维护好网络政治安全是根本

本报记者 **罗 俊**

根据中国国家互联网应急中心的最新数据显示，今年3月19日至5月18日，2077个位于美国的木马或僵尸网络控制服务器，直接控制了我国境内约118万台主机，同时，2016个位于美国的IP对我国境内1754个网站植入后门，涉及后门攻击事件约5.7万次。在社会发展全面信息化的今天，网络安全问题已经上升到事关国家安全的重大战略问题，没有网络安全就没有人民安全，更没有国家安全。如何筑起网上长城，让网上中国长治久安，俨然成为当下最为迫切的话题。

制图：潘旭涛

现实：网络大国隐患多

2014年是我国接入国际互联网20周年。据统计，到2013年底，我国互联网上网人数6.18亿人，普及率已达45.8%。其中，我国移动互联网用户数占移动电话用户的67.8%，手机网民达到了5亿人。毫无疑问，中国已经是一个网络大国，可同时也是被信息窃取和网络攻击的主要受害者，网络安全压力巨大。

“网络安全的首要方面是网络与信息系统的安全。”中国互联网信息办公室副主任王秀军介绍说。当前，少数国家利用掌握的互联网基础资源和信息技术优势，大规模实施网络监控，大量窃取政治、经济、军事秘密以及企业、个人敏感数据，甚至还能远程控制他国重要网络与信息系统。“斯诺登事件就是一个很好的例子，试想，在危机时刻，如果一个国家涉及国计民生的关键基础设施被人攻击后瘫痪，甚至军队的指挥控制系统被人接管，那真是‘国将不国’的局面。”

除了开篇提到我国面临来自美国的网络攻击外，权威数字还表明，同期监测发现，135台位于美国的主机承载了563个针对我国境内网站的钓鱼页面，造成网络欺诈侵害事件约1.4万次，主要是仿冒网站，诈骗个人位置信息、个人数据信息、口令密码信息等。此类行为既有商业窃密，也有网络欺诈，致使中国网民蒙受巨大损失。

然而，除了网络与信息系统的安全外，目前更重要的是急需维护好网络政治安全。“政治安全是根本。”王秀军介绍说。目前，境外敌对势力将互联网作为对中国渗透破坏的主渠道，以“网络自由”为名，不断在网上进行有针对性的攻击诬蔑、造谣生事，试图破坏中国的社会稳定和国家安全。“在互联网上，能否赢得意识形态领域渗透和反渗透斗争的胜利，在很大程度上决定我们党和国家的未来。”

战略：列为“一把手工程”

实际上，从上世纪80年代初期开始，中国国务院就开始设立相关机构，加强对信息化的领导和管理。可是由于历史原因，我国的互联网管理、网络安全管理曾是“九龙治水”，存在多头管理、职能交叉、权责不一、效率不高等弊端。比如，原有的管理体制机制难以统筹经济社会、国计民生各领域的网络安全和信息化，难以统揽党委、人大、政府、政协、高检、高法等单位和部门的网络安全和信息化，难以使科技、公安、财政、保密等相关职能部门就具体政策进行协调。

随着网络安全和信息化在国家安全与发展中的地位与作用不断提升，客观上也要求把网络安全和信息化作为国家的重大战略，由党和国家最高领导亲自抓。“世界上许多国家，也都将网络安全和网络空间发展工作作为国家的‘一把手工程’。”王秀军介绍说。2014年2月27日，中央网络安全和信息化领导小组宣告成立。

据国家信息化专家咨询委员会委员汪玉凯介绍，这一领导小组不单是领导信息化工作，而且把网络安全放在更突出的位置，将网络安全问题与国家信息化整体战略一并考虑，同时可以发挥集中统一领导作用，统筹协调各个领域的网络安全和信息化重大问题，制定实施国家网络安全和信息化发展战略、宏观规划和重大政策，不断增强安全保障能力。

可以说，中央网络安全和信息化领导小组的成立，规格之高是前所未有的。这充分体现了党中央对网络安全和信息化工作的高度重视。“为做好领导小组决定事项的贯彻落实，中央还成立了领导小组办公室，与国家互联网信息办公室一个机构、两块牌子。”王秀军说。

行动：多措并举保安全

从政策层面来看，中央已经对网络安全和信息化工作作出了整体布局，在中央网络安全和信息化领导小组第一次会议上，审议通过了2014年重点工作，对当前和今后一个时期的网络安全和信息化工作进行了部署。

王秀军介绍说，今年的工作是加强顶层设计和战略统筹，加快制定网络安全和信息化发展战略、宏观规划和重大政策；创新改进网上宣传，弘扬主旋律，激发正能量，综合治理网络生态；加快制定急需的网络安全和信息化法律法规与技术标准，加强自主创新，建设网络安全保障体系；大力提升国民经济和社会发展各领域信息化水平，促进信息产业发展，推动文化、出版、广播电影电视数字化发展，推进军民融合；加快人才队伍建设，提升全社会的网络安全意识，分领域、分类型、分层次加快人才培养。

在具体的技术层面，中国工程院院士、光纤传送网与宽带信息网专家邬贺铨认为，在网络安全方面，如果自己没有过硬的技术，就很难实现安全可控的管理。在他看来，提高技术自主创新能力、加快建设网络人才队伍和在国际互联网治理中积极发挥作用是我国目前最需要在实际行动上下功夫的三个方面。

“当前，我国所用的个人计算机和手机的操作系统几乎都是国外的，核心芯片依赖进口，这是很大的隐患。”邬贺铨说，“外国的核心技术是买不来的，也是市场换不来的，但我国的市场对培育自主创新的技术和产品具有十分重要的作用。这就要求我们在培育网络核心技术方面也要发挥市场在资源配置中的决定性作用和更好发挥政府的作用。”

网络窃密：美国贼喊捉贼！

徐 蕾

“斯诺登事件”的尴尬还在，美国却像得了健忘症似的，忘了自己才是当今世界上最大的网络窃密者，也是中国网络的头号攻击国，几天前竟然指责中国军人从事黑客犯罪。无中生有不说，其跳出来贼喊捉贼的时机恰好在亚信峰会讨论安全议题以及中俄元首会晤之际，蓄谋之久、用心之卑劣实在让人不齿。 其实，这已经不是美国第一次用网络安全的名义拿中国说事。从2011年到2014年，美国以类似网络安全话题指责中国达12次，中国均予以驳斥和抗议，让世人越来越看清美国的真面目。

此次，中方的回击除了通过外交强烈抗议，并要求美国撤销起诉外，还决定终止中美网络工作组活动。去年，中美同意在战略安全对话框架下建立网络工作组，以寻求合作。然而此次事件的发生，证明美方对通过对话合作解决网络安全问题缺乏诚意。如果说斯诺登的棱镜门事件揭示了中国乃至全球面临来自美国国家网络安全战略的直接威胁，那么此次早有预谋的“起诉事件”更告诉我们中国加强国家网络安全的迫切性，更证明了中国把网络安全放在国家战略高度之决策的英明，更坚定了中国在网络安全方面果断布局和加大投入的决心。 与其被动挨打，不如主动出击。在网络安全方面，我们看到中国正在制定相关审核制度，正在加强核心技术自主创新和国产化，正在通过相关政策法规和法律手段保障我国的网络空间利益，正在积极改变中国在国际网络空间话语权劣势的局面。

风物长宜放眼量。中国作为负责任的大国，要在全球网络治理的转型中提出公平公正的战略主张，推进全球网络空间治理新秩序，造福全球网络。

我国将出台网络安全审查制度

记 者 22日从国家互联网信息办公室获悉，为维护国家网络安全、保障中国用户合法利益，我国即将推出网络安全审查制度。该项制度规定，关系国家安全和公共利益的系统使用的重要技术产品和服务，应通过网络安全审查。

国家互联网信息办公室发言人姜军指出，网络和信息技术产品是否安全、是否可控，事关国家安全，事关中国经济社会健康发展，事关广大人民群众合法权益不受侵犯。长期以来，少数国家政府和企业利用自己产品的“单边垄断”和技术“独霸”优势，大规模收集敏感数据，不但严重损害了广大用户的利益，而且对其他国家的网络空间安全造成巨大威胁。这位发言人表示，近年来，我国政府部门、机构、企业、大学及电信主干网络遭受大规模的侵入、监听，深受其害。特别是去年6月初发生的“斯诺登事件”，为世界各国敲响了警钟，充分印证了“没有网络安全就没有国家安全”这一深刻的道理。目前，我国网民数量跃居世界第一，已成为网络大国，加强法律制度建设势在必行。网络安全审查制度的出台，将成为维护国家网络安全最有效的法理依据，对于网络强国建设具有重大推动作用。

据专家介绍，基于维护自身安全和社会稳定，针对信息技术产品及其供应商开展不同形式的网络安全审查，我国并非第一家，在美国早有先例。2012年，美国众议院情报委员会就以国家安全为由，对我国企业进行安全审查。此外，为应对日益应用广泛的云计算，美国政府还针对云计算服务提供者进行安全审查，并明确规定联邦政府部门只能选择通过审查的云计算服务提供者提供的服务。

据了解，我国即将推出的网络安全审查制度，规定对进入我国市场的重要信息技术产品及其提供者进行网络安全审查，审查的重点在于该产品的安全性和可控性，旨在防止产品提供者利用提供产品的方便，非法控制、干扰、中断用户系统，非法收集、存储、处理和利用用户有关信息，对不符合安全要求的产品和服务，将不得在中国境内使用。

（本报记者 **徐 蕾**）

美国是如何进行网络安全审查的

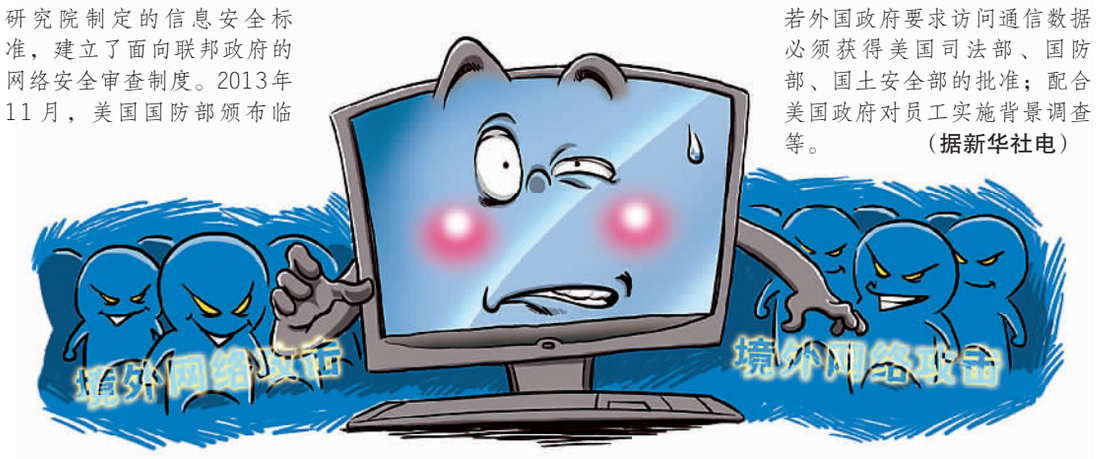
2000年，美国率先在国家安全系统中对采购的产品进行安全审查，随后陆续针对联邦政府云计算服务、国防供应链等出台了安全审查政策，实现了对国家安全系统、国防系统、联邦政府系统的全面覆盖。审查对象不仅涉及产品和服务，还会针对产品和服务提供商。

随后，美国等西方国家为保障国家安全、防范供应链安全风险，逐步建立了多种形式的网络安全审查制度。将全方位、综合性的供应链安全审查对策上升至国家战略高度。

美国网络安全审查标准和过程是不公开的。美国对供应链安全审查的过程、标准、机制完全封闭，不披露原因和理由，不接受供应方申诉。主要考虑对国家安全、司法和公共利益的潜在影响，且其审查没有明确的时间限制。

美国安全审查的要害之一，是安全审查结果具有强制性。美国国家安全系统委员会2000年1月发布的《国家信息安全保障采购政策》规定，自2002年7月起进入国家安全系统的信息技术产品必须通过审查。2011年12月，美国政府发布《联邦风险及授权管理计划》，要求为联邦政府提供云计算服务的服务商，必须通过安全审查、获得授权；联邦政府各部门不得采用未经审查的云计算服务。美国在政府采购招标文件中还进一步规定，向联邦机构提供云计算服务的基础设施必须位于美国境内。

从开始建立至今，美国的网络安全审查范围不断延伸。2000年1月，美国国家安全系统委员会发布了《国家信息安全保障采购政策》，对涉及国家安全的信息系统采购的信息技术产品进行安全审查。2002年，美国联邦政府执行美国国家标准技术研究院制定的信息安全标准，建立了面向联邦政府的网络安全审查制度。2013年11月，美国国防部颁布临时政策，规定国防系统及其合同商采购的产品和服务要经过供应链安全审查。

美国网络安全审查的内容不局限于技术。美国联邦政府要求，不仅要审查产品安全性能指标，还要审查产品的研发过程、程序、步骤、方法、产品的交付方法等，要求企业自己证明产品已达到了规定的安全强度。

美国要求被审查企业签署网络安全协议，协议通常包括：通信基础设施必须位于美国境内；通信数据、交易数据、用户信息等仅存储在美国境内；若外国政府要求访问通信数据必须获得美国司法部、国防部、国土安全部的批准；配合美国政府对员工实施背景调查等。 （**据新华社电**）