网络战正成为一种低风险的颠覆手段

迟延年
(武警杭州指挥学院,杭州 310023)

摘 要:互联网已被广泛应用于国家间的政治文化渗透,以美国为代表的西方国家更是将其作为干涉别国内政,甚至颠覆别国政权的手段。为了更好地进行网上攻防,各国注重加强网络战力量的建设。为了确保互联网领域的安全,我们必须加快核心信息技术发展,依法维护互联网领域的合法权益,并加强网络安全力量建设。

关键词:网络战;颠覆手段;"Twitter 革命"
中图分类号:D61 文献标志码:A 文章编号:1002—2589(2009)19—0119—02

自从互联网进入大众化、全球化的时代,网络"无疆界"、"零距离"、"即时性"的特性便被有意识地用于进行国家间的政治文化渗透。与以往常用的电台、电视、报纸等工具相比,互联网不仅传播速度快、范围广、信息量大,而且可以匿名、匿源传播,成本低廉,隐蔽性好,灵活性强,不仅降低了"舆论攻击"和渗透的门槛,也有利于一些政府和团体掩饰自己的介入。由于西方发达国家在相当程度上掌握着网络的技术制高点,控制着网络的连接权、话语主导权,因此在"网络战"方面具有先天优势。近年来,不少发生动荡的国家不约而同地指责来自"外部敌对势力"的网络威胁,认为这是造成动荡局势的重要根源之一。

一、两起通过网络操纵的颠覆阴谋

1.发生在摩尔多瓦的"Twitter 革命"。4 月 7 日,摩尔多瓦大选后发生的那场未获成功的"颜色革命"就被称为"Twitter 革命"(Twitter 是美国的一个微型博客社交网站)。摩尔多瓦的青年组织"HydePark"和"ThinkMoldova"策划了"Twitter 革命",其网站得到了美国国务院文化和教育局的资金支持。"ThinkMoldova"领导人之一纳塔利娅·莫拉里在自己的博客中这样描述:"6 个人,只用了 10 分钟的快速思考便作出决定,然后用数小时通过网络、'脸谱'、博客、短信和电子信箱将消息传播出去……结果 1.5 万名年轻人走上街头。"哈伊·莫斯科维奇事发当天一直在通过 Twitter 网站对示威活动进行图文报道。第二天,他和同伴们通过"脸谱"和 Twitter 网站向外传播消息时,还特地为消息制作"#pman"的标签,这几个符号正是摩首都基希讷乌市中心广场的罗马尼亚语缩写。当网络被切断后,莫斯科维奇就用群发短信的方式散布信息。摩尔多瓦"Twitter 革命"的幕后推手是金融大鳄乔治·索罗斯,他经常利用 Twitter 等网站,在美英看不顺眼的国家制造动乱。索罗斯开放社会研究所有专门的技术人员,负责向"相关人员"传授如何利用互联网在"封闭社会"推动"民主运动",以推翻"专制政权"。而且,他们的目标不只是摩尔多瓦,还有塔吉克斯坦、叙利亚和泰国。尽管摩尔多瓦"颜色革命"最终没有成功,但充分显示了社交网站在造谣惑众、制造混乱方面的"别样作用"。

2.伊朗成"新颠覆手段试验场"。Twitter 等社交网站再次显示出巨大的"煽动力",是在 6 月份的伊朗大选,它成为策划、煽动伊朗社会动荡的重要推手。美英和以色列情报部门通过 Twitter、facebook、Youtube 等网站,散布耸人听闻的消息让伊朗民众"中毒",并引发强烈不满情绪。首先,在选举当晚散布消息称穆萨维获胜,于是当几小时后内贾德宣布胜选时,看上去就像一个大骗局;随后,一些社交网站和微型博客的用户开始接收到一些关于政治危机和街头抗议行动的似真似假的匿名消息,主要是枪击和大量人员死亡等"骇人听闻"的消息,而这些消息直到现在都未得到证实;与此同时,中情局还指使美英等国的反伊朗政府者继续煽动混乱局面。处于混乱中的普通民众,无法分辨 Twitter 上信息的真实性,没人清楚信息发布者到底是德黑兰抗议活动的目击者还是中情局特工。其实,这正是美国中情局想要的效果,其目的就是制造更大的混乱,让伊朗人内讧。

二、美国加紧网络战能力建设

网络战攻防对美军而言并非新概念,各军种内部早已建立了从事网络攻防的专门单位。不仅直属国防部的美国国家安全局、国防信息系统局有自己的网络战部队,美战略司令部也在 2005 年成立了由顶级电脑专家和黑客组成的"网络战联合功能司令部",空军 2008 年成立了专门负责网络攻防的第 24 航空队。陆军也早已建立计算机应急反应分队,重点

作者简介:迟延年(1970-),男,山东莱州人,现为武警杭州指挥学院军事理论教研室主任,副教授,军事学硕士,主要从事军事理论研究。

是对付战术层次的电脑威胁，必要时发起网络攻击，侵入别国军事网络。海军则在“舰队信息战中心”成立了“海军计算机应急反应分队”。目前美军共有 3 000~5 000 名信息战专家，5~7 万名士兵涉足网络战。如果加上原有的电子战人员，美军的网络战部队达到 8.87 万人左右。

国务卿希拉里·克林顿积极推行“网络外交”，重视利用社交网站“脸谱”、视频共享网站 Youbube、图片共享网站 Flicdr 和 Twitter 这些平台传递外交政策信息，声称要以网络软管理来应付那些打压国内媒体的国家。美国防部长罗伯特·盖茨也坦言，Twitter 等社交媒体网络是美国“极为重要的战略资产”，奥巴马政府已经把社交网站视为“箭袋中的一支新箭”。2009 年 6 月 23 日，国防部长盖茨正式下令成立网络战司令部，把分散在全军的网络战部队整合起来，并强化各机构间的协调作战能力。美国政府的专门研究报告《关于美国获得和使用网络攻击能力的技术、政策、法律与道德问题》称，网络攻击的范围很广，既包括小规模冲突，也可能是全面战争。在战场上，网络攻击可以用来抑制敌人的防空能力，破坏指挥、控制和通信系统，瓦解智能武器。报告指出，网络攻击还包括一些较为隐蔽的行动，可以用于旨在影响政府、事件、组织或个人的秘密行动。

对于 Twitter、“脸谱”等社交网站在伊朗动荡中所起到的“关键作用”，西方表现得颇为兴奋，因为他们发现，在互联网上，“一种新的、强有力的力量正在生成”。伊朗危机证明了，Twitter 已成为一种强有力的政治工具，这种既可以影响伊朗，又不使自己深陷其中的方式正是美国所需要的。

三、我国要加紧应对网络战的准备

1.加快信息技术发展，确保核心专网的绝对安全。由于美国拥有对互联网域名根服务器的监控权，加上在计算机硬件和软件上的极端垄断地位，美国已牢牢掌握了国际互联网的控制权。5 月 30 日，微软宣布不再为古巴、朝鲜、叙利亚、苏丹和伊朗五国用户提供 MSN 接入服务，理由是这五国被美国政府列入了禁止提供授权软件服务的被制裁国家名单。微软的“小试牛刀”，为世界敲响了警钟：在制海权、制空权、制天权之兵，制网权将成为左右未来战争胜负的另一战略制高点。这并非耸人听闻，虚拟空间的“多国演义”正在上演，除美国外，俄罗斯、日本、印度等国都在积极准备应对所谓“第六代战争”，把“网络防御—攻击”视为保卫国家利益的重大问题。以美英为代表的西方故意虚构、炒作“中国网络间谍”，并渲染中国黑客的“官方背景”，表明他们已将中国视为其网络战的重要目标。

网上的攻防没有硝烟，但却可能造成实实在在的巨大损失，必须切实做好互联网的防御，尤其要确保金融、电力、国防等核心专网的安全。一要确保核心专网与国际互联网物理隔离。任何的技术防护都可能被攻破，所以，金融、电力、国防等国家要害系统必须独立建设专网，不与国际互联网连接，确保国家的核心利益不受威胁。二要尽快摆脱美国在互联网领域的软件和硬件控制。目前互联网领域的软件和硬件都是美国的天下，使用别人的产品和技术，难免受制于人。所以，必须加快网络核心技术的自主化进程，下决心集中力量攻关，扶持国内网络核心技术及产品的推广，争取国内终端早日用上性能可靠的“中国芯”和自主产权的操作系统。三要加强网络防护技术研究，提高屏蔽、锁定、反击网上恶意攻击的能力。只有这样，才能真正形成互联网防御的“铜墙铁壁”。

2.要理直气壮地维护互联网领域的合法权益。对一个国家来讲，网上的有害信息一般可以分为三类：一是色情信息，会对青少年的健康成长造成危害。二是宣传邪教的信息，会对民众的身心造成危害。三是国内外敌对势力的策反、离间宣传，会蛊惑人心，影响社会稳定与国家安全。另外，分裂势力、恐怖势力也会利用互联网进行串联，从事危害社会稳定和国家安全的秘密活动。所以，任何一个国家的政府都有权对本国的网络实施必要监管，最大限度地避免网络带来的不良影响。美国在本国的图书馆等公共场所，也会通过硬件、软件来过滤有害信息。5 月 19 日，工业和信息化部发文，要求在我国境内生产销售和进口销售的计算机预装 “绿坝–花季护航”绿色上网过滤软件。相关部门针对谷歌传播不健康信息的事实，要求谷歌从其中文搜索网站中过滤掉国外色情网站。美国对我国政府这些合理合法的监管措施进行大肆攻击，以涉嫌违反“监管透明”原则及 WTO 规定为由，要求我国取消预装“绿坝”软件的计划。

笔者认为，美国这样做，一方面是其霸权主义心态在互联网领域的表现。难道在美国本土，美国政府能坐视互联网危害其民众思想及国家安全而不管吗？只是因为，安装“绿坝” 的行为 “体现了中国进一步强力控制互联网接入的意图”，所以美国一定要阻止—典型的霸权主义心态。对各自国内的互联网用户实施监管，是互联网领域的“内政”，我们并没有要求美国用户安装“绿坝”，在中国境内，我们有拒绝有害信息的权力，美国的干涉是无理取闹！另一方面，美国主导的发生在摩尔多瓦和伊朗的“Twitter 革命”给了我们一个启示：美国关心的不是中国青少年会否受到色情信息的毒害，它真正担心的是“中国强力控制互联网接入”后，美国就失去了在中国策划“Twitter 革命”的可能性。不要忘记，“法轮功”、藏独、疆独等势力都受到美国相关部门或明或暗的支持。

美国总是对别国提出这样那样的要求，却不检点自己的行为—自我标榜成全球反恐先锋，但却拒绝向中国引渡东突恐怖分子，反而将其释放。此次策划乌鲁木齐“7·5”暴力恐怖事件的幕后黑手热比娅，目前就定居在美国，其分裂活动得到了美国部分国会议员和美国国家民主基金会的支持，并曾受到时任美国总统小布什的接见。美国就是这样，永远有理由损人利己！所以，要理直气壮地对美国的指手画脚说“不”！坚决维护互联网领域的合法权益。

3.要加强网络安全力量建设。一方面，害人之心不可有，防人之心不可无。有效的防御离不开专业的网络安全力量。另一方面，人不犯我，我不犯人，人若犯我，我必犯人。为了在受到网络攻击时实施强有力的反击，也必须拥有专业的网络安全力量。所以，国家、军队以及各专业网，都要组建专门的网络安全力量，在加强防御，确保自身安全的基础上，以其人之道反治其人之身，对网络攻击实施有力的反击，震慑别有用心者的不良企图。 （责任编辑 / 吴凤华）