《美国研究》2012 年第 3 期

网络空间的中美关系：竞争、冲突与合作[①]

蔡翠红

〔内容提要〕在中美关系各领域，网络空间问题在极短时间具有了极其重要的意义。网络空间不仅对传统中美关系形成了冲击，而且还引发了相应的博弈与竞争，如网络空间治理权之争、网络战略优势竞争，以及与之相随的网络技术优势的夺取、网络军备竞赛和网络话语权竞争等。网络事务管理的主权性与网络空间运行的开放性之间的矛盾构成中美关系网络冲突的根源。网络空间的全球性及世界各国所面临的网络信息安全等共同威胁，促成了中美关系在网络空间的合作，如在网络治理的国际制度建设、应对网络犯罪、技术合作、网络冲突控制等方面。避免网络空间的中美关系走向安全困境，需要相对稳定的实践。对网络监管和网络主权的认同、建立中美网络空间的战略互信是实践的重要方面。

关键词：美国外交 中美关系 网络空间 安全困境

中美关系在全球网络化进程中出现了新的竞争、冲突和合作态势，尤其是随着中国实力的上升和社会网络化程度的提高，中美关于网络空间的歧义与合作需求开始扩大。“在未来的国际政治中，或许没有比美中关系更重要的国家间关系了。而在两

① 本文为作者主持的国家社会科学基金项目《21 世纪中美关系中的网络政治研究》（项目批准号 12BGJ018）和教育部人文社会科学研究项目《网络政治学视角下的中美关系》（项目批准号 09YJCGJW004）的成果之一。感谢本刊匿名审稿人对本文提出的修改建议。

国关系中，没有什么问题像网络安全问题一样，如此迅速地冒出来，并引发了很多摩擦”。[①] 从“谷歌事件”到“网络窃密”的指控，从“网络安全最严重威胁”的界定，再到“互联网自由”的人权谴责，中美在网络问题上的摩擦日益频繁。[②] 有学者甚至将中美在网络空间的关系界定为数字版的新冷战。

中美关系在网络空间的拓展包括两个方面，一是信息网络对传统中美关系的冲击，二是中美关系在网络空间的博弈。

网络空间的中美关系不仅是现实中美关系在网络空间的映射与再现，还将是一个新型数字领域的竞争、冲突与合作的复合体。那么，网络空间对中美关系哪些领域、哪些方面产生了影响？如何使网络空间的中美关系避免走向安全困境，从而推动中美关系这一领域的良性发展？本文试图对这些问题进行梳理和分析。

一 竞争：网络无政府状态下的博弈

网络空间具有无政府主义状态的基本特性。作为一个全球开放互联的体系，网络空间不存在清晰的国家边界，单个政府不能对其进行有效管理，目前网络治理的国际机制也尚未完善。无论从法律、政策还是从安全角度来看，网络空间都还是一个没有形成全球共同规范的未知领域（uncharted territory），无论是权威、透明度，还是责任都不是很清晰。从某种意义上而言，目前的网络空间如公海和外太空一样，是一个无政府状态的全球公域（Global Commons）。

在这种无政府状态下，网络空间的中美关系首先是竞争的关系。这些竞争可以分为两方面，一是针对网络空间无政府状态的治理权之争，二是针对这一电子公所的网络战略优势竞争，包括网络技术优势的夺取、网络军备竞赛和网络话语权竞争等等。对于网络这样一个无政府状态下的全球公域，任何一个国家都想捷足先登，抢占高地，并夺取优势。[③] 中美作为两个超级大国，当然也不例外，竞争也由此产生。作为互联网的发源地，美国在技术、管理、经济，甚至文化上意图主导信息网络。这自然导致其他国家与其在信息网络治理权方面进行竞争，例如针对网络技术规范、网络空

---

① Kenneth G. Lieberthal & Peter W. Singer, “Cybersecurity and U. S.-China Relations,” February 23, 2012. available at: http://www.brookings.edu/papers/2012/0223_cybersecurity_china_us_singer_lieberthal.aspx.

② Kenneth G. Lieberthal & Peter W. Singer, “Cybersecurity and U. S.-China Relations.”op. cit.

③ 对此，美国早已提出信息优势（Information Edge）的概念并谋求长期保持信息优势。Joseph S. Nye, Jr. and William A. Owens, “America's Information Edge,” *Foreign Affairs*, Volume 75, No. 2, March/April 1996, pp. 20～36; Kevin O'Connell and Robert R. Tomes, “Keeping the Information Edge,” *Policy Review*, December 2003, pp. 19～37.

间国际行为规则等。

网络治理权就在于谁能以何种立场建立一套对自己有利的网络规范,并要求他人依此原则在网络空间里从事活动。网络治理权涵盖结构、功能、文化三个层面。一是对网络空间结构层面的治理。这是早期网络治理的重点,如域名管理、IP 地址分配、网际费用结算等。互联网是美国人发明的,作为互联网运行基础的根服务器、域名体系和 IP 地址资源都由美国政府授权的机构管理和控制,因而在结构层面,美国已然捷足先登;二是对网络空间功能层面的治理,比如针对垃圾邮件、隐私保护、授权访问等安全措施与规则等;三是对网络空间文化层面的治理。随着网络的蔓延和普及,文化层面的治理将越显重要。网络治理权的利益相关方有很多,作为治理主体的制度行动者也同样有很多选择,比如国际组织、主权国家、跨国行为体、次国家行为体、市民社会、行业机构、网络精英等等。[①] 而主权国家则是当前国际体系中利益争夺的主要行为者。究竟谁能够在网络治理权这块大蛋糕中分得大块,这决定着谁的利益将得到更多体现。

美国一直谋求掌控全球网络空间发展、治理与安全规则机制主导权。作为互联网核心的发源地,它拥有包括 IP 地址分配等诸多源头服务的控制权。2005 年 6 月,美国商务部发表声明,宣布美国计划永久保持对互联网的监管,成为域名的主人。[②] 在国际标准方面,多年来美国通过标准规则控制产业链下游市场,中国自主研发的无线局域网标准在国际申标的进程中多次遭到美方的阻挠,这不仅是个别美国企业出于自己的利益而使技术问题政治化的结果,还说明了美国政府不愿在网络国际标准方面被竞争对手赶超。

作为信息化进程的后起之秀,中国在网络空间治理权方面总体处于弱势,但中国争取网络空间治理话语权的立场也是鲜明的。2011 年 9 月 12 日,中国与俄罗斯、塔吉克斯坦和乌兹别克斯坦四国驻联合国代表在第 66 届联大上提出确保国际信息安全的行为准则草案。这份文件呼吁与“散布旨在宣扬恐怖主义、分离主义和极端主义或破坏其他国家政治、经济和社会稳定的信息”作斗争。同年 9 月 22 日,由俄罗斯牵头组织的 52 国情报部门负责人闭门会议在叶卡捷琳堡召开,俄安全会议和外交部联合起草的《联合国确保国际信息安全公约草案》再次提交会议讨论。这份 18 页的文件禁止把网络用于军事目的或颠覆他国政权,但仍为各国政府保留了很大的在国家

① 蔡翠红:《国际关系中的网络政治及其治理困境》,载《世界经济与政治》2011 年第 5 期,第 108 页。

② Kenneth Neil Cukier, “Who Will Control the Internet?” *Foreign Affairs*, November/December 2005, Vol. 84 Issue 6, pp. 7～13.

局域网内的行动自由。[①]这在某种程度上是中俄等国对美国借助信息网络颠覆它国政治体制企图的抗议，也是争取网络治理权和话语权的努力。

中美网络战略博弈亦日趋激烈。网络已经成为输出软实力、塑造良好国家形象、建立公众互信、协调外交资源、促进国家利益、达到国家战略目标的主要手段。美国、日本、印度等相继推出涉及网络的国家战略，建立国家级网络空间管理机制，并在理念创新和规则制定方面"圈地插旗"、抢占先机。美国尽管在近年有国力衰落的疑虑，但在网络空间仍然保持全球战略的主动态势。在传统的"防御性"战略的基础上，美国已开始试探"网络空间的先发制人"行动战略，力图占据网络威慑(cyber deterrence)的高位。[②] 奥巴马政府一方面将网络将关键基础设施升级为国家战略资产，另一方面又于 2009 年 6 月成立网络战司令部(Cyber Command)，全面提升网络攻防能力。2011 年 3 月，美国网络司令部司令基思·亚历山大(Keith Alexander)首次勾画了提升美军网络战能力的五大战略支柱。[③]同年 5 月，美出台首份《网络空间国际战略》，[④]内容与目标已从美国自身的网络空间范围扩展到全球网络空间，表明美国已全面展开网络空间竞争与掌控。

在网络空间的总体战略方面，中国是后来者，迄今为止尚未发布成文的国家网络安全战略。然而，美国对外关系委员会资深研究员亚当·西格尔(Adam Segal)认为，中美两国正在进行网络空间战略竞争，他认为这从 2011 年 3 月 31 日中国发布的《2010 年中国的国防》白皮书中首次具体提到网络空间可以看出。[⑤]一些西方学者认为，中国正在利用网络战的非对称优势提升其军事竞争力。[⑥]

---

① Adrian Croft and Georgina Prodhan, "UK, U. S. Talk Tough on Web Freedom at Cyber Talks," Reuters Website, November 1, 2011, available at: http://www.reuters.com/article/2011/11/01/us-technology-cyber-conference-idUSTRE7A00EK20111101.

② Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice?" *Strategic Studies Quarterly*, Fall 2010, pp. 102～135.

③ 提升美军网络战能力的五大战略支柱为：将网络空间看作与陆海空天一样重要的作战领域；采用主动的网络防御措施和其他新型防御方法；在国家网络安全战略上，与政府机构和私营部门进行协作；加强与国际伙伴的联系；招募一支网络安全队伍。Elizabeth Montalbano, "Cyber Command Pursues 'Defensible' IT Architecture," March 21, 2011, available at: http://www.informationweek.com/news/government/security/229400008?cid=RSSfeed_IWK_Government.

④ U. S. White House, *International Strategy for Cyberspace*, May 2011, available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

⑤ Adam Segal, "China's Defense: Intricate National and Volatile," *China & U. S. Focus* (Online), March 30, 2011, available at: http://www.chinausfocus.com/peace-security/china%E2%80%99s-defense-intricate-national-and-volatile/.

⑥ Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*, Vol. 8, Issue 1(2008), Article 2, pp. 28～80, available at: http://epublications.bond.edu.au/cm/vol8/iss1/2.

中美网络战略博弈在具体战术与策略层面首先表现为网络技术优势的夺取。美国非常清楚,任何国家想要保持在信息领域和网络空间的主导权,一个必不可少的条件就是要有先进的网络信息技术作为基础。美国在网络产品、技术和应用协议等方面都占据绝对优势。但是美国也面临着在国家创新能力、增长势头方面的挑战。所以,美国一方面鼓励扶持硅谷和波士顿的128号公路沿线这样的基于大学研究机构、政府市场、风险投资、高校培养出的技术工人和新兴企业相结合的信息技术创新基地,另一方面政府在政策上鼓励创新,调整一系列相关政策如反垄断政策以促进创新;在资金上提供研发资助;在全球范围吸纳信息技术人才;鼓励先进军用技术民用化等等。中国在信息化浪潮中奋力追赶,并在很多网络技术与安全策略方面力求自主创新(Indigenous Innovation)。近年来,中国在一些关键信息技术领域取得突破,如先进集成电路芯片与光电子器件、高性能计算机与软件、下一代互联网与信息安全、第三代移动通信与无线通信、数字电视与音视频编码、信息技术在产业中的应用等。①

其次是网络军事化加速升温,中美网络军备竞赛显现。② 美国是世界上第一个引入网络战概念的国家。2011年5月美国公布的《网络空间国际战略》提出,③如遭受严重网络攻击,美国将以武力还击。2011年7月美国防部公布的首份《网络空间行动战略》,④则直接将网络空间定位为军事"行动领域",把美国可能遭受的严重的网络攻击定性为战争行为,并进行反制,反制手段既包括动用网络攻击武器,也包括动用传统的军事力量。美国《外交政策》杂志网站发表文章说,美军在网络空间的扩张可能会引发网络军备竞赛。如果美军参与攻击性的网络行动,那么其他国家也会跟进。⑤ 中国国防部也于2011年5月宣布设立了"网络蓝军"。虽然中国国防部称中国"网络蓝军"并不是黑客部队,而是根据训练的需要,为提高部队的网络安全防护水平而设立的。但是美国《时代》周刊网站称,尽管中国的"网络蓝军"名义上是自卫,但考虑到中国丰富的人才储备和政府慷慨的资金投入,中国能够在虚拟战场上进行

① 邬贺铨:《中国信息技术发展的现状和创新》,载《中国信息界》2006年第12期,第21~22页。

② Mark Clayton, "The New Cyber Arms Race," *Christian Science Monitor*, March 7, 2011.

③ U.S. White House, *International Strategy for Cyberspace*, May 2011, available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

④ U.S. Department of Defense Strategy for Operating in Cyberspace, July 2011, available at: http://www.defense.gov/news/d20110714cyber.pdf.

⑤ David E. Hoffman, "The Cyber Arms Race," *Foreign Policy* (Online), June 1, 2011, available at: http://hoffman.foreignpolicy.com/posts/2011/06/01/the_cyber_arms_race.

迅速和匿名攻势，这一前景将令世界其他领导人坐卧不安。[①]

再次是中美网络话语权的竞争。欧美的网络化程度在全球领先，网络运行规则也由它们主导，在网络信息传播中英语也占据优势。而且，从当前国际网络话语体系看，美国的政治话语不仅似乎成为判断是非的合法标准，而且往往带有攻击性。例如，从2007年开始，美国乃至主要西方国家的主流媒体几乎不约而同地开始炒作“中国黑客威胁”的集体行动，将“来自中国的黑客袭击”与“中国政府支持的黑客袭击”划上等号，制造“中国黑客威胁论”。[②]近两年美国各界频频出现网络空间的“中国威胁论”。美中经济与安全评估委员会前主席拉里·沃策尔(Larry Wortzel)和共和党众议员兰迪·福布斯(Randy Forbes)称“现阶段最恶劣的、可能对美国安全构成最大威胁的网络攻击行为来自中国”。[③] 更有研究人员将中国称为“网络威胁的特洛伊之龙”，[④]认为中国间谍行为是对美国科技安全的最大威胁。美国《华尔街日报》2012年1月27日刊登《中国的网络盗窃行为是国家政策：必须予以反对》一文，称“中国政府有一项关于在网络空间从事经济间谍行为的政策”。[⑤] 2012年3月8日，美国国会下属的美中经济与安全评估委员会(US-China Economic and Security Review Commission)发布的由美国诺斯罗普·格鲁曼(Northrop Grumman)公司撰写的分析报告称，当台海或南海地区爆发冲突时，中国的网战能力可对美军构成“真正威胁”。[⑥]

受制于政治软实力的不足、话语自主创新的缺乏，中国的政治和新闻话语体系在国际网络传播体系中不但处于边缘，而且总是处在防御状态，不停地遭到合法性的质疑。在这场话语权竞争中，美国占据着明显优势。中国作为崛起大国，应更好地利用互联网，释疑对外政策，改善国家形象，讲述能够让国内和国际社会都信服的“中国式

---

① Chris Gayomali, “China Admits to Assembling a 30-Strong Team of Elite Cyber Commandos,” *Time* (Online), May 27, 2011, available at: http://techland.time.com/2011/05/31/china-admits-to-assembling-a-30-strong-team-of-elite-cyber-commandos.

② 沈逸：《网络安全与中美安全关系中的非传统因素》，载《国际论坛》2010年7月第12卷第4期，第46页。

③ Larry Wortzel and Randy Forbes, “Bolster U.S. Cyber Defenses: Make Comprehensive Push Against Global Threats,” *Defense News* (Online), May. 31, 2010, available at: http://www.defensenews.com/article/20100531/deffeat05/5310303/bolster-u-s-cyber-defenses.

④ John J. Tkacik, Jr., “Trojan Dragon: China's Cyber Threat,” *Backgrounder* (Published by The Heritage Foundation), No. 2106, February 8, 2008, pp. 1～12, available at: http://www.heritage.org/research/AsiaandthePacific/bg2106.cfm.

⑤ Mike Mcconnell, Michael Chertoff and William Lynn, “China's Cyber Thievery Is National Policy—and Must Be Challenged,” *Wall Street Journal*, January 27, 2012, on page A15. 类似言论还可参见 Michael Evans & Giles Whittell, “Cyberwar Declared as China Hunts for the West's Intelligence Secrets,” *Times* (Online), March 8, 2010, available at: http://technology.timesonline.co.uk/tol/news/.

⑥ Bryan Krekel & Patton Adams & George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp, March 7, 2012.

叙事”,促进国家利益,争取更多网络话语权。

二 冲突:网络主权与虚拟空间开放性的矛盾

网络空间的中美关系是冲突的关系。中美对网络空间的理解存在诸多分歧,例如经贸领域的政策和技术壁垒、政府行使网络空间管理权的限度、网络监管与审查、互联网自由与基本人权的关系等。分歧产生的根本原因在于网络主权与虚拟空间开放性的矛盾,其后果不仅可能对中国的政治稳定构成威胁,而且也放大了中美意识形态和价值观方面的冲突。

网络主权与虚拟空间开放性的矛盾又包括两方面,一是传统主权的可控领域和网络空间二者的不重合性,二是主权国家对网络空间实施权力的意愿与虚拟空间的开放性之间的矛盾。它们构成了网络空间中美关系冲突的起源。在互联网时代,国际政治已经从地域空间、外太空扩展到网络空间,国家主权也从领土、领空扩展到“信息边疆”和网络空间。国家主权在网络空间的自然延伸,就形成了网络主权,其主要内容就是国家在网络空间的管辖权行使。[①] 网络主权体现为对内和对外两个方面,对内体现为国家对其领域内任何信息的制造、传播和交易活动拥有最高权利;对外体现为国家有权决定采取何种方式,以什么样的程序参与国际信息活动,并且有权在网络空间利益受到它国侵犯时采取措施进行保护,决不允许任何外来干涉。[②] 然而,网络空间的开放性使得国家信息疆域并非以传统的领土、领空、领海划分的。信息边疆也可以说是一个虚拟的概念,因为每一台上网电脑都可看作是信息边疆上的一道关口。这些特性决定了网络主权与虚拟空间开放性之间的矛盾,并使网络空间的中美关系呈现冲突的一面。

网络空间中美关系冲突首先体现在经贸领域的政策和技术壁垒方面。中美在网络应用开放、跨境信息流动监管、信息和通讯技术行业的外国投资、数字跨境服务、数字版权保护等等方面都存在一定的矛盾与冲突。例如,由于中美知识产权侵权制度存在较大差异(中国著作权法中无间接侵权行为概念)及网络侵权的难以界定,相对于美国,中国著作权相关法律在现实生活中无法为著作权人提供充分的保护,并由此产生一些数字知识产权纠纷。美国还有针对网络审查国家的出口限制条例。2006年2月,众议院就专门提交过H.R.4780法案即“2006全球网络自由法案”,其中第

① 李鸿渊:《论网络主权与新的国家安全观》,载《行政与法》2008年第7期,第115~117页。

② 杨琳瑜:《网络主权视野下的互联网建设、运用、管理:“谷歌事件”的理性解读及其启示》,载《云南行政学院学报》2011年第1期,第105页。

三编专门指出对互联网限制国家的出口管制，“自本法案颁布之日起 90 天内，国务卿应与商务部长磋商，并发布条令确定恰当的外交政策控制规定与出口许可证制度，使美国辖下的任何人能够了解到，向互联网限制国家的、全部或部分地参与促进互联网审查制度的最终用户出口任何物品，均应遵守联邦法规汇编第十五编 730～774 条（通常称为“出口管理条例”）之规定。”①

此外，针对中国政治安全的信息技术企业商业纠纷政治化倾向也日趋明显，最典型的案例就是“谷歌事件”。② 美国国务卿克林顿不仅发表书面声明表示美国政府对谷歌事件的关切，还明确表示支持谷歌公司的决策，批评中国对网络信息的管制，并将中国列入“限制网络自由”的国家。可以说，谷歌公司最终从中国大陆市场退出的决定不乏美国政府的官方授意与支持，其背后蕴藏着奥巴马政府以“谷歌事件”为借口对中国施压而试图实现更多其他利益的动机。

在政治方面，网络空间中美关系冲突体现为中美意识形态和价值观的分歧，网络空间成为意识形态较量的新战场，中国传统意识形态和价值观受到前所未有的挑战。以美国为首的西方发达国家从来没有停止过对中国的政治图谋和意识形态渗透。他们公开地将无边界、低成本、高速度的网络视为“中国和平演变的源泉”，认为民众“会在这些讨论区接触到不同的政治观点，这将慢慢动摇中共政权对人民的思想控制，对中国政治发展带来一定的冲击和震撼”。③ 因而，2010 年初希拉里在关于“网络自由”的演讲中，④曾表示“美国以后将把不受限制的互联网访问作为外交政策的首要任务”，并首次将互联网自由与传统的四大自由（言论自由、宗教自由、免于贫困的自由、免于恐惧的自由）并列。2011 年初，希拉里发表题为《互联网的是与非：网络世界的选择与挑战》的演讲，宣布将投入 2500 万美元，以资助技术公司开发互联网访问工具，使身处“压制性国家”的网络活跃分子、持不同政见者和一般公众能够绕过网络检查。⑤

中美在网络空间的政治冲突对中国的政治稳定形成了威胁。一方面，西方的网络渗透可能引起中国公众信仰危机和文化危机。网络打开了言论的阀门。西方的民

---

① “Global Online Freedom Act of 2006，” 109th Congress 2d Session H. R. 4780，available at：http://www.govtrack.us/congress/bill.xpd？bill＝h109－4780.

② 美国方面对“谷歌事件”解读较为负面，如：Timothy L. Thomas，“Google Confronts China's ‘Three Warfares’，” *Parameters*，Summer 2010，pp. 101～113.

③ 彭前生：《刍论网络政治风险》，载《前沿》2010 年第 7 期，第 26 页。

④ Hillary Rodham Clinton，“Remarks on Internet Freedom，” January 21，2010，available at：http://www.state.gov/secretary/rm/2010/01/135519.htm.

⑤ Hillary Rodham Clinton，“Internet Rights and Wrongs：Choices & Challenges in a Networked World，” U. S. Secretary of State Remarks at George Washington University，February 15，2011，available at：http://www.state.gov/secretary/rm/2011/02/156619.htm.

主观念、政治模式、价值取向、人生态度和生活方式乘势进入,可能加剧公众的信仰危机和文化危机,从而可能削弱甚至瓦解形成国家凝聚力和维系社会政治稳定的文化基础。同时,网络不断培育出新的现实群体和虚拟群体,而群体认同的不断加强也使国家权威在人们政治观念中的至高无上的地位面临新的挑战。另一方面,恶意和敌意的网络政治参与较普通的网络渗透具有更大的破坏性。借助互联网的传播功能和组织功能,互联网成为渗透破坏、宣传煽动、操控境内活动的主要途径和重要场所,成为境内外敌对势力和敌对分子进行颠覆破坏活动的手段和工具。

在外交方面,网络空间给中美关系带来的冲突主要表现在两方面:一是网络活动所导致的外交冲突以及现实外交冲突行为在网络上的体现,可以分为基本理念、政策层面和具体热点问题等几个层面;二是由社交网站的屏蔽等监管引起的公共外交屏障冲突。

近年来中美网络外交冲突频频发生,形态多样。中美网络外交冲突和现实中美关系情形类似,可以分为几个层面:一是基本理念层面的冲突。近两年来,美国将网络自由与人权问题挂钩频频对中国进行施压。2011 年 2 月 15 日,希拉里·克林顿在乔治·华盛顿大学的演讲中公开点名中国、古巴等国家是“实行书报检查、限制网络自由、逮捕批评政府的博主的国家”。她宣称,要让压制互联网自由的国家付出经济代价,并且面临像埃及和突尼斯一样的动乱威胁,甚至提出要陷网络控制国家于“专制者困境”;[①]二是政策层面的冲突。中国出于保护自身民族企业的利益和维持有中国特色的管理方式,对于一些美国互联网公司的在华运作设置了相应的合理条件,从而使得一些美国公司望而却步,这在美国看来即损坏了美国互联网公司的公平竞争机会。另一些公司即使进入了中国市场,也被认为被迫向中国政府提供数据和信息。而美国的一些反制政策,如对于网络信息加密技术的出口限制、对翻墙软件的设计投资等,也一直是网络空间中美关系的冲突源;三是具体热点问题层面的网上冲突。科索沃战争中美国轰炸中国大使馆事件、美国对台售武问题、中美撞机事件、奥运火炬传递、谷歌事件等冲突中都少不了中美黑客的较量。这些较量中包含的网络民族主义情绪往往无益于外交冲突的解决,相反,由于网络民族主义的非理性和极端性,可能会影响外交谈判的原则和弹性。但是一般情况下,这些较量也有助于释放一些中美民间敌对和冲突的情绪。由审查和监管引起的公共外交屏障则是指中国境内不能正常访问脸谱(Facebook)、推特(Twitter)等美国社交网络所形成的中美民间与

① Hillary Rodham Clinton, “Internet Rights and Wrongs: Choices & Challenges in a Networked World,” U.S. Secretary of State Remarks at George Washington University, February 15, 2011, available at: http://www.state.gov/secretary/rm/2011/02/156619.htm.

公众交流的屏障。

三 合作:网络的全球性与“共同命运”之唤

除了竞争与冲突,网络空间的中美关系还是合作的关系。这种合作首先源于网络空间的全球性。网络空间的一个基本特征就是它打破了地域和国家界限,把世界连成了一个“网络地球村”。“国际互联网”一词本身就表明了这种传播体系是超越传统的民族国家边界而被镶嵌在国际生活空间中的技术结构。网络政治本质上是一种全球政治,政治主体、政治对象、政治活动空间都具有全球性。互联网的无政府状态特性、主权超越性以及技术影响不定性都呼唤着网络空间的全球治理。① 互联网本质上具有共享性和开放性的特征,这为参与者在网络空间发展和深化合作提供了机遇。中美政府在这一点上表现出了共同的认知和合作意愿。2011 年 12 月美国国务卿希拉里·克林顿在伦敦互联网自由大会上表明,“互联网本身不是消耗性(exhaustible)和竞争性的,一个人利用对互联网的使用并没有减少其他人的机会”。② 2010 年 6 月 8 日,中国国务院新闻办公室发布的《中国互联网状况》白皮书也明确提到了积极开展国际交流与合作。③ 因此,无论是从客观上网络空间的特性看,还是从中美的主观认知看,中美之间的协调与合作都成为必需与可能。

网络空间的全球性还使网络信息安全这种非传统安全对世界各国构成了共同威胁,使各国在某种程度上有了“共同命运”。中美在网络空间的共同利益与面临的共同威胁是以合作姿态采取共同立场和行动的基础。网络犯罪、信息安全问题等对世界各国的国家利益都构成了挑战,这些问题的解决需要全世界各国政府联合行动始有望解决。作为非传统安全问题,网络安全问题不只是个别国家的国内安全问题,而是一个必须通过开展长期、广泛和深入的国际合作,包括各国政府、各种国际组织、民间团体、私营企业和个人之间的充分合作,才有可能解决的国际安全问题。国际合作和发挥不同的利益相关者作用是国际网络安全的路径图的重要组成部分。④ 此外,从行为主体自身来看,即使从美国这一超级大国自身利益出发,国际合作也是必要的,因为只有借助合作,才能有效分担成本,减少其控制全球信息空间在主权和道义

---

① 蔡翠红:《国际关系中的网络政治及其治理困境》,载《世界经济与政治》2011 年第 5 期,第 107 页。

② Hillary Rodham Clinton, “Remarks at Conference on Internet Freedom,” U. S. State Department website, December 8, 2011, available at: http://www.state.gov/secretary/rm/2011/12/178511.htm.

③ 参见《中国互联网状况》白皮书,available at: http://www.scio.gov.cn/zxbd/wz/201006/t660625.htm.

④ Christine Sund, “Towards an International Road: Map for Cybersecurity,” *Online Information Review*, Vol. 31, No. 5, 2007, pp. 566～582.

上面临的阻力,并实现最大范围的控制,尽管美国希望这种国际合作是美国主导或支配下的不对等合作。

中美首先可以在网络治理的国际制度方面进行合作。网络空间这些年来的迅速发展是国际社会共同努力创造的成果,是人类共同的财富,加强全球互联网治理一直是世界各国的共同愿望和要求。作为两个举足轻重的大国,中美需共同合作,在遵循《联合国宪章》和其他国际公认的基本准则和维护本国信息领域国家主权、利益和安全的前提下,依据联合国、国际电信联盟有关决议和相关国际公约,共同促进和平利用国际信息网络空间的制度规范和国际政策的制定。中美都派代表参加了历届信息社会世界峰会(WSIS)及与互联网相关的一些其他重要国际或区域性会议,中美都是联合国中同意一系列推进网络安全的国际讨论建议的 15 国之一。2011 年 11 月 1 日至 2 日在伦敦召开的网络空间国际会议(London International Conference on Cyberspace)是首次由政府召集的网络议题国际会议,美国、中国和俄罗斯都派代表参会,美国副总统拜登还通过视频形式向大会的召开表示欢迎并致辞。虽然很难在参会的近 60 个国家间达成一致,但这是向制订网络空间国际规则迈出的第一步。2011 年 12 月 7 日至 8 日,由中国互联网协会和美国微软公司联合主办的第五届中美互联网论坛(US-China Internet Industry Forum,CIIF)在华盛顿举行,来自中美互联网业界、学界和政府部门的 180 多名代表与会交流,议题包括互联网服务提供者的社会责任、社交网络发展、互联网治理、网络安全等。该论坛已成为中美在互联网领域沟通合作的重要平台。①

其次,在应对网络犯罪方面,中美可以发表共同声明、建立信息分享机制,协调网络执法与司法程序等。针对超地域性、国际性趋势越来越强的网络犯罪,中美必须加强相互合作。世界上第一个针对网络犯罪的国际公约《网络犯罪公约》(*Convention on Cybercrimes: Europe Treaty Series* No. 185),是由美国与欧盟等国共同草拟的,目的是寻求应对日益猖獗的网络犯罪问题的应对措施。对参与《网络犯罪公约》的经验数据的分析表明,国家间的相互依赖和支持是应对网络攻击和网络犯罪的重要条件,而且合作程度越大,网络攻击的应对能力就越强。② 在应对网络犯罪方面,中美已开展一系列国际合作,中美执法合作联合联络小组(China-US Joint Liaison Group on Law Enforcement Cooperation, JLG)的成立就是一个很好的例证。2011 年 11 月 1 日至 2 日,中美执法合作联合联络小组第九次会议在华盛顿举行,会议讨

---

① 王恬、温宪、张旸:《让互联网成为促进中美关系积极因素》,载《人民日报》2011 年 12 月 10 日第 3 版。

② Qiu-Hong Wang & Seung-Hyun Kim, "Cyber Attacks: Cross-Country Interdependence and Enforcement," May 2009, Report from National University of Singapore, available at: http://weis09.infosecon.net/files/153/paper153.pdf.

论了中美两国在打击网络犯罪、刑事司法协助、知识产权刑事执法、追逃等等领域的执法合作问题。[①] 中国还参加了国际刑警组织亚洲及南太平洋地区信息技术犯罪工作组(The Interpol Asia-South Pacific Working Party on IT Crime)等国际合作队伍,并先后与美国、英国、德国、意大利等国家举行双边或多边会谈,就打击网络犯罪进行磋商。

当然,除了制度合作,中美还需要在信息技术方面进行合作与分享。中美两国处于信息化进程的不同阶段,在网络信息领域存在一定的冲突与竞争,但总的说来,网络信息战略的根本出发点都是为着本国的信息化进程服务,加强网络的安全利用,从而提高其综合国力。中美在下述网络基本目标方面是一致的:加强网络信息基础设施建设,保证网络信息能够有效、低耗地传输;鼓励工商业界利用网络信息资源提高产品附加值,积极参加全球市场竞争;开展教育和培训,提供训练有素的网络信息人才和信息用户;支持网络信息服务机构的发展,满足日益增长的社会信息需求。[②] 基于这些目的的共同性,中美信息网络技术合作能够将成本收益比例最优化。中美应发挥各自优势和互补性,加强合作,实现互利共赢。美国有技术、人才、资金和经验等方面的优势,中国有世界最大的互联网市场及信息化进程快速发展的前景。因此,为了推动中美双方在计算机科学和信息技术的合作与交流,在中国国家自然科学基金委员会和美国国家科学基金会的共同倡导下,中美计算机科学高峰论坛 2006 年开始举办。[③] 2011 年 10 月 21 日,美国前总统比尔·克林顿在中美联合主办的硅谷高科技创新和创业高峰会议上表示,信息技术领域空间巨大,中美在该领域并非"零和游戏",两国应该创造更多机会分享彼此的创新成果,充分利用信息技术为创造就业等服务。[④]

此外,中美两国的网络冲突控制合作机制也必须提上议程。全球信息空间的技术和物理特性、中美关系面临偶发突发事件所带来的不确定性使虚拟中美关系的冲突控制显得格外重要。鹬蚌相争,渔翁得利,能够从中美相争中谋取额外利益的国家与非国家行为体不在少数。这一方面可以通过双方网络战略透明机制实现,另一方面则应建立一定的中美网络危机解决机制。中美两国不希望网络空间变得更加"复

---

① "The Ninth Meeting of the China-US Joint Liaison Group on Law Enforcement Cooperation Opens in Washington," November 3, 2011, available at: http://www.fmprc.gov.cn/eng/wjdt/wshd/t874534.htm.

② 狄娟娟:《试论中美国家网络信息政策》,载《科技情报开发与经济》2009 年第 19 卷第 20 期,第 87 页。

③ 中美首届计算机科学高峰论坛(US-China Computer Science Leadership Summit)目前已经举行过三次,分别是 2006 年 5 月、2010 年 7 月、2010 年 6 月。

④ Bill Clinton, "Opening Keynote Speech at 2011 Silicon Valley Technology Innovation & Entrepreneurship Forum (SVIEF)," October 21, 2011, available at: http://www.svief.org/english/yqjb/BillClinton.htm.

杂与多变”,那么就需要加大开放力度。[①] 显然,2011 年 3 月 31 日中国发布的《2010 年中国的国防》白皮书,是中国透明化其军事现代化的一个举措。始于 1997 年的中美国防部防务磋商机制的目的之一就是管控危机和风险,避免误判。[②] 2012 年 5 月,中国国防部长梁光烈访问美国,在会晤美国国防部长帕内塔时,双方亦同意就应对互联网安全威胁进行合作。帕内塔说,为避免将来数字化威胁导致的危机,美中两国共同应对网络安全问题具有极其重要的意义。梁光烈在表示中国是近年来网络入侵的最大受害者之一的同时,也明确表示北京愿意参与加强网络安全的共同努力。[③] 如何将信息空间的中美冲突保持在可接受的范围之内,如何确保避免因为未经授权或纯粹民间的网络袭击,引发两国之间的大规模冲突,将在未来构成一个严峻的中美关系考验。

四 展望:网络空间的中美关系需走出安全困境

网络空间的中美关系呈现冲突、竞争与合作。在网络无政府状态下,对国家而言,一方发出的信号往往被另一方理解为威胁,便针锋相对地发出同样的威胁信号,安全困境就会产生。网络空间的中美关系走出安全困境需要以下稳定的实践。

实践之一是对网络监管和网络主权的认同。国家间对主权制度的相互承认是逃离“霍布斯世界”的一种方式。同样,对网络主权的承认是虚拟中美关系摆脱安全困境的要点之一。在霍布斯的世界中,安全是由国家权力来决定的,但主权原则改变了这种情况。网络主权制度可以使各国相互承认各自相应的网络监管权,国家对被潜在敌人控制的恐惧减少,国家间合作的可能性增加。尽管网络本身具有开放性,但是网络空间中美关系的健康发展需要强调网络主权与虚拟空间开放性的平衡,原因在于下述两方面。

首先,网络空间本身的性质决定了其监管需求。理论上,网络空间是没有边界的,目前没有一个终极管理者。因此,网络空间是极端个人自由主义滋生的良好场所。在网络政治参与中,相当大数量的参与者不是基于公民的责任感,有时甚至是

---

① Adam Segal, “China's Defense: Intricate National and Volatile,” *China & U.S. Focus* (Online), March 30, 2011, available at: http://www.chinausfocus.com/peace-security/china%E2%80%99s-defense-intricate-national-and-volatile/.

② 中美国防部防务磋商机制始于 1997 年,目前已召开过 12 次。第 12 次中美国防部防务磋商 2011 年 12 月 7 日在北京举行。

③ “US, Chinese Defense Officials Agree to Work Together on Cybersecurity,” May 8, 2012, available at: http://www.infosecurity-magazine.com/view/25654/us-chinese-defense-officials-agree-to-work-together-on-cybersecurity/.

为了发泄心中的不满情绪，这种参与往往超出了法律和制度的许可，表现出狂热性、发泄性、破坏性等显著特征。[①] 当目的无法实现时，利益表达的需求并没有消除。如果某个人或某个群体在政治沟通中经常遭受挫折，他们往往就会由和平转为对抗，以极端的形式进行表达，从而破坏正常的政治秩序，导致社会不稳定。

其次，依法管理互联网是世界各国通行做法。通过隐性的政治控制来强化国民对当局和政治典则的认同，维护政治秩序，是所有政治体系的本能反应和必然举措，对于后发展国家尤其重要。这种控制一般体现为三个方面，即国家垄断信息、控制传媒、塑造民族国家意识以及节制政治参与。[②] 很多专家曾预测，对网络空间的政治监督行为定会失败，只可能出现两种结局：一个自由扩张、为政治权力的控制范围所不及的互联网；或者是一个被政府控制扼杀、不能实现其潜在的社会和经济利益的互联网。让这些专家不解的是，在中国这两种情况都没有发生。[③]

实践之二是中美网络空间的战略互信的建立。在网络空间，缓解中美之间日益严重的安全困境并非易事。中美两国对彼此网络行为的怀疑都与日俱增，而这种怀疑很容易影响它们对彼此长期意图的整体判断。温特认为二者或警觉或攻击，取决于对对方意图的理解。如果一方发出的信号是威胁的，那么另一方经过接受、解读和赋予意义后，也会被理解成为威胁，威胁感就由此而生；如果一方发出的信号是友好的，经过同样的认知过程，也会被理解成为友好，那么双方就不会产生威胁感。在没有确凿证据的情况下，美国倾向于将来自中国的黑客袭击视作“政府资助的行为”，通过炒作来自中国的“威胁”来营造和凸显中国政府对美国的所谓“敌意”，甚至认为中国满是针对美国的“网络民兵”(Cyber-militia)。[④] 这种宏观战略上将中国塑造成为美国的“敌人”的做法，旨在维护美国对网络话语权的主导权。这给外界的印象是，中国政府正系统地通过有组织的黑客行动窃取西方国家的机密情报，威胁包括美国在内所有西方国家的信息安全。这种对中国黑客和中国威胁的判断，以及在此基础上形成的政策，可能构成一个呈现螺旋式互动的自我实现的预言。

布鲁金斯学会约翰·桑顿中国中心主任李侃如(Kenneth Lieberthal)认为，中美双方的决策者和公众都必须面对如下事实，即网络领域的发展带来的是紧张关系，而

---

① 郭小安：《网络政治参与和政治稳定》，载《理论探索》2008 年第 3 期，第 128 页。

② 刘邦凡、王磊、李汉卿：《信息爆炸条件下的政治控制》，载《理论探讨》2009 年 10 月下半月刊，第 4～5 页。

③ George Yeo & Eric X. Li, “Rise of the Dragon: China Isn't Censoring the Internet. It's Making It Work,” *The Christian Science Monitor*, January 23, 2012.

④ Shane Harris, “China's Cyber-Militia,” *National Journal*, June 2008. Vol. 40 Issue 21, p. 32.

不是互信。[①] 这恰恰反映了中美网络领域的战略互信的强烈需求。作为互联网的发源地,信息技术在美国整体国家发展中具有特殊重要的地位。正因为如此,面对中国日益发展的信息网络能力,无论是普通美国民众、理论研究者还是政策制定者,都会产生深刻的不安全感,并对威胁可能的来源投射强烈的不信任乃至敌意。这种倾向从根本上来讲是双方缺乏战略互信的产物。美国担心其日益依赖的信息系统在为其带来不对称优势的同时也可能成为美国的"阿基里斯之踵",担心中国会利用这种不对称优势弥补与美国的军事实力差距,[②]担心中国的人口规模及其中央集权化的政治制度创造出一个与外界互联网既有联系又相对独立的平行互联网,并对美国所主导的互联网形成抗衡与威胁。美国在意识形态领域的攻势,在信息技术领域所具有的优势,以及冷战后美国在历次高科技局部战争和对外军事干涉行动中的网络行动,也让中国担心"美国在操作系统中留下的后门"可能对中国国家安全构成严重威胁。[③] 如何克服这些心理因素,增加中美在网络空间的互信,减少虚拟领域的矛盾和冲突、增加合作并保持相对稳定,是中美关系面临的巨大挑战。

最后,需要指出的是,无论是竞争、冲突还是合作,网络空间的中美关系某种程度上都是实体世界中美关系的体现。由于核心利益、政治制度、文化传统等差异,中美之间的矛盾和分歧是客观存在的,这些矛盾和分歧必然在网络空间浮现。同时,信息本身的不确定性也会导致美国潜意识中的可能对手的构建并导致中美网络空间安全困境的可能产生。避免安全困境的途径不仅依赖于网络主权的相互确认,更在于中美在网络空间的战略互信的建立。

蔡翠红:复旦大学美国研究中心副教授

(本文责任编辑:魏红霞)

---

① Kenneth G. Lieberthal & Peter W. Singer, "Cybersecurity and U. S.-China Relations," February 23, 2012. Brookings Institution Website, available at: http://www.brookings.edu/papers/2012/0223_cybersecurity_china_us_singer_lieberthal.aspx.

② Jason Fritz, "How China Will Use Uyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*, Vol. 8, Issue 1(2008), Article 2, pp. 28～80, available at: http://epublications.bond.edu.au/cm/vol8/iss1/2.

③ 沈逸:《数字空间的认知、竞争与合作:中美战略关系框架下的网络安全关系》,载《外交评论》2010 年第 2 期,第 41 页。