脑里的医院账户密码,恐怖分子就能查阅镇长的电子病历。他们计划对这份病历做些手脚,修改镇长日常用药的剂量,在不知不觉中将他毒死。

恐怖分子还有更为穷凶极恶的计划,例如借助电脑病毒切断小镇电力供给,或者运行一款电脑程序令技术人员以为当地水库遭到化学污染。一旦向水库投入清洁用的化学物质,即令恐怖分子得逞——彻底污染当地水源。

令人庆幸的是,这一切只是一场仿真演习。目标小镇是美国军方网络战争的主要模拟器——电子小镇,位于一个2.4米x3.0米的沙盘之上。这个小镇里的火车、手机信号传输塔和交通信号灯都是玩具店能买到的袖珍模型,全部与镇上的迷你发电厂连接。

电子小镇精巧逼真的设计,反映了五角大楼对网络战争的重视。随着网络技术高度应用,美国军方意识到,未来的战争不仅会在海陆空等传统阵地打响,更有可能向看不见摸不着的网络虚拟空间转移。

军方担心,未来某一天恐怖分子会利用网络技术攻击美国的电力或金融系统。前国防部长帕内塔认为,这样的网络攻击极其致命,堪称“网络版珍珠港事件”。现任国防部长哈格乐也警告,这样的袭击一旦发生,“不费一枪一弹,即可令全国电力和金融系统瘫痪,令军舰或武器库电脑系统休克”。

正因如此,尽管国防预算连年缩减,五角大楼用于网络战争的投入却显著增长:今年投入39亿美元,预计明年将增至47亿美元。

电子小镇就是美国空军新建的网络练兵场之一,军方高层希望借助电子小镇彻底革新作战方式,增强军队网络攻击力。

承建电子小镇的承包商“反黑客”公司创始人斯库迪斯介绍,军方要求电子小镇不仅能训练网络士兵的防御能力,还能提高他们的攻击力,“教会他们网络攻击的动态性:能移动、能引爆、能杀人”。

在军方要求下,“反黑客”公司在电子小镇中添加水库和飞机跑道,还在郊区安装一座玩具火箭发射器,将在年底定期训练时模拟下述情景:恐怖分子更改火箭电脑控制程序,令其袭击医院等平民目标。受训人员的任务是挫败这一阴谋,用网络技术令火箭偏离目标。

网络部队招兵买马

网络战争虽然在虚拟空间打响,但仍需要有血有肉的士兵投入,美国军方为此招兵买马,希望打造一支功夫过硬的网络奇兵。

隶属美军战略司令部的网络司令部现有900多人就职,预计未来两年内将扩招至4900多人。其中三分之一将成为“国家任务组”,利用

电子小镇之类的练兵场受训,掌握网络技术,保护发电站、水库等重要基础设施。另外三分之一将成为“网络保护组”,负责保卫五角大楼网络安全。最后一部分人将组成“战斗任务组”,负责捣毁网络攻击,展开攻击性网络行动。

美国国会数据显示,全军目前有1000多名最高水平的网络战士,但仍然供不应求。美国空军网络指挥官沃特里诺特少将指出,这远远难以满足军方需要,“我们需要2万甚至3万名这样的人才”。

为壮大网络部队,军方不仅在现役军人中筛选人才,也面向全社会招募有天赋的电脑奇才,候选人甚至包括在校初中生和高中生。

通常这些学生会被邀请玩“网络爱国者”之类在线游戏,与假扮敌人的业内高手过招,看谁能先摧毁对方网络。游戏中表现最好的学生可在军方实习,参与一些临时任务。“我们给予他们安全许可,让他们分析那些侵入我们系统的网络攻击。”沃特里诺特说。

位于佛罗里达州赫伯特菲尔德的空军第39信息演习中队是美军最大的网络军事学校,一些被军方选中的少年电脑奇才在这里接受训练,利用电子小镇等模拟器发起实时网络攻击。项目负责人威格乐介绍,训练越来越尖端,假以时日并加倍投入,必能达到保卫美国网络安全的目的。

然而,与有限的国防预算相比,网络战争的巨大需求堪比无底洞。“全都要钱,我们得面对这个财政现实,我们需要双倍人力,可我得掂量掂量这得花多少钱。”威格乐说。

另一方面,军方虽斥巨资培养网络战士,却难以保证他们能抵御

私营企业的高薪诱惑。为保证商业机密和数据安全,越来越多大企业愿意重金雇用网络安全公司服务,而这些公司往往从军方挖墙脚。

网络战争危言耸听?

更多时候,没有硝烟的网络战争既不惊险也不传奇,不过是为计算机安装防火墙、识别有病毒的电子邮件而已。

在五角大楼,各位将军、指挥官每天清晨打开电脑阅读电子邮件时,网络战争就已经打响,他们每个人的收件箱中几乎都暗藏着全球黑客埋下的诱饵。如果某位将军一时大意,点开了一封看似无害的电子邮件中的链接,黑客即有机会入侵国防部网络系统,窥探美国的顶级军事机密。

然而一些学者质疑,窃取知识产权和商业间谍才是目前美国遭受网络攻击的主要类型,所谓“网络版珍珠港事件”其实有些危言耸听。

他们认为,美国军方之所以如此看重网络战斗力的升级换代,与承包商的强势游说不无关系。随着阿富汗和伊拉克局势趋于稳定,网络军备升级自然就成为各大承包商的下一商机。

“棱镜”项目曝光者斯诺登曾经就职的博斯公司每年收入58亿美元,其中半数来自美国军方和情报部门订单。

美国前国家情报总监麦克康纳尔如今就供职于该公司,负责公司业绩增长最快的网络安全业务。麦克康纳尔对网络战争极为看重,曾将其与大规模杀伤武器相提并论。他负责的部门手持为期5年、价值56亿美元的订单,为五角大楼提供情报分析服务。

相关链接

美军网络战斗力

美军在2010年5月建立网络司令部,是统一协调保障美军网络战、网络安全等与电脑网络有关的军事总指挥。

五角大楼表示,网络司令部任务包括侦察、监视、发展、维护和分析。路透社则称,网络司令部是美国军方黑客团队。

网络司令部司令亚历山大说,将在2015年秋季前组建40支网络安全部队,其中13支主要专注于进攻性行动。

美国空军网络司令部副司令海滕说,空军已经选定6种网络工具为攻击性武器。不少网络安全分析师推断,其中包括美国和以色列联手研制的“震网”和“火焰”病毒。这两款病毒据称将用于攻击伊朗核设施电脑网络,“震网”被认为是全球首个用于攻击工业设备的电脑病毒。

正当防卫变攻击

名为“我爱你”的电子邮件附件是时下较常见且往往得手的黑客“钓鱼”软件,由于瞄准美国军方高层发出,这类攻击一旦成功,套取的信息价值之高堪称“钓鲸”。美国空军军官学校计算机系负责人吉布森说:“几乎所有空军将领都时常收到这类邮件,这是军队当下面临的最大威胁。”

针对这类攻击,空军军官学校不仅要求网络安全士官严加防守,还教授他们最狡猾的进攻技巧,期待他们反守为攻。

例如,新生将学习“社交工程学”,即熟知敌国将领名字和容貌,利用社交网络、报纸、电视等渠道掌握他们的日常行踪和生活各方面,在此基础上向他们发出隐含“钓鱼”软件的电子邮件。由于掌握收件人的大量信息,这些邮件编造得极具欺骗性,运气好就能骗得对方点击查看附件或链接。

这样的训练似乎已不属于保护自身网络安全的正当防卫,而是更具挑衅性质的黑客攻击。教授此课的吉布森也承认,校内已因此产生分歧和顾虑。但他坚称:“在我们生活的这个世界,只有知道对方是谁并会如何攻击自己,才能当个称职防守者。”

本刊主编 汪一新 卫蔚

(本刊除“论坛”及本报记者署名文章外,均由新华社供稿)