加拿大网络安全战略评析*

□ 唐小松

[提　要] 信息时代,网络安全备受瞩目。加拿大政府出台了由确保联邦政府网络系统安全、加强各方合作保障联邦政府以外网络安全、维护公众网络安全三大支柱构成的网络安全战略,这既是维护国家社会公共安全、提升政府公信力和威望的需要,也是保障国内国际经济活动安全、促进经济发展、协同国际网络安全合作、提升自身国际地位的需要。当前,资金投入不足、政府部门执行力较弱、国际合作力度不够、自主性较差等问题制约了加拿大网络安全战略作用的发挥。

[关 键 词] 加拿大、网络安全

[作者简介] 唐小松,广东外语外贸大学教授

[中图分类号]TP393.08

[文献标识码] A

[文章编号] 0452 8832(2014)3 期 0092-13

网络方便和丰富了公众的工作和生活,人们对网络依赖的增强也使网络空间变得更脆弱,网络攻击与网络犯罪事件与日俱增。为了创造一个更加安全和谐的网络空间,2012 年 10 月,加拿大公共安全部发布了"加拿大网络安全战略:为建设一个更加繁荣强盛的加拿大",①该战略由三个支柱构成,概述了总体战略目标以及一系列行动计划,具有纲领性作用。2013

* 本文为广东外语外贸大学加拿大研究中心课题"加拿大中等强国外交与对外政策"研究成果的一部分。

① "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada," Public Safety Canada, 2010.

年,公共安全部发布了"加拿大网络安全战略 2010-2015 年行动计划",[①]列出了具体行动计划以及各项行动的相关主导部门,这在一定程度上推动了该战略的实施。

一、加拿大网络安全战略的构成

加拿大网络安全战略是其应对网络威胁的行动计划,由三个支柱构成:

(一)确保联邦政府网络系统安全

加拿大联邦政府各部门在网络安全中的角色和职责分工明确。[②]

公共安全部负责战略实施的总体协调,汇报网络安全战略实施情况,评估网络威胁并预警网络风险,增强公众网络安全意识,告知公众潜在威胁以及自我保护措施。具体职责包括推广和执行网络安全战略,建立并维护各部门间网络安全管理机制,开发用于评估的水平性能测量战略。其下属的加拿大网络事件反应中心是监控网络威胁并提出相关建议的关键部门,指导国家对网络安全事件的回应。

国库委员会秘书处通过制定政策、建立标准和评估手段,加强政府对网络事件的管理能力,并对政府信息技术安全负责。具体职责包括政府信息技术基础设施的更新、增强网络安全恢复能力、修订信息技术事件管理计划,以及通过各种政府安全团体项目、论坛和培训提高政府人员的网络安全意识。

国防部和军队致力于增强自身网络防护能力,与其它政府部门一道识别网络威胁并作出反应,与盟国军队共享网络实践信息,完善军队网络安全政策和法律框架。

---

① "Action Plan 2010-2015 for Canada's Cyber Security Strategy," Public Safety Canada, 2013.

② 以下有关加拿大网络安全战略内容的表述皆出自"加拿大网络安全战略"和"加拿大网络安全战略 2010-2015 年行动计划",具体参见"Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada"和"Action Plan 2010-2015 for Canada's Cyber Security Strategy"。

此外,通讯安全局、服务共享局和政府服务部也参与到确保政府网络系统安全行动中,并协助相关项目的实施。

为了提高联邦政府网络系统安全性,加拿大政府将在专门技术、系统和管理等方面持续投资,以适应不断变化的威胁,并计划在五年内额外投资 1.55 亿美元,加强联邦政府信息技术基础设施,提高对持续演进的网络威胁的侦查和回应能力。[①]政府还将加强其网络架构的安全,持续减少进入政府电脑系统的网关。另外,高科技产业的全球化使得对供应商可信度的评估变得困难,一些犯罪团伙利用国际供应链安全领域的差距,攻击网络漏洞。加拿大政府将加紧强化这方面的技术,降低网络攻击风险。

没有网络安全意识作为支撑,再复杂的安全系统也会十分脆弱。为此,政府部门通过举办论坛、开展培训等形式,强化全政府范围内工作人员的安全意识,促进政府网络系统的安全。

(二)保障联邦政府以外的网络安全

有效的网络安全不能仅靠一己之力,而是需要通过合作和信息共享,网络安全的总体态势才能得到提高,各地区、各省和联邦政府的组织之间也要通力合作增强应对网络事件的能力。[②]为此,在加拿大公共安全部领导下,政府成立了联邦各省各地区副部长委员会,正在实施信息共享草案;在司法部领导下,由联邦、各省和各地区协同经营的高级官员网络犯罪工作小组合作委员会从 2001 年开始启动;2013 年 8 月,加拿大政府又出台了指导性文件《加拿大网络事件管理框架》,覆盖了各省、各地区政府、重要基础设施部门和其它公私营部门合作者,用以补充和联结现有联邦、各省、各地区的紧急管理框架和计划,也包括重要基础设施部门的紧急计划。[③]

政府和私营部门共同承担网络安全风险。网络攻击者进入政府网站

① "Harper Government Invests in Cyber Security," Public Safety Canada, http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2012/20121017-eng.aspx.

② "Cyber Incident Management Framework for Canada," http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-eng.aspx.

③ *Ibid.*

盗取重要的工业信息会严重削弱加拿大工业的竞争力,进入私营部门网站获得重要情报,也会对加拿大的国家安全造成威胁,因而双方建立良好的合作关系有助于降低此类风险。加拿大公共与私营部门已建立了长期的合作,但还需进一步加强,要通过已有的结构和组织来培养,通过建立跨部门合作机制为公共和私营部门提供宽广的合作平台,对于潜在的和已显现的威胁分享精确的实时信息、防护技术和其他有效做法。加拿大大部分重要基础设施是由私营部门或省、市和地方政府所有的,[①]电力、电信、银行和交通等重要基础设施部门的程序控制系统影响重要基础设施的运作,其安全至关重要,联邦政府将与上述基础设施部门在维护网络安全上达成共识,共同应对网络威胁。

在加拿大网络安全战略中,也涉及了加强国际合作的内容,主要由加拿大外交与国际贸易部和公共安全部负责。加拿大外交与国际贸易部指派外交专员在位于日内瓦的联合国办公室处理网络安全问题,并负责制定网络安全对外政策,以及与一系列国际组织建立合作关系,共同应对网络安全问题。加拿大是签署欧洲委员会《网络犯罪公约》的非欧洲国家之一,政府正准备立法承认该公约。加拿大公共安全部注重加强与美国的合作,在超越边界的行动计划下与美国国土安全部共同制定并实施了《加拿大—美国网络安全行动计划》,旨在加强两国在网络事件管理和增强网络安全公共意识方面的合作,并联合私营部门分享网络安全信息。2012 年 10 月,前加拿大公共安全部部长维克·陶斯曾指出,"加拿大和美国在合作维护共享的基础设施方面有共同利益,我们共同致力于保护重要的网络系统,对任何网络破坏行为进行回击并加以恢复,携手为我们的公民创建更加安全的网络空间"。[②]

① "2012 Fall Report of the Auditor General of Canada, Chapter 3—Protecting Canadian Critical Infrastructure against Cyber Threats," http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html.

② "Canada and the U.S. Announce Cyber Security Action Plan," http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2012/20121026-1-eng.aspx.

(三)帮助公众维护网络安全

执法部门强化网络犯罪打击力度。现有调查权和调查工具已不能满足加拿大执法部门打击跨国网络犯罪的需要,加拿大皇家骑警成立网络犯罪联合中心分析网络犯罪趋势、网络安全态势,并负责起草加拿大网络犯罪战略,以解决欺诈、有组织犯罪和身份盗窃等网络犯罪行为;加拿大工业部负责立法改革,以更好地保护公众在网络空间的安全,目前已通过针对身份盗窃的立法,其他立法改革也将一一出台,通过"有法可依"来增强执法能力。

同时,执法部门注重提高公众网络安全意识。加拿大政府推出"网络安全意识月"活动,引导公众安全上网,并向其宣传保护措施。2013 年 10 月,加拿大公共安全部部长史蒂文·布莱尼在该活动开始时表示,"十月份的网络安全意识月提醒我们,可以采取一些简单的措施来保证上网的安全,我鼓励所有加拿大公众多花些时间来学习如何更好地保护自己和家庭"。[①] 2011 年,公共安全部曾制定了一套包括广告、合作伙伴、网络、社会媒体、议会参与、展览活动和内部沟通计划等方面的方案,用以宣传网络安全,该方案目前正在实施中。通过上述举措,加拿大政府旨在鼓励形成一种网络安全文化,

二、加拿大重视网络安全的原因

从加拿大政府的网络安全战略可以看出其对网络安全的重视程度,其原因主要有以下三点:

其一,维护国家社会公共安全,提升政府公信力和威望。

近年来,全球网络用户数量增长迅速,社交网络、云计算和移动互联方式的普遍使用,使信息交流途径发生了根本变化。人们在分享更多信息的

① "Minister Blaney Launches Cyber Security Awareness Month and Encourages Canadians to Get Cyber Safe," http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2013/20131001-eng.aspx.

同时,也将重要信息或个人信息委托给了无法掌控的第三方,[①]网络犯罪事件不断增加,安全隐患越来越多,造成的损失也越来越严重。网络安全对于一个国家的影响是全方位的,而首当其冲的是最基本的社会公共服务。

从政府层面来看,加拿大需要通过强化网络安全来提升政府服务和执政能力。保证政府网络系统的安全不仅仅是运作效率的问题,还关乎国家安全和主权,影响到保护驻外事务处、军队和执法人员的人身安全,关乎经济的完整性以及加拿大公众个人信息的安全。[②]一旦政府网络系统遭到攻击,政府的司法、税务、供水、供电、气象等方面的公共服务将无法进行,国家将陷入难以想象的混乱状态;政府网络系统含有大量重要信息,网络不法分子对其进行盗取,将使外交、情报等机构陷入危险甚至瘫痪的境地,公众也会因为个人信息外泄而面临人身和财产安全威胁,最终导致政府公信力下降,执政难以维持。美国的"监听门"事件引起各国普遍关注,加拿大也是美国的监听对象之一,这也给加拿大敲响警钟,更加重视网络安全和国家信息安全。

从个人层面来说,提升网络安全可以方便公众生活、提高国民生活服务质量,这是加拿大政府义不容辞的责任。2013 年一份调查显示,加拿大人平均每月花费在网络上的时间超过 41 个小时,观看视频的时间达 25 个小时,每人观看 291 个视频,均高居世界第二。[③] 2012 年,加拿大有 78%的家庭购买了高速上网服务,[④] 93%的人使用电子邮件进行沟通交流,72%的人使用电子银行支付账单、查看报表以及在账户之间转移资金,70.6%的民

① Ron Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," Canadian Defence & Foreign Affairs Institute, August, 2012.

② "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada," Public Safety Canada, 2010.

③ "2013 Canada Digital Future in Focus," http://theexchangenetwork.ca/upload/docs/Canada's%20Digital%20Future%20in%20Focus%202013.pdf.

④ "Communications Monitoring Report 2013," Canadian Radio-television and Telecommunications Commission, September 2013.

众通过网络了解新闻,54.2%的民众通过网络下载或观看电影,[①]由此可见,网络已与加拿大公众的日常生活息息相关,这更需要安全的网络环境作为保障。此外,加拿大崇尚自由交流、分享观点,这都需要通过开放的交流网络完成,但层出不穷的新交流方式也带来很多无法预见的安全隐患和隐私漏洞。例如,网络甚至能为恐怖分子提供资源,使其在防护自己的网站的同时向对方发起攻击。[②]

其二,保障国内国际经济活动安全,促进经济发展。

重视网络安全对加拿大经济安全具有重要意义。在国内经济活动中,越来越多的商业活动通过网络完成。2012 年,加拿大公司通过网络实现商品和服务交易额达近 1220 亿美元,是 2007 年的两倍,其中制造业、批发贸易和零售贸易的销售占比超过 61%,[③]电子商务零售业营业额则达到 223 亿美元,同比增长超过 10%。[④]加拿大互联网经济发展之迅猛、对网络依赖程度之高可见一斑,这对互联网环境的安全提出了更高要求,任何网络安全事件都将对加拿大电子商务业造成巨大影响,进而影响其经济安全。在国际经济活动方面,作为高度依赖国际市场的国家,加拿大在能源、贸易、金融领域与美国和亚洲联系密切,而网络是其联系的纽带。[⑤]加拿大需要一个安全的网络环境,保障各项交流谈判及国际贸易的顺利实施,进而开拓更广阔的国际市场。

然而,恶意软件对网络安全造成的影响日益引起人们的关注。仅在 2010 年,加拿大反诈骗中心就收到了来自 18146 位受害者的身份欺诈报

---

① "Canadian Internet Use Survey, Internet Use, by Age Group, Internet Activity, Sex, Level of Education and Household Income," Statistics Canada, http://www5.statcan.gc.ca/cansim/a26? lang=eng&retrLang=eng&id=3580153&tabMode=dataTable&srchLan=-1&p1=-1&p2=9.

② "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada," Public Safety Canada, 2010.

③ "Digital Technology and Internet Use, 2012," Statistic Canada, June 12, 2013.

④ "2013 Canada Digital Future in Focus," http://theexchangenetwork.ca/upload/docs/Canada's%20Digital%20Future%20in%20Focus%202013.pdf.

⑤ Ron Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," Canadian Defence & Foreign Affairs Institute, August, 2012.

告,总损失超过940万美元,其中以支付卡欺诈最为常见,据估计,还有很多身份盗窃与欺诈案件并未向警方报告。①一份英国国际网络安全保护联盟的调查显示,69%的加拿大商业公司受到过不同形式的网络攻击,②表明网络安全漏洞已经给加拿大民众的人身和财产安全以及商业信息安全造成威胁,严重影响到加拿大经济运行秩序、破坏了经济的良性发展,这也是加拿大重视网络安全的一个重要因素。

其三,协同国际网络安全合作,提升自身国际地位。

各国互联网彼此相连,同时又分属不同主权范围,这决定了加强国际交流与合作的必要性。③国际互联网的突出特点在于相互贯通、快捷方便,同时又难以有效监管和追踪,任何一国都无法在网络空间中独善其身,或独自应对各种挑战。④网络病毒通过互联网传播的速度快,且很多传播源都来自国外,要彻底清除病毒就要各国之间协调合作。对于同一恶意代码或漏洞,一个国家或国际组织在找出应对方案后,彼此分享就能更快解决网络安全问题,节约网络安全防护成本。美国、英国和澳大利亚是加拿大三个最密切的安全和情报伙伴,这些国家分别于2011年、2009年和2011年发布了各自的网络安全战略,欧盟则于2013年发布了网络安全战略,八国集团(G8)各国也一致认为,需要加强合作来确保信息基础设施,包括计算机网络和交流系统的安全。⑤这表明了国际社会对网络安全重要性的认识更加深入,加拿大也有必要出台自己的网络安全战略,进一步开展与相关国家的合作,展现负责任的国家形象,提升国际地位与影响力。

---

① "National Identity Crime Strategy," http://www.rcmp-grc.gc.ca/pubs/cc-dc/strat/ei-ie-eng.htm.

② "Nearly 70% of Canadian Business Hit by Cyber Attacks, Says Year-Long Surver," http://www.ctvnews.ca/sci-tech/nearly-70-of-canadian-businesses-hit-by-cyber-attacks-says-year-long-survey-1.1272687.

③ 中华人民共和国国务院新闻办公室:"中国互联网状况",2010年6月8日,http://www.gov.cn/zwgk/2010-06/08/content_1622866.htm。

④ 袁征:"中美关系中的网络安全问题",《和平与发展》,2013年第4期,第17页。

⑤ "Still the Fire-Proof House? An Analysis of Canada's Cyber Security Strategy," http://www.academia.edu/1534361/Still_the_fire_proof_house_An_analysis_of_Canadas_Cyber_Security_Strategy.

加拿大和美国共享了很多重要基础设施,网络安全对这些基础设施及系统造成的破坏,将直接影响美加双方边境民众的生活和商业往来。[①]在此背景下,双方迫切需要就网络安全开展合作,《加拿大—美国网络安全行动计划》便是成果之一。美国的网络安全战略早在克林顿政府时期就已萌芽,经过小布什政府和奥巴马政府的进一步发展,网络安全已成为美国国家安全的重要组成部分。美国凭借其在互联网技术上的压倒性优势,试图主导网络空间秩序,巩固霸权地位。而作为美国的近邻和盟国,加拿大对该政策的追随不足为奇,其在国际网络安全领域获得更大话语权的期待,使其日渐加大对网络空间的投入。在 2010 年的里斯本峰会上,北约需要加强的作战能力是讨论的重点内容,而在新能力的排行中,"网络防御"赫然排在前列。网络军事化已成事实,网络战是未来战争的方向,自身网络防护能力的提升是掌握网络战主动权的根本保障,北约相当一部分成员国都制定了网络安全计划,加拿大作为成员国之一,推出本国网络安全战略,以期与各盟国合作建设坚实的网络防护体系。

三、加拿大网络安全战略评估及其对中国的启示

加拿大网络安全战略的发布,使其在预防和应对网络威胁方面有了指导性方针政策,能够更有针对性、有重点地开展工作。该战略强调政府部门间的协作,注重宣传,突出全民参与,有利于网络安全环境的建设。但值得注意的是,加拿大网络安全战略本身及实施过程中还存在诸多问题。

第一,资金投入不足,人力物力保障难以跟上发展需要。加拿大在网络安全方面的投入与其他国家相比少得可怜,2010 年,政府计划在 5 年内投资 9000 万美元来应对网络攻击,2012 年又增补 1.55 亿美元。2011 年,英国政府推出总额 6.5 亿英镑(超过 10 亿美元)的"网络安全战略"(Cyber

① "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada," Public Safety Canada, 2010.

Security Strategy),用4年时间提升该国的网络安全水平。美国2012年网络安全风险投资总额达14亿美元,世界前20大网络安全公司美国独占15家。[①]另据加拿大审计署的一份调查显示,尽管15年来有10亿美元的资金用于加拿大网络安全保护,但究竟有多少落实到位并不明晰。加拿大审计总长表示,有5.7亿美元的资金进入了加拿大通讯安全局,该局是负责保护重要政府系统免受网络威胁的高度机密机构,但这些资金用于很多项目。[②]没有足够的资金支持,加拿大网络技术设备的更新跟不上发展的需要,也难以支持专家对网络安全防护措施展开更深入的研究。加拿大公共安全部的官员也认识到,设备陈旧化、应急措施缺乏、难以招募和留住网络专家等困难正威胁着政府应对网络攻击的能力。[③]面对层出不穷的网络攻击工具和技术,加拿大政府已意识到网络威胁环境的演进超过了政府应对能力的提升。[④]联邦政府表示,网络威胁的频率和严重程度在不断增加,保护加拿大网络安全将成为一项持续的挑战。

第二,各部门执行力度不够,效率低下,网络安全信息通道传递不畅,应对网络攻击捉襟见肘。尽管加拿大网络安全战略2010—2015年行动计划明确了各政府部门的职责范围,但各部门的执行并未达到预期效果。加拿大网络事件反应中心成立7年以来,其角色和职责仍不为外界清晰认知,加上其每天只运作15小时、每周仅运作5天,难以对网络威胁进行充分监控,阻碍了该中心及时为应对新的网络威胁提供建议的能力。[⑤]其他部

① 袁沈钢:"中美网络安全产业对比及启示",2013年9月30日,http://news.sciencenet.cn/sbhtmlnews/2013/9/278425.shtm。

② "2012 Fall Report of the Auditor General of Canada, Chapter 3—Protecting Canadian Critical Infrastructure against Cyber Threats," http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html.

③ "Canada Has Poor Security against Cyber Attacks, Documents Warn," http://www.thestar.com/news/canada/2012/06/07/canada_has_poor_security_against_cyber_attacks_documents_warn.html.

④ "2012 Fall Report of the Auditor General of Canada, Chapter 3—Protecting Canadian Critical Infrastructure against Cyber Threats," http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html.

⑤ *Ibid.*

门更是应付了事,负有保护政府信息系统责任的通讯安全局未能为网络安全反应中心提供及时信息。[①]据统计,加拿大负责网络安全的政府部门至少有 13 个,但其相互传递和分享信息都成为难题,更不用说展开协调合作了。除了内部协调不力,政府部门与私营部门的信息分享也不尽如人意,相关组织和企业未能在第一时间收到网络威胁信息,因而难以及时采取应对措施。同时,由于私营部门对政府网络安全组织机构不甚了解,遇到网络威胁时也就难以及时将信息上传到对应部门,限制了政府部门作用的发挥。此外,政府部门与私营部门的合作不够均衡,在对重要基础设施部门加大关注的同时,忽视了金融业等领域,在分享信息时也有诸多障碍。

第三,国际合作力度不够,实施网络安全的自主性较差。加拿大网络安全战略绝大部分都是在关注对内政策,较少涉及国际事务。[②]该战略提到网络空间具有全球性,也认为网络安全需要对外政策支持,但是未能列出具体做法,对加强国际合作认识缺乏深度也不够全面。主要负责对外事务的加拿大外交与国际贸易部,并未被赋予网络安全方面较大权力,所承担的责任也很小,严重限制了它利用丰富的外交资源进行国际合作的能力。开展国际合作的广度过于集中在与美国、西欧等发达国家的合作上,仅有一处提到"在可能的情况下帮助不发达国家提升网络安全保障能力",但并未说明包括哪些国家以及具体的实施细节。事实上,加拿大有必要与亚洲、南美等新兴经济体国家合作共同保障网络安全,强化全球网络安全的薄弱环节,创造一个更加全面的国际网络安全合作框架,开展更为广泛的网络外交活动。该战略对美国的跟随与配合,严重限制了加拿大网络安全战略的自主性。为了配合美国的网络安全行动,保护共有重要基础设施,倡导所谓的"网络自由"、在网络军备竞赛中占领制高点,加拿大很难根据自身实际情况来制定战略,而是陷入美国的控制。在美国"监听门"中,众

① "Critical Cyber Security Gaps remain, Auditor General Says," http://www.cbc.ca/news/politics/critical-cybersecurity-gaps-remain-auditor-general-says-1.1173615.

② Ron Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," Canadian Defence & Foreign Affairs Institute, August 2012.

多国家表达了愤怒,欧洲国家领导人也在2013年10月的布鲁塞尔峰会上予以猛烈抨击,但加拿大却选择听之任之。这种不对称关系,势必会严重影响到加拿大的网络安全,网络安全战略的执行效果也将大打折扣。

第四,重安全防御,轻主动出击。纵观加拿大网络安全战略,全盘重视战略防御,其焦点在于巩固自身的网络安全体系以及网络威胁出现并造成一定损失之后的应对策略,鲜有涉及主动出击方略。网络空间的自由和快速传播特质给犯罪分子实施盗窃和攻击提供便利,但也为网络安全的维护带来契机,各部门利用网络收集相关情报,了解犯罪动机、周期,破解犯罪手法,实施主动出击,一举捣毁其整个网络系统,是网络安全攻防的应有策略。先发制人、主动出击,对于扼制网络恐怖主义不失为一种良策,可以从源头解除恐怖威胁。但加拿大网络安全战略似乎只主张被动防御,没有展示主动出击的意图。这与加拿大中等强国的定位有关,也与其长期以来形成的将安全防卫寄托于美英等盟国的惯性不无关系。

加拿大网络安全战略对中国网络安全建设有着重要的借鉴意义。中国共产党第十八届三中全会指出,"要改进社会治理方式,激发社会组织活力,创新有效预防和化解社会矛盾体制,健全公共安全体系。设立国家安全委员会,完善国家安全体制和国家安全战略,确保国家安全"。[①]这说明,中国已充分认识到公共安全的重要性,而具体到公共安全的重要组成部分——网络安全,并未明确说明,目前也没有得到足够重视。当今社会已全面网络化,开始迈入大数据时代,加强网络安全十分迫切,势在必行。

首先,当务之急是要加快制定中国的网络安全战略,形成网络安全建设的纲领性文件,以有效指导网络安全的具体维护实施。网络安全战略既要全面,包括明晰的战略目标、权责明确的组织结构等,又要有具体实施步骤,每一步都落实到具体部门,部门之间要有分工合作和信息共享等,还要有加强国际合作的内容,特别是与周边国家以及西方发达国家的合作,分

① "中共中央十八届三中全会公报发布(全文)",2013年11月12日,http://finance.sina.com.cn/china/20131112/194917300619.shtml。

享经验、联合打击。

其次,制定网络安全相关法律法规。目前我国网络规模大、网民数量多,电子商务发展迅猛,2013 年仅"双十一"一天淘宝总交易额达 350.19 亿元人民币。随之而来的网络攻击上升、网站数据篡改量增多、网络系统复杂性及脆弱性增加等问题,都使网络变得更加不安全。为此,应制定权责明晰、结构严密、体系完备、功能健全的网络安全法律规范体系,形成统一高效权威的网络安全法律保护屏障。①

最后,应采取积极、透明、合作的方式,有效回应国际社会关于中国对其他国家进行网络攻击活动的质疑。针对美国、英国和加拿大等西方国家指责中国政府支持网络黑客攻击,特别是美国声称与中国军方有关的黑客多次攻击其网站等毫无根据的责难,中国政府一方面应制定并完善自己的网络安全防护计划,创建更加公开透明安全的网络环境,以积极正面的方式向世界证明中国在和平利用网络空间服务自身经济、社会建设;另一方面应加强与西方网络强国的交流合作,既可借鉴其先进经验、分享网络防御实践、共同完善网络空间国际规则,又可让他国更加了解自身的网络安全政策和实践,以开放、包容促进相互谅解、消除疑虑,实现多赢。

【完稿日期:2014-2-15】
【责任编辑:李 静】

① 徐汉明:"加强网络安全立法研究 完善网络安全法律体系",《法制日报》,2013 年 7 月 25 日,第 11 版。