奥巴马政府网络空间战略面临的挑战及其调整

鲁传颖

[内容提要]奥巴马政府将网络空间政策提高到战略高度,试图打造一个集战略思想、政策举措和行动策略三位一体的网络空间战略。但在实践中,奥巴马政府构建了一个复杂而矛盾的体系,战略思想有内在矛盾,政策效力之间相互抵消,"棱镜门事件"更使得美国网络空间战略陷入困境。随后,奥巴马政府着手调整,一方面对进攻性的网络政策进行全面审查,另一方面放弃对 ICANN 的控制权,推进网络空间全球治理进程。这将会对国际网络空间的"建章立制"产生重大影响。

[关键词]美国网络战略　网络空间治理　棱镜门　多利益攸关方

[作者介绍]鲁传颖,上海国际问题研究院助理研究员,主要从事网络空间治理和网络安全研究。

2014 年 3 月 14 日,美国商务部下属的国家电信和信息管理局(NTIA)宣布将放弃对"互联网名称与数字地址分配机构"(ICANN)的控制权,并在移交声明中指出,将由 ICANN 管理层组织全球"多利益攸关方"(Multi-stakeholder)讨论接收问题,但明确拒绝由联合国或其他政府间组织接管。① 鉴于 ICANN 在国际互联网管理中的战略地位及其特殊的移交方案设计,美国此举的深层含义表明,奥巴马政府正着手对网络空间战略进行重新调整布局。本文首先对奥巴马政府的网络空间战略进行梳理,对"棱镜事件"后其面临的挑战进行分析,并在此基础上探讨美国网络空间战略的调整及其对国际网络空间治理的影响。

一、奥巴马政府的网络空间战略

美国政府历来重视网络空间战略。早在克林顿时期,美就通过实施《国家信息基础设施:行动计划》(NII)建立"信息高速公路",发展网络经济战略。"9·11"后,小布什政府将网络战略重点转向网络安全,并先后于 2003 年和 2008 年出台了《确保网络空间安全国家战略》和《综合国家网络安全倡议》(CNCI)两份重要文件,强调发展保卫国家网络安全的能力。② 奥巴马政府则将网络空间战略列为重中之重,试图构建一个包含网络安全、网络经济、网络监控、网络自由等在内的全方位战略,主导国际网络空间的权力、资源和财富分配。在美国国务院、国防部、情报部门、国土安全部等各部门的积极配合下,奥巴马政府集战略思想、政策举措和行动策略三位一体的网络空间战略逐渐浮出水面。

奥巴马政府分别于 2009 年和 2011 年发布《网络空间政策评估》和《网络空间国际战略》两份政策报告,对外公布美国在网络空间的战略思想和战略目标。③ 2012 年 12 月,奥巴马总统签署绝密的《第 20 号总统政策指令:美国网络行动政策》,详细规定了美国在网络空间采取进攻性和防御性政策的原则、目标和方案;明确美国在网络空间的利益包括国家安全、公共安全、国家经济安全、"关键基础设施"的安全可靠运行、"关键资源"的控制权等;详细制

① The NTIA, "NTIA Announces Intent to Transition Key Internet Domain Name Functions", http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions. (上网时间:2014 年 4 月 19 日)

② 沈逸:《美国国家网络安全战略》,时事出版社,2013 年,第 153-163 页。

③ 刘兴华:"奥巴马政府对外网络干涉政策评析",《现代国际关系》,2013 年,第 12 期,第 53-55 页。

定了“进攻性网络效应行动”(OCEO)和“防御性网络效应行动”(DCEO)两个行动方案,规定在必要时可以对他国网络空间的数据、信息以及关键基础设施采取控制、运行中断、拒绝执行指令、性能降级、甚至完全破坏。[①]《第 20 号总统政策指令》暴露了美国在网络空间建立霸权的实质,并对美国整个网络政策体系导向产生了重要影响。

在白宫战略思想的指引下,美国国务院、国防部、情报部门、国土安全部等各部门纷纷提出各自的网络空间政策规划。美国国务院作为《网络空间国际战略》主要执行部门,积极推动在网络空间的价值观外交,强化盟友之间的价值观同盟,并通过在网络空间“建章立制”,试图建立起一套符合美国利益的网络空间规则;[②]国防部发布了《网络空间行动战略》,宣布成立网络司令部,加速发展网络部队,[③]并通过网络军演、军事交流等方式加强盟友之间在网络战领域的合作;国家安全局(NSA)、中央情报局(CIA)等情报部门加大了网络情报搜集力度和广度,并且将大数据技术引入网络情报分析,为美国政府提供大量有价值的情报,一举成为美国网络空间战略的核心部门。除此之外,各部门之间还开展了一系列协调与合作,如国防部与国土安全部签订“2010 协议备忘录”,增加在政策法规、任务成效和预算等三方面的合作;国土安全部、司法部、国家安全局等部门通过加强协作,制定网络安全框架、指南和程序维护美国关键基础设施的网络安全。[④]

美国政府网络空间政策主要通过国际和国内两个行动策略来实施。在国际层面,美国主要是推行一种“去政府化”的网络空间治理模式,一方面从理论上把网络空间描述为“全球公域”,否认网络主权;另一方面推行“多利益攸关方”治理模式,以企业、非政府组织、公民社会为网络空间治理主体,限制国家及政府间组织在网络空间治理中发挥作用。美国之所以采取如此策略,是因为其垄断负责互联网运营的国际机构和企业,[⑤]如负责互联网 IP 地址分配、域名注册和域名解析服务的 ICANN 和负责网络协议和标准制定的 IETF 等都位于美国,[⑥]美国 IT 企业则基本上垄断了全球市场的网络设备、操作系统、数据库、搜索引擎、社交网络、云计算等领域。因此,无论是强调网络空间的“全球公域”属性还是“多利益攸关方”治理模式,无非都是借此抹杀他国网络主权,给美国创造在网络空间“全球介入”(Global Access)的能力。此外,为进一步抢占网络空间治理领域的话语权,美国务院牵头搭建名为“伦敦进程”(London Agenda)的网络空间治理平台,向其他国家兜售美国的思想和价值观;国防部也通过开展网络军演,打造网络军事盟友体系;情报部门则通过“五只眼”国际情报联盟、北约情报共享机制、盟友间情报共享机制等各个层级的网络情报分享行动,建立以美国为核心的国际情报体系。

在国内层面,奥巴马政府积极推动公-私(Public-Private)合作。美国的网络资源大多分布在政府之外的企业、非政府组织和社会当中,推动公-私合作是为了整合这些资源并将其转化为美国的网络权力。2013 年 2 月奥巴马总统签署《关于提高关键基础设施网络安全的行政命令》,授权相关政府部门制定安全标准和实施指南,通过监督、协商、合作等手段加强对关键基础设施所有者和运营商的安全检查,让其参与政府制定和执行标准的决策,促使其主动与政府分享机密信息。[⑦] 奥巴马政府还积极推动对于美国具有战略意义的网络技术发展,如大数据和云计算技术。大数据通过对海量数据的挖掘和整合,可以掌握原先只有政府才能掌握的有关政治、经济、社会敏感信息。掌握了先进的大数据技术,即意味着可以轻易突破其他国家的数据主权。对此,奥

① The White House, “Presidential Policy Directive 20”, http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf. (上网时间:2014 年 4 月 19 日)

② Margaret P. Karns & Karen A. Mingst, *International Organizations, The Politics and Process of Global Governance*, Lynne Rienner Publishers, 2010, pp. 258-262.

③ US Department of Defense, “DOD Strategy for Operating in Cyberspace”, http://www.defense.gov/news/d20110714cyber.pdf. (上网时间:2014 年 4 月 19 日)

④ The White House, “Executive Order - Improving Critical Infrastructure Cybersecurity”, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. (上网时间:2014 年 4 月 8 日)

⑤ NazliChoucri, *Cyberpolitics in International Relations*, London: MIT Press, 2012, pp. 208-216.

⑥ 中国现代国际关系研究院:《国际战略与安全形势评估(2012-2013)》,时事出版社,2013 年,第 120 页。

⑦ Larry Clinton, “A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense”, *Journal of Strategic Security*, Issue 2, 2011, pp. 104-106.

巴马政府特别责成白宫科技政策委员会成立大数据高层指导小组，要求联邦政府各个部门积极支持“大数据研发计划”。① 美国政府不仅在每年庞大的 IT 采购预算中优先采购云计算服务，还建立联邦云计算示范工程，并通过一揽子计划鼓励亚马逊、谷歌、微软、IBM 等企业在全球获得领先地位，②把美国打造成全球数据的存储、交换中心。这样一来，美国政府无需进入他国即可获得网络数据的“全球介入”能力。

综而言之，奥巴马政府的网络空间战略具有三大特点。一是全局性和战略性。奥巴马政府将网络空间视为权力、财富、资源不断聚集的，与陆、海、空、天同等重要的第五战略空间，并将网络空间“建章立制”视为与二战后建立美国主导下的国际秩序同等重要。二是继承性和延续性。在小布什政府后期，美国已经开始探索在网络空间建立霸权，具有标志性意义的“奥林匹克计划”和“棱镜计划”正是这一时期开始执行，奥巴马上台后延续了上述项目并加大投入。此外，小布什政府在任期结束之前，曾委托分别来自民主党和共和党的两位众议员引领美国战略与国际问题研究中心（CSIS）制订《致第 44 届总统网络安全报告》。该报告建议在小布什时期网络安全战略基础之上建立一个包括外交、情报、军事、经济的综合性网络安全战略。③ 奥巴马对此照单全收，其后来发布的多项网络空间战略都源自该报告的思想。三是控制性和进攻性。因受“9·11”影响，小布什时期的网络空间战略主要强调发展保卫网络安全能力，特别是防范网络恐怖分子对美国关键基础设施的攻击。奥巴马时期的网络空间战略则更强调控制性和进攻性，无论是积极发展网络军事力量，开展网络监控，还是推动网络空间的“建章立制”，都是采取进攻性手段实行对网络空间权力、资源、财富的控制。

二、奥巴马政府网络空间战略面临的挑战

奥巴马政府的网络空间战略是一个复杂而矛盾的体系，体现在：战略思想存在内在矛盾，既要维护网络空间开放、透明、可操作性，又要建立美国的网络霸权；协调机制不畅，导致国务院、国防部、国土安全部及情报部门的政策相互抵触；国际和国内层面的行动策略彼此冲突。“棱镜门”事件更加速了矛盾的爆发，暴露出奥巴马政府过度推进进攻性网络政策、开展网络监控、干涉他国主权和垄断互联网管理权，把网络空间推向政治化、意识形态化和军事化的困境。

由于各种因素影响，美国的网络空间战略面临国际和国内多重挑战。首先，在国际上陷入信任危机。美国一直把建立国际网络空间的“行为规范”标榜为其网络空间国际战略的主要目标之一。“规范”（Norms）一词在《韦氏新国际英语词典》中的多项解释暗含着“正确的”、“正面的”、“广为认可”等褒义。言下之意，美国要树立网络空间行为准则的典范，并对其他国家不符合规范的行为进行约束和惩罚。自 2013 年 6 月起，美国国家安全局前雇员爱德华·斯诺登持续不断向媒体披露“棱镜计划”的具体细节，揭露美国政府窃取联合国秘书长潘基文的文件、对巴西总统罗塞夫的私人手机、德国总理默克尔的办公室，甚至到访的中国前国家领导人的通讯进行监听。④ 虽然奥巴马辩称，情报收集是每个国家的正常工作，“棱镜计划”主要针对网络犯罪和网络恐怖主义等特定对象，但正如《纽约时报》所指出的，提前窃取潘基文与奥巴马会晤中的谈话要点，监听默克尔的私人通话等既与防止网络犯罪无关，也与打击网络恐怖主义无关。⑤ 美国在网络空间的行为与自己所标榜的“行为规范”相去甚远，在国际上广受指责；盟友之间在网络政策上的协调被中断，默克尔总理不仅要求彻底审查美国在欧洲的监控行

① The White House, “Big Data Initiative”, http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf.（上网时间：2014 年 4 月 19 日）

② The White House, “Federal Cloud Computing Strategy”, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/vivek-kundra-federal-cloud-computing-strategy-02142011.pdf.（上网时间：2014 年 4 月 19 日）

③ James A. Lewis, *Securing Cyberspace for the 44th Presidency*, December 2008, p. 1, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.（上网时间：2014 年 3 月 20 日）

④ “Prism”, *The Guardian*, June 11, 2013, http://www.theguardian.com/world/prism.（上网时间：2014 年 4 月 19 日）

⑤ “Obama Weighing Security and Privacy in Deciding on Spy Program Limits”, *The New York Times*, December 20, 2013.

动,甚至提议建立欧洲自己的互联网。[①] 在罗塞夫总统的提议下,2014 年 4 月在巴西召开全球互联网峰会,打算讨论美国"棱镜计划"对网络空间秩序的负面影响。虽然在美国政府的强烈要求下最终取消了相关议题,但在会场上下依旧有很多参会者就"棱镜计划"对美国政府提出了强烈批评。[②]

其次,国内基础分化。美国政府一直采取诸多策略寻求国内对于网络空间战略的支持,如在网络空间推广美式价值观以迎合国会和民众;在网络安全问题上高调批评中国,以外部威胁为由迫使企业和民众支持政府的网络战略;在网络安全防范等领域推动公-私合作,将非政府组织、企业、社会纳入政府的网络政策框架内等。"棱镜门"事件消解了美国政府在推动国会、非政府组织、企业、公民社会在网络战略上形成共识的努力,斯诺登揭露了一个包括"棱镜"、"X 关键分"(X-Keyscore)、"美景"(Fairview)、"核心"(Main core)等近 10 个监控项目在内的监控体系。[③] 该监控体系由国家安全局、中央情报局、联邦调查局等多个情报机构参与,几乎覆盖了网络空间的社交网络、邮件、即时通讯、网页、影片、照片等所有信息。美国政府不仅要求微软、谷歌、脸谱等 9 家主要全球互联网企业向监控项目开放数据库,甚至在所有经过美国境内的洲际光纤上拦截数据。"棱镜计划"破坏了法律对民众隐私的保护,激起了国会、企业和全社会对美国政府的声讨。在参议员艾尔·弗兰肯的提议下,参议院司法委员会向国会提交了《监听透明法 2013》(Surveillance Transparency Act of 2013),要求对《爱国者法》第 214、215 条款进行修改,限制情报机构对互联网和电话元数据的收集;对《外国情报收集法》(Foreign Intelligence Surveillance Act)第 702 条款进行修改,重新审查"棱镜"项目对互联网信息的收集。[④] 参议院情报委员会主席范斯坦对中央情报局监控国会议员电脑大为光火,态度强硬地指责其涉嫌违反宪法、破坏三权分立原则。为了挽回"棱镜门"给企业声誉造成的负面影响,涉及监控项目的企业纷纷与政府划清界限。苹果、微软、雅虎等 8 家全球著名的互联网企业发表公开信,要求政府改革监控体系。[⑤] 微软和谷歌甚至向法院诉讼联邦政府。美国民众对于政府打着反恐旗号开展无孔不入的监控表示不满。据媒体报道,有 85% 的民众反对政府监听项目,并有超过一半的民众视斯诺登为英雄。美国公民社会联盟在网上发起"停止监视我们"(Stop Watch Us)行动,向美国政府施加压力,得到数以万计网民在网站上的签名、留言,以及数百个公民团体的响应,他们通过组织游行示威、向国会请愿、发起网络倡议等方式配合该行动。[⑥]

第三,网络空间分裂风险加大。美国强行推广"互联网自由"战略,把广大发展中国家推向对立面,使当前网络空间面临着巨大的分裂风险。美国务院是推进美国网络空间国际战略的主要部门,在希拉里国务卿主政时期,曾多次就"互联网自由"发表演讲。美国政府将"互联网自由"定义为"包括网络空间保护个人自由表达其观点的权利、向领导人请愿的权利、基于信仰进行礼拜的权利"。围绕"互联网自由"这一新概念,美国务院采取了一系列政策举措。一是在价值观引导下,形成国际、国内网络价值观同盟,排斥他国的网络价值观。二是通过强调互联网信息的自由流通,反对其他国家的互联网公共政策,阻止他国在网络空间行使主权,进而把美国的权力和利益拓展到他国网络空间。在伊朗、突尼斯、埃及、叙利亚等中东国家的政治动荡中,美国的推特、脸谱、优兔等社交网络媒体发挥了重要作用,是当地反政府势力号召、组织、宣传推翻政府活动的主要平台。美国政府借所谓"互联网自由",力

① "Angela Merkel Rebukes US and Britain over NSA Surveillance", *Telegraph*, http://www.telegraph.co.uk/news/worldnews/europe/germany/10604664/Angela-Merkel-rebukes-US-and-Britain-over-NSA-surveillance.html. (上网时间:2014 年 4 月 19 日)

② Veridiana Alimonti, "Privacy and Surveillance", http://content.netmundial.br/contribution/privacy-and-surveillance/273. (上网时间:2014 年 5 月 7 日)

③ "List of Government Mass Surveillance Projects", April 1, 2014, *Wikipedia*, http://en.wikipedia.org/w/index.php?title=List_of_government_mass_surveillance_projects&oldid=602236932. (上网时间:2014 年 4 月 19 日)

④ "Surveillance Transparency Act of 2013", S. 1452, 113th Congress (2013).

⑤ "Apple, Facebook, Google Call for Government Surveillance Reform", *Los Angeles Times*, http://www.latimes.com/business/technology/la-fi-tn-apple-facebook-google-call-for-government-surveillance-reform-20131209,0,1482369.story#ixzz2zLRIpKQV. (上网时间:2014 年 4 月 19 日)

⑥ "Stop Watching Us", https://optin.stopwatching.us/. (上网时间:2014 年 4 月 19 日)

挺西方通讯服务商拒绝所在国政府关闭网站的要求，还鼓动开放注册波斯语、阿拉伯语账号为反对派推波助澜，树立在社交网络积极支持反对派的形象。三是以“互联网自由”为借口，要求其他国家向美国企业开放市场，把美国的互联网企业推向全球。美国通过给对美国企业造成竞争压力的他国企业贴上违反“互联网自由”标签，在道德上进行抹黑从而影响国际市场对其产品的采用。美国的“互联网自由”政策引起越来越多国家的反对，在 2012 年迪拜国际电信联盟大会上，共有 89 个信息发展中国家提出要将“成员国拥有接入国际电信业务的权力和国家对于信息内容的管理权”写入《国际电信规则》，落实信息社会世界峰会（World Summit on the Information Society）突尼斯议程中提出的“互联网政策是一国主权”的共识，并不顾美国的强烈抵制强制表决通过了决议。虽然因最终投票的国家没有达到法定数量导致该条款无法生效，但发展中国家依旧借此向美国展示了强硬立场。此外，发展中国家为了抵制美国的“互联网自由”战略，必将出台更多互联网管理措施，以牺牲网络空间的开放性、透明性来维护网络主权，从而进一步加剧网络空间分裂的风险。网络空间的统一、开放、透明、可操作是美国网络国际战略的前提，也是网络空间的价值所在，一个分裂的网络空间显然不利于奥巴马政府推行其网络空间战略。

第四，网络安全形势恶化。奥巴马政府大肆渲染美国面临的网络安全威胁，投入大量人力、物力发展网络军事力量，把网络空间推向了军事化。[①] 2009 年 6 月，美国成立网络司令部，并开始组建网络作战部队。不仅如此，美国还将网络战运用到实践中，通过震网病毒（Stuxnet）破坏伊朗的核设施；秘密开发火焰病毒（Flame），在全球感染难以计数的计算机，搜集他国的军事情报。美国的进攻性网络军事政策打开了网络战的“潘多拉魔盒”。[②] 表面上，美国希望通过威慑方式增加网络安全，却加剧了网络空间的军事化，反而恶化了美国的网络安全形势。一是在美国大力发展网络军事力量的刺激下，各国纷纷成立网络部队，加大了研发网络武器的力度，以挑战美国在网络军事方面的优势，迫使奥巴马政府不断加大在网络军事领域的投资，从而陷入网络军备竞赛的恶性循环之中。二是在缺乏有效网络军控机制下，网络武器开始泛滥并逐步向非国家行为体扩散。网络武器只是一些复杂代码所构成的病毒程序，可以轻易地通过便携式存储设备复制、转移，恐怖分子获得网络武器的机会将由此大大上升，而美国是网络恐怖主义主要攻击目标之一。三是由于网络空间的匿名性，在“归因”（即科学地寻找发起攻击的源头）方面难以做到客观、公正，各种误判将会引起国家间的网络军事冲突，并将影响到整体网络安全。网络空间的互联性使得美国的高网络依存度成为其在安全领域的“阿喀琉斯之踵”。[③]

三、奥巴马政府对网络空间战略的调整

面对诸多挑战，奥巴马政府不仅重新审查了“棱镜计划”，更重要的是对整个网络空间战略的战略思想、政策举措和行动策略进行了调整，旨在构建一个更加均衡的网络空间战略，包括战略目标上调整网络空间治理观念，解决治理理论与实践的矛盾；国际层面上在进攻性网络政策与防御性网络政策之间采取平衡，以避免网络空间的“巴尔干化”；国内层面上对企业和民众做出一定程度的让步，在保障网络安全和保护公众隐私之间寻找平衡，避免网络战略影响民众对政府的支持。此外，还大力加强与网络新兴大国之间建立信任措施，为在网络空间“建章立制”创造有利环境。

在具体贯彻过程中，奥巴马政府采取了四大措施。第一，调整对网络空间全球治理的认知，正视网络空间的主权属性，缓和网络空间治理困境。奥巴马政府一直视网络空间为“全球公域”，否定“网络主权”，并将这种认知延伸到网络空间全球治理进程当中。当前网络空间的全球治理有三大主要平台，分别是联合国下设的互联网治理论坛（IGF）、国

① Adam Segal, “Chinese Computer Games: Keeping Safe in Cyberspace”, *Foreign Affairs*, March/ April 2012, pp. 16-17.

② Mark D. Young, “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power”, *Journal of National Security Law & Policy*, Vol. 4:1732010, pp. 173-176.

③ Panayotis Yannakogeorgos & Adam Lowther, *Conflict and Cooperation in Cyberspace*, New York: Taylor & Francis Group, 2013, pp. 50-66.

际电信联盟(ITU)以及“伦敦进程”。[①] 奥巴马政府认为,在互联网治理论坛和国际电信联盟这两个平台中发展中国家数量占优,它们更支持“网络主权”,于是采取各种措施抵制其发挥作用,并于 2011 年创立“伦敦进程”,试图以此主导国际网络空间治理进程。网络发达国家与网络发展中国家在网络主权问题上相互对立,加剧了网络空间全球治理的困境。2013 年 6 月,由包括美国在内的 15 国代表组成的联合国专家组发表了一份报告,首次明确“国家主权和源自主权的国际规范和原则适用于国家进行的通信技术活动,以及国家在其领土内对通信技术基础设施的管辖权”。报告进一步认可“联合国宪章在网络空间的适用性”。[②] 与 2010 年版联合国专家组报告相比,这是一个巨大进步,为寻找网络空间治理共识奠定了理论基础,同时也表明美国正在调整网络空间全球治理的观念。

第二,调整在网络空间全球治理上的策略,理顺治理理论与实践的矛盾,避免网络空间分裂。一直以来,美国政府理论上支持“多利益攸关方”模式在网络空间治理中发挥主导作用,并主张限制政府和政府间组织发挥作用。[③] 但实际上,美国却控制着 ICANN 这样掌握互联网战略资源的国际机构不肯放手。ICANN 垄断了互联网的 IP 地址分配、域名注册和域名解析服务等关键性资源,美国通过控制 ICANN 掌握了互联网的封疆权和路由权。[④] 在伊拉克战争和阿富汗战争中,美国就通过 ICANN 停止对伊、阿两国的互联网域名解析服务,切断两国与国际互联网的联系,给两国造成严重的政治、经济、社会冲击,为美国取得军事胜利创造了条件。因此,奥巴马政府一直视其为国家战略资产,拒绝放权。2014 年 3 月,美国商务部下属的国家通信管理局突然宣布将放弃 ICANN 的控制权,将其移交给全球“多利益攸关方”。此举的深层原因在于,奥巴马政府将网络空间战略的重心转移到国际战略中,旨在加快网络空间的“建章立制”进程。在战略目标上,向国际社会表明美国无意在网络空间谋求霸权,以恢复美国在网络空间“建章立制”上的道德形象和合法性,继续主导网络空间治理进程。在策略上,对内可以拉拢在网络空间拥有强大影响力的非政府组织、互联网公司、学术界和舆论界,对外可以尽快修复网络空间战略的盟友体系。“棱镜门”事件后,美国先是对愤怒的欧洲领导人进行安抚,随后又积极支持欧洲制定的《布达佩斯网络犯罪公约》成为国际标准。放弃 ICANN 的控制权是进一步向欧洲做出让步的姿态。[⑤] 当然,奥巴马政府不会放弃对 ICANN 的影响力。只要能保证 ICANN 在国际化进程中其功能、总部、人员构成、决策程序等不发生改变,美国政府依旧可以通过在 ICANN 董事会、支持组织和咨询委员会中的绝对话语权,发挥重大影响力。此外,此次移交并不包括具有域名解析功能的 13 台根服务器。为了控制整个移交过程和结果,美国政府还通过与国会之间“互动”,向国际社会施加压力。如近期美国众议院通过的“持续审视域名公开事务法案 2014”(Domain Openness Through Continued Oversight Matters Act of 2014),提出要对政府“移交 ICANN”的行为进行研究和评估,并要求政府确保“多利益攸关方”不受其他国家和政府间组织影响。[⑥] 一旦该法案获得通过,相关的审计和调研将至少需要 1 年时间,从而大大放缓移交进程。

第三,加强在网络空间的行为规范建设,重塑道德形象。美国长期以来过度追求发展网络空间的技术能力和行动能力,却忽视了网络空间的伦理道德,这是导致其网络空间战略受阻的主要原因。鉴此,奥巴马政府一是加强了对相关政策的网络伦理审查。“棱镜门”之后,奥巴马总统任命了一个独立的调查委员会对政府的情报监控活动进行审查。2013 年 12 月,该委员会发布了一份名为《变动世界中的自由与安全》(Liberty and Security in a Changing

① Margaret P. Karns& Karen A. Mingst, *International Organizations, The Politics and Process of Global Governance*, London: Lynne Rienner Publishers, 2010, pp. 540-541.

② United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98, June 24, 2013.

③ Roger Hurwitz, “Depleted Trust in the Cyber Commons”, *Strategic Studies Quarterly*, Fall, 2012, pp. 21-23.

④ 杨剑:《数字边疆的权利与财富》,上海人民出版社,2012 年,第 207-215 页。

⑤ “U. S. to Relinquish Remaining Control over the Internet”, *The Washington Post*, March 15, 2014.

⑥ “Domain Openness through Continued Oversight Matters Act of 2014”, H. R. 4342, 113th Congress 2nd Session(2014).

World)的报告,认为"国家安全局存在一些严重和持续地违反隐私及相关规定的行为,引发了人们对国家安全局有效、合法管理自己职权能力的担忧"。报告还指出,"监控计划破坏了网络空间的开放、统一,应当对国家安全局进行改革,建议下一任国安局局长由平民担任,网络司令部与国家安全局的长官不能由同一人担任。"①奥巴马政府进一步承诺,政府将与国会一道就《爱国者法案》旨在允许政府收集民众电话元数据的第 215 条款进行修改。二是基于《外国情报监听法》加强公众监督,避免类似"棱镜计划"的监听行动超出法律允许范围。三是要求情报部门加强公开和透明,尽可能多地向公众提供关于网络监控的信息,并责成司法部出台对《爱国者法案》第 215 条款的司法解释。四是责成深处漩涡中心的国家安全局通过参加国会听证、公开材料等形式回应民众诉求。2013 年 8 月,国家安全局公布了一份关于其任务、职责、合法性来源以及关于监控项目一些细节的报告,以增加民众的知情权。但与此同时,审查报告中对国家安全局进行组织改革的提议并没有得到落实。2013 年 4 月,国家安全局局长基思·亚历山大宣布辞职,继任的麦克·鲁杰不仅是军队少将,而且身兼国家安全局与网络司令部两职。在美国军费缩减的背景下,国家安全局的财政拨款依旧保持增长。事实表明,尽管美国政府加强了对网络监控的监管,但网络监控依旧是美国网络空间战略的核心支柱。

第四,加大建立信任措施(CBMs)力度,缓和网络空间的政治化、军事化趋势。美国与新兴大国在网络空间"建章立制"上的立场差异以及沟通机制的缺乏,导致双方互信缺失,加剧了网络军备竞赛和网络安全形势恶化。因此,奥巴马政府借鉴在核安全领域的合作模式,加大了与网络新兴大国在网络空间建立信任措施的力度。② 2013 年 6 月,美俄之间达成了一项在网络空间建立信任措施的协议,内容包括:建立军事热线,双方的网络协调员可以就网络安全危机直接对话;建立双方计算机应急响应机构(CERT)之间的联系,加强技术、数据等领域交换;成立网络工作组,讨论网络空间威胁,寻找合作领域;加强双方政策文件的交换,增加网络军事发展的透明度。③ 同年 7 月,在网络安全领域一直相互指责的中美两国也在网络问题上取得共识。双方在第五轮中美战略与经济对话(S&ED)之前的战略与安全对话(SSD)框架下设立了中美网络安全工作组,就网络安全领域的对话与合作展开了讨论。双方提出要建立经常性交流机制,加大在维护网络安全与打击网络犯罪领域的合作。此后,双方停止了网络安全领域的相互指责。工作组于 2013 年 12 月在北京又召开了一次会间会,双方对于落实网络工作组第一次会议达成的共识表示满意,并将进一步加强各个领域的合作。2014 年 4 月,曼迪昂特公司再次发布《中国网络间谍的报告》,但与上一次相比,没有了美国政府的造势,因而报告并没有掀起任何波澜。

建立信任措施虽然不能从根本上扭转国际网络空间军事化趋势,但可以避免由误判导致的军事冲突,从而降低网络空间军备竞赛的速度,为国际网络空间的"建章立制"创造有利环境。

结语

奥巴马政府调整网络空间战略首先是要纾缓国际、国内压力,其次是要在进攻与防御之间寻找均衡的策略,最后还要落实到网络空间的规章制度、行为规范,但其调整不会改变美国以网络军事力量建立网络霸权、以发展进攻性网络能力维护安全,并主导网络空间秩序的战略思想。美国在战略思想和政策上的调整,缓和了各方在网络空间治理中的对立情绪,有助于国际网络空间"建章立制"朝着有利于美国主导的方向发展,并压缩网络主权与政府主导模式的国际空间。新的形势下,网络空间治理理论创新关系到网络空间未来的发展,也是各个网络新兴大国面临的首要问题。○

(责任编辑:沈碧莲)

① The White House, "Liberty and Security in a Changing World", http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. (上网时间:2014 年 4 月 19 日)

② Meyer Paul, "Diplomatic Alternatives to Cyber-Warfare", *The RUSI Journal*, Volume 157, Issue 1, 2012, pp.14-19.

③ "U.S. and Russia Sign Pact to Create Communication Link on Cyber Security", *The Washington Post*, June 17, 2013.