印度如何维护国家网络安全

刘 翔
（广州市科技创新委员会，广州 510030）

摘 要：本文研究了印度近年来维护国家网络安全采取的一些新的举措，分析了印度目前的网络安全形势，认为印度通过立法、发布新政、制定新的体系框架、开发自有操作系统、加强网络监管和提高民众网络安全意识取得了积极成效。本研究将为我国把握世界网络安全形势、维护国家网络安全提供参考。

关键词：印度；国家安全；网络安全
中图分类号：G327.351 **文献标识码：**A DOI：10.3772/j.issn.1009-8623.2015.05.008

网络安全是指通过采取各种技术和管理措施，使网络系统连续可靠地正常运行，从而确保网络数据的可用性、完整性和保密性[1]。信息化时代，网络安全日益成为各国关注重视的焦点。习近平总书记主持召开中央网络安全和信息化领导小组第一次会议时强调，网络安全和信息化是事关国家安全和国家发展，事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。印度是我国邻国，也是世界知名信息技术大国，在维护国家网络安全方面也早有行动，并积累了一些经验。2013 年斯诺登泄密事件更是重新引发了印度政府对网络安全的重视，采取了一些新的举措。本文拟作简要介绍，言其大略，探析印度如何维护国家网络安全。

1 印度网络安全形势不容乐观

据印度时报报道，截至 2013 年 12 月，印度互联网用户达 2.38 亿人[2]。印度网络快速发展的同时也存在巨大的安全隐患。2014 年 1–5 月印度共有 9 174 个网站受到来自世界各地的黑客攻击，攻击形式主要有网络钓鱼，扫描，垃圾邮件，恶意代码，网页入侵。此外，同期印度还有 62 189 起网络安全事故上报印度计算机紧急响应小组[3]。有数据显示，印度已成为继美国之后的第二大垃圾邮件发送国。印度还是恶意软件的主要受害国之一，2010 年在印度境内肆虐的“超级工厂”病毒就对该国的网络基础设施造成严重破坏。印度的网络犯罪现象也极为严重，小到盗用个人信息、传播病毒，大到经济诈骗，甚至危害国家安全。世界知名杀毒软件供应商偌顿公司发布的报告显示，76% 的印度互联网用户成为网络犯罪的受害者[4]。网络安全软件开发商卡巴斯基近日发布的一项报告也显示，印度的手机上网用户在世界上第二易遭受网络攻击，仅次于俄罗斯[5]。

此外，由于印度在政治上属民主国家，科技文化上紧跟西方，英语又是其官方语言，以英语为媒介的印度互联网与西方国家的网络基本上是一体化的，这就使得印度比许多非英语国家更容易暴露在网络犯罪国际化的威胁下，给国家网络带来严重的安全隐患。

2 专门立法从源头上打击网络犯罪

为打击网络犯罪，早在 2000 年印度国会就通过了《信息技术法案》。该法案规定向任何计算机或计算机系统传播病毒或导致病毒扩散，以及对电

作者简介：刘翔（1983—），法学硕士，主任科员，主要研究方向为经济法学、科技政策。
收稿日期：2015-05-14

脑网络系统进行攻击或未经许可进入他人受保护的计算机系统等行为，都构成网络犯罪。该法还对一些网络犯罪的具体惩罚做了明确规定，如黑客可被判处 3 年以下有期徒刑，或最高 20 万卢比的罚款；网上传播淫秽色情信息将面临最高为 5 年的有期徒刑。未经许可进入他人受保护的计算机系统，最高可判处有期徒刑 10 年。这是印度第一部有关如何规范网络活动的专门法。印度由此跨入了当今世界 12 个在计算机和互联网领域专门立法的国家之列[1]。为适应信息技术的发展和形势的不断变化，印度在 2008 年和 2011 年又先后两次修订《信息技术法案》中涉及网络犯罪的相关内容。《信息技术法案》的制定和实施，为打击网络犯罪、维护网络安全提供了一个基本的法律框架。

3 发布国家网络安全政策强化顶层设计

2013 年 7 月 2 日，印度通信与信息技术部发布了《印度国家网络安全政策 2013》（National Cyber Security Policy–2013）[6]，从国家层面引导政府机构、非政府组织、企业、个人等多方开展网络安全行动，建立一个自上而下的网络安全框架。政策主要包括使命、任务、目标、战略四部分内容。其中在战略部分提出要采取 13 大措施创造安全网络环境：

（1）创建安全网络环境；

（2）创建安全网络框架；

（3）鼓励开放式标准；

（4）强化控制框架；

（5）创建网络安全威胁早期预警、反应和弱点评估机制；

（6）强化电子政务服务；

（7）加强对关键网络设施的保护；

（8）促进网络安全研发；

（9）降低供应链风险；

（10）加强网络安全人才培养；

（11）提高网络安全意识；

（12）加强公私合作；

（13）加强信息共享与合作。这项国家政策将统一印度政府之前制定的多个不同的网络安全项目，强化顶层设计，统筹推进网络安全有关项目的实施。

4 制定计划改进关键部门网络安全

印度政府为应对日益增多的网络攻击和虚拟世界中的安全挑战，于 2013 年 5 月宣布实施一个为期 5 年的项目，从整体上加强国家关键部门的网络安全设施。项目由国家关键信息基础设施保护中心（NCIIPC）承担，该中心负责协调全国各地的关键基础设施网络安全运营工作，并制定为期 5 年的计划以彻底改善和整合所有关键基础设施（如电力、交通、供水、电信和国防）的网络安全设备。该中心还计划成立部门计算机应急响应小组（CERT）与其连网，在所有关键系统上安装传感器，向指挥和控制中心提供网络攻击的实时信息。印度政府还对 NCIIPC 和 CERT 进行了任务分工。NCIIPC 负责照看绝对关键、易受攻击威胁和对计算机与信息技术依赖较大的部门，比如，能源（电力、煤炭、石油和天然气）、运输（铁路，民航）、银行及金融、电信、国防、航天、执法和安全等部门。其他部门由 CERT 负责。印度政府要求各部门提高警觉意识，各个机构自行建立可靠的安全系统，随后与 NCIIPC 进行连接，当不同系统遭受相同病毒的攻击时，就不必单独对其进行分析和制定不同的应对措施。NCIIPC 还建立了一个网络安全运行中心（控制一天 24 小时的实时监视信息和反应）以及一个国家关键信息基础设施保护研究所，培训首席信息安全官，每日发布网络警情。

5 制定新的体系框架形成合力共同应对网络威胁

2012年，印度总理办公室（PMO）、中央调查局（CBI）和其他政府部门频频遭受网络攻击。在此背景下，印度内政部着手制定了新的网络安全体系框架，明确相关部门的职责，共同应对网络空间对国家安全的新威胁。

该框架包括三大部分。一是印度政府将成立一个专职计算机法证（计算机犯罪证据的检验、搜集及保存）服务的国家研究中心。该中心将作为全国性的研究和培训中心，为执法机构提供计算机取证分析，还将参与培训各邦从事打击网络犯罪的警务人员。二是内政部提议在各邦设立网络犯罪警局（CCPS），牵头对网络犯罪进行专门调查[7]。三是

与印度软件服务业行业协会（NASSCOM）和印度数据安全委员会（DSCI）进行合作，为网络犯罪调查人员提供技术援助。

6 开发自有操作系统从技术上维护国家网络安全

印度国防发展与研究组织（DRDO）认为，目前印度互联网用户包括政府机构在内所使用的操作系统不是 Windows 就是 Linux，都来自国外。这些操作系统不仅很容易遭受攻击，自身也存在许多漏洞，从某种程度上可以说是网络威胁的技术根源。为此，2013 年 DRDO 做出了开发本国自有操作系统的决定。目前，DRDO 已在全国范围内召集 150 多名工程师，准备用三年时间完成整个操作系统的开发[8]。并且在开发过程中将严格遵循独立自主原则，不依靠任何来自国外的技术或人员帮助，真正打造一款印度人自己的操作系统，从技术上彻底维护印度网络安全。

7 加强网络监管提高民众网络安全意识

除了采用法律、制度、政策、技术手段外，印度政府还致力于通过加强监管，提高民众网络安全意识来积极应对网络安全。

（1）加强对网络运营商的监管。网站运营商须告知用户不得在网站发表有关煽动民族仇恨、威胁印度团结与公共秩序的内容。印度通信与信息技术部有权查封网站和删除内容。网站在接到政府通知后必须在 36 小时内删除不良内容。

（2）加强对网吧的监管。2008 年11 月 26 日，印度第一大城市孟买发生震惊世界的连环恐怖袭击事件。印度情报部门调查后发现，互联网成为恐怖分子日常沟通联络、发布指令的主要媒介，一些恐怖袭击策划活动竟然是在印度的网吧完成的。因此，印度政府规定，网吧经营者必须保留一年内客户访问的所有网站记录，并要求客户在上网前出示有效身份证件。网吧所有电脑还应配备安全过滤软件，防止客户访问色情、淫秽和恐怖主义等不良网站。

（3）加强对网络通信的监控。随着信息技术的发展，“Twitter”、“Facebook”等网络通信手段日益流行，成为人们相互沟通的新工具，极大地方便了人们的日常生活，但也带来一些负面影响。如一些不法分子就是通过“Twitter”和“Facebook”挑拨种族矛盾、煽动暴力冲突，导致2012 年 7 月印度阿萨姆邦发生了大规模种族冲突流血事件。为此，印度政府要求在印度开展网络通信业务的通信软件运营商提供拦截加密信息及解密办法，以便政府能够在必要的时候对相关通信方式实施监听或监视[4]。

（4）在加强网络监管的同时，印度政府也非常重视提高民众的网络安全意识。如印度信息技术部专门针对提高民众网络安全意识的“信息安全意识计划”，常年通过网络、报纸、电视等媒体，向民众普及网络安全知识，在全社会营造良好网络氛围。

8 结语

上述从六个方面大致浅析了印度维护网络安全的一些具体做法和有益经验。其中，既有战略高度的顶层设计、谋篇布局，如立法、发布新政、制定新的体系框架，也有技术层面的更新升级，如开发自有操作系统。既有政府层面的监管措施，也注重提高民众的网络意识。应该说这六个方面的举措从上到下，从宏观到微观形成了一个比较立体化的国家网络安全保护网，具有一定借鉴意义。■

参考资料：

[1] 张立 王学人. 印度网络安全策略探究. 南亚研究季刊, 2011 年第 4 期, 总第 147 期.

[2] Milind Deora. India Has More Than 238 Million Internet Users: Govt. Research.. The times of India, 2014-02-20(17)

[3] Shauvik Ghosh. Govt looks to beef up cyber security before Independence Day. Livemint, 2014-08-09.

[4] 王水平. 印度：用技术与法律手段应对网络犯罪. 光明日报, 2012–12–22.

[5] Moulishree Srivastava. India was among top 10 sources of spam in February: report. Livemint, 2014-03-24(06).

[6] Minstry of Communication & Information Technology, Government of India. National Cyber Security Policy-2013, MCIT, New Delhi, 2013-07-23.

[7] 顾舟峰 卢新月. 印度制定新网络安全体系框架. 人民邮电报，2012–06–06.

[8] 赵培培. 为确保网络安全印度决定开发自有操作系统. (2013-01-28)[2014-03-06]. http://security.zdnet.com.cn/security_zone/2013/0128/2142718.shtml.

How India Safeguard its National Cyber Security

LIU Xiang

（Guangzhou S&T and Innovation Committee, Guangzhou 510030）

Abstract: The author analyzed the new measures taken by the Indian government in safeguarding the national cyber security over the past few years. The Indian government has passed the new laws, issued new policies, formulated the new framework, and developed the new computer operating system to strengthen the cyber security supervision and the awareness of the Indian people on safeguarding the national cyber security. This research could be a reference to understand the situation of the cyber security in the world and safeguard the national cyber security of our country.

Key words: India；national security；cyber security

（上接第 33 页）

Study on the Cooperation Modes of Science and Technology Service between Guangdong and Hong Kong

SHANG Hui-min, LV Liang-wen

（Guangdong Institute of Scientific and Technical Information, Guangzhou 510033）

Abstract: In recent years, Guangdong and Hong Kong explored a variety of science and technology cooperation modes. Some cooperations are successful, while some face problems due to the effect of different economic development level and different social system in the two regions. This paper mainly studies the current situation of the regional cooperation in science and technology service and the future cooperation modes between them. It also gives some advices on promoting the service cooperation between Guangdong and Hong Kong.

Key words: Guangdong and Hong Kong；science and technology service；cooperation modes；countermeasure