台军要跟大陆打网络战

□纪　铭/文

美军一份最新的研究报告认为，台湾是世界上最大的电脑零部件制造地之一，将信息技术应用于网络战的能力不断增强，特别在网络攻击、密码破译、散布电脑病毒上尤为突出。于是，台湾当局便在此上面打起了如意算盘——

积极进行网络战部署

台军“汉光21号”演习的最新动向表明，台军军事战略正日益由“防卫型”向“进攻型”转变。台“国防部”自始至终存在着对大陆进行“反制”的“毒蝎作战计划”，其中第一击锁定的5类目标中就有大陆的网络和通信中心。

据分析，台军网络战的策略是利用台湾强大的计算机硬件和软件优势，对大陆可能的军事行动进行“反制”和“阻吓”，开辟第二战场（信息战场）以协助主战场（传统战场）的防守和反击。制定的方案大致包括两个方面。

硬件部署。利用台湾在计算机硬件上的优势以及大陆对台湾产计算机配件的依赖，在销售到大陆的产品中嵌入病毒芯片，在合适的条件下，通过遥控触发病毒，对计算机系统和用户数据进行破坏。台军提出了在特定硬件比如主板和板卡的秘密接口规范的建立问题，就是在所有硬件中包含一个可以破坏板卡硬件及其相关设备的自杀指令。这个病毒硬件的方案称作为“木马”计划，也有另外一个名称叫作“宙斯盾”或“神盾”计划。据此，在台湾“国防部”下达的网络战任务中，台军会在特定时候对某些型号的硬件加上病毒芯片再销往大陆，并且有权通过海关监控硬件厂商各种型号产品出口到大陆的销量。一旦台“国防部”监控并预测到某种型号的产品有必要加上病毒芯片，就会马上采取行动。

病毒部署（即软件部署）。病毒部署其实是一种软件部署的方式，分为纯软件和软硬结合两种。软硬结合的方式就是通过硬件对信号的捕捉，使得软件病毒能够在需要的时候通过硬件遥控激活。台军在纯软件方案中，针对大陆流行的操作系统大致划分了三个方向：一个是D&W“达尔文”计划，攻击的对象为DOS和Windows操作系统的机器；一个是针对Linux及Unix以及大陆科研单位和教育部门中比较流行的VAX/VMS系统的“茉莉”计划；还有一个就是高度保密的Internet网络计划。

此外，在网络战中，台军网络战部队还将进行病毒注射行动。病毒注射是网络战的一个重要组成部分，包括网络注射和开放式注射两种，其中开放式注射又包括无线电注射和线缆注射等几种。病毒注入以后，将以三种方式进行侵犯，一个是对关键数据的修改或者破坏，另外一个就是数据的窃取和传播，再有就是类似于CIH病毒的对关键硬件的破坏和摧毁。值得注意的是，台军提到大陆的GSM通讯网络将是无线攻击的重点。台军的目标是一旦病毒注射计划开始，就攻击大陆所有的网站。

大力加强网络战建设

台湾当局认为，信息制胜是孙子兵法的精髓，可以做到不战而屈人之兵，而网络战是信息战的主要手段之一。所以，台军要积极地利用较先进的信息技术迅速发展其网络战的能力，其目的是在网络战中“先机制敌”，实施主动性的信息攻击措施。从2004年1月起，台军方的“军事事务革新案”宣称，将以“资电先导”，致力于科技、指挥控制、通信战力的提高，企图打网络战与电子战以及不对称战，达成“先制”解放军的目的。

台军方认为，网络战的武器完全可以做到立足于本岛，而不像其他武器那样几乎靠从美国进口。台湾当局认为，台湾社会和军队的信息化程度要低于美国，但远高于大陆；台湾有高度发达的计算机产业和信息基础设施以及众多的计算机人才，是进行网络战的内在的优势，是台军在网络战中创造“不对称战争优势的最佳切入点”。因而，台军强调以己方网络战“点”的优势去攻击大陆之要害部位——信息与指挥中枢，达到以弱胜强、以小胜大的目的。为此，台军近年


电脑已成为台军必备的军用物资

来主要采取了以下一些措施。

一是建立指挥机构。台“国防部”已成立网络战最高指导机构——“国军信息战策略规划指导委员会”以及负责网络战所需先进技术研究与规划的“国军信息战实验室”和专门处理信息战、保护计算机安全的“信息战委员会”。台参谋本部还设立了通信电子参谋次长室，并成立了通信电子资讯局，负责台军的通信、电子、信息战等的政策与计划。这些机构制定了一系列有关网络战的计划，如台“国防部”制定的“资安”计划、“毒蝎作战计划”等。从2001年开始，台军方为信息网络战拨出专项预算，其组织、装备和经费会逐年扩大。

二是成立了一个专门研究大陆通讯网络连接方式的小组。该组的目的就是精确勾画大陆军用网络和民用网络的分布和部署，以便通过不设防的民用网络，有效攻击大陆军方的军用网络和截击在民用网络上流通的军用数据。目前，台军的网络研究小组已经解决了计算机病毒的网络触发和控制问题。另外，台军还组建了一个研究小组，着重研究中国电信IP电话网络的安全性和可攻击性，目的是使台军网络战部队可以在战时通过Internet对中国电信的程控电话交换机网络进行控制和破坏。

三是组建黑客部队。代号为“老虎部队”的网络战部队于2000年1月1日正式组建，是一个常备黑客小组。据台军规划，“老虎部队”直属参谋本部，针对信息战的攻防技术进行研究与开发，专门侦测和记录大陆网站的漏洞和修补情况，作为战时的技术储备。台军方每年还从地方招收计算机专业的博士和硕士数十名，以充实网络战的人才储备。台湾当局曾扬言，已研制出上千种军用计算机病毒，具备摧毁大陆网络、进入大陆计算机窃取或假造数据的能力，还可释放蠕虫病毒致瘫大陆的指挥和控制系统。

四是开展网络作战训练。比如在台军“国防大学”开展信息网络战试验和训练，组织部队学员实施网络攻击模拟实验。学员经6小时的训练后，其网络目标辨识正确率达77%，目标弱点侦测正确率达100%。因而台军得出的结论是“只要有标准的网络作战程序与对应的软件工具，并施以短期的教育训练，所有人都可以正确地对分配或指定之目标进行侦察与攻击作业”，并据此提出网络作战要平战结合，平时即对民网各类目标进行侦察整理，建立一套网络战攻击目标库，以便战时启用。

五是加强对通信网路的建设。台军方光纤网路系统的完成使台军的网络战力大幅提高。台军认为，军方光纤通信网路系统为建立“国防”信息基础建设（DII）创造了有利条件，不但能满足台湾军方新一代指、管、通、资、情、监、侦等系统的传输需求，还可配合台信息基础建设（NII），与民间通资系统相结合，具备互为支援的功能。

不断提高网络防御能力

台军深知台湾岛内的经济严重依赖计算机系统，如果针对台湾的银行及其他核心部门的网络战一旦奏效，将对台湾的经济造成严重威胁，其威力不亚于导弹；加之台军各单位“公文电子化”建制日益成熟，资料传输、交换使用频繁，网络漏洞和风险也越来越大。

针对可能面临的网络攻击，台军将网络的威胁划分为两类并制定了相应的防护措施：对付电脑病毒将主要采用密闭网路，指挥控制系统采用实体隔离措施，以减少病毒由因特网直接入侵机会；其次是建立入侵侦测机制，以模拟黑客攻防及电脑病毒危机应变能力。而对可有效摧毁电子装备的电磁脉冲武器，台军认为首先是要强化远程预警能力，其次是系统采用分散式设计，以避免系统装备因遭破坏而丧失指挥、控制能力，造成指挥机制的全面瘫痪。

台军为了避免未来遭受网络攻击的威胁，台“国防部”于1999年编列了“网安”计划，大力提升台军的网络安全防护能力，并研发更为先进的网络安全防护系统，以适应未来的网络战。☆

（责编/牛俊峰）


网络战就是电脑干扰对手的战斗