《美国研究》2013年第3期

中美关系中的网络安全问题[①]

汪晓风

〔内容提要〕网络安全问题源于网络空间日益重要的经济价值、外交用途和军事意义。网络安全问题正逐步改变美国对国家安全威胁的总体判断，并促使其国家安全战略转型。中美关系中，网络安全已经扩展到经济和贸易、政治与外交、军事与安全等诸多领域。国际上，中美围绕网络安全治理的原则、规范和主导权展开竞争，呈现出多层博弈和阵营分化的趋势。网络安全问题凸显了中美关系中竞争和对立的一面，其重要性的上升或将挑战九一一以来中美合作的战略基础，对中美发展新型大国关系产生不利影响。中国应从战略高度认识和定位网络安全问题，从增强国际竞争力的角度发展网络空间实力，推动中美在网络安全问题上的共同利益和合作共识。

关键词：美国外交 网络安全 中美关系

当前，网络安全已成为国际社会面临的又一全球性公共问题，引发中美两国政府的高度关注。美国不断提升网络安全在国家安全战略中的地位，最新发布的《情报界安全威胁评估报告》将网络威胁置于美国面临的各类国家安全威胁之首。[②] 中国也将网络空间安全与海洋、太空安全并重，提出要从战略高度予以重视。[③]

网络安全已扩展到中美关系的经济与贸易、政治与外交、军事与国防等各领域。美国指责中国的互联网访问限制及内容审查政策，认为美国企业在华业务因此受阻，

---

① 感谢《美国研究》匿名评审专家指出的问题和修改意见。

② U.S. Intelligence Community, *Worldwide Threat Assessment of the U.S. Intelligence Community*, Apr. 18, 2013, available at: http://www.intelligence.senate.gov/130312/clapper.pdf, p.1.

③ 《中国共产党第十八次全国代表大会文件汇编》，北京·人民出版社2012年版，第39页。

美国还以国家安全为由限制中国信息技术企业在美销售和投资活动。中国对美国通过互联网途径传播价值观、干预中国内部事务、影响中国社会政治进程等问题保持警惕。双方都指责对方进行网络攻击、发展网络武器和推动网络空间军事化。

在国际层面，中美各自倡导的网络空间安全行为规则也已形成竞争态势。中俄等国在联合国发起的"信息安全国际行为准则"被美方拒绝。美日欧强调不受限的网络空间开放、信息自由流通等主张被中国及其他发展中国家视为对互联网主权的干涉，将对本国社会政治稳定形成威胁。国际社会在网络安全问题上跟随中美而"立场分野"的现象已经显现。

这些都对中美发展以"平等互信、包容互鉴、合作共赢"为核心的新型大国关系构成挑战。那么，网络安全如何发展为中美关系中的重要议题？网络安全问题在中美关系中哪些领域引发矛盾和冲突？网络安全问题对中美关系产生了怎样的影响？本文拟对这几个问题予以分析。

一 概念界定及网络安全问题的由来

网络安全问题源于网络空间的迅速成长及其对社会各领域的全面渗透，网络空间不断增长的财富价值、世界经济社会运行与网络空间的相互依赖、网络空间整体安全的防护需求是网络安全问题产生的主要根源。

（一）网络安全的概念

分析网络安全，首先面临的问题就是如何界定这个概念。[①] 由于研究领域、观察角度和追求目标的不同，对于网络安全的含义会有不同理解。国际电信联盟曾推荐了一个工作定义，"网络安全是用以保护网络环境和机构及用户资产的各种工具、政策、安全理念、安全保障、指导原则、风险管理方式、行动、培训、最佳做法、保证和技术的总和"。[②] 这一表述侧重技术和管理需求，其目标主体是网络整体环境，包括各类信息基础设施、机构及用户资产。美国 1999 年国家安全战略报告中首次使用"网络安全"一词，之后陆续发布多份关于或包含网络安全的战略和政策文件，但都没有明

① 本文所指网络安全对应的英文表述是 Cybersecurity 或 Cyberspace Security，指涉对象是网络空间。

② Telecommunication Standardization Sector of ITU, *Recommendation X.1205: Overview of Cybersecurity, Data Networks, Open System Communications and Security/Telecommunication Security*, Apr. 2008, p. 2, available at: http://www.itu.int/rec/T-REC-X.1205-200804-I.

确界定这一概念。[①] 这表明美国决策层对网络安全的认识仍不统一，或者有意保持战略模糊，以便在具体政策上采取有利的解释。

网络空间迅速发展带来的一个直接挑战即如何维持其有效运转。这种有效性既包括整个网络环境的连通、稳定和安全，也包括数据处理、存储和传递的完整、保密和安全。这个意义上的网络安全重点是降低网络环境存在的各种风险、防范网络活动面临的各种威胁，其目标一般被归纳为信息系统安全三原则：保密性(Confidentiality)、完整性(Integrity)和可用性(Availability)。[②] 网络环境和网络活动面临的各种风险或威胁都可划分为对应类别，如保密性涉及国家机密、知识产权、商业机密、账户信息等。而可用性威胁既有如地震、海啸等自然灾害对通讯电缆的破坏，也有分布式拒绝服务(Distributed Denial of Service，DDos)等人为攻击，一些国家设置的网络防火墙有时也被视为可用性威胁。[③]

一般而言，对于技术层面共同面临的风险或威胁，各国政府、互联网企业、国际和非政府组织等利益攸关方较易达成共识，形成共同遵守的规则，采取一致的应对措施，各种政策协调也比较容易展开。而各国政府更关注技术变革在政治层面的影响，网络空间的发展及其与各领域的融合为国家安全增加了新的不确定因素。网络环境的可信性、安全与稳定，网络活动的合法、有序与可控，成为国家安全的关注对象。防止源于网络空间的安全威胁或通过网络空间发起的攻击影响经济、政治、军事等其他领域的稳定，也成为国家安全的重要关注。因此，各国政府运用各种国家资源，维护有利于经济发展繁荣、社会政治稳定和军事国防安全的网络环境，防止国内和跨国网络活动对国家安全造成威胁，便构成了国家网络安全的主要内容。

(二)网络安全问题的产生

网络安全的重要性源于网络空间不断增长的技术、经济、社会和政治价值。互联网发端于冷战时期美国应对前苏联核威慑的军事指挥和控制系统，兴起于 20 世纪

---

① 克林顿政府 1999 年发布的《新世纪国家安全战略》(*A National Security Strategy for A New Century*)首次使用网络安全的概念。小布什政府主要将网络安全看作国土安全问题，两份《国家安全战略报告》(2002 年和 2006 年)均未提及网络安全，而是通过《国土安全战略》(2002 年和 2007 年)、《保护网络空间国家战略》(2003 年)中阐述网络安全政策。奥巴马政府的《国家安全战略报告》(2010 年)又将网络安全纳入国家安全范畴，《网络空间的国际战略》(2010 年)全面阐述了美国在网络空间的内外政策。美国国防部《军事及相关术语词典》(*Dictionary of Military and Associated Terms*)2011 年 1 月修订版没有收录"网络安全"词条。

② 这三个基本原则是信息系统安全的经典表述，通常被称为"CIA 三元体"(CIA-Triad)，保密性是指未经授权无法访问系统或取得数据的特性；完整性是指未经授权无法改变数据内容的特性；可用性是指经授权可访问系统并在授权范围内使用数据的特性。

③ 美国《网络空间国际战略》(2011 年)认为"国家级的过滤网和防火墙对互联网的开放、互通、安全和可靠是一种破坏和威胁"。见 U.S. White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011.

90年代美国推动的互联网商业应用，如今基于互联网的网络空间连接着世界几乎每一个角落、运行着亿万个应用，成为世界经济社会运行的基础平台，成为大国博弈和争夺国际事务主导权的重要领域，也成为高价值的攻击目标和各国的防御重点。

1.大数据时代：网络空间不断增长的数据资源成为国家安全的高价值目标。

网络空间的发展不仅是一个数字化（Digitalization）的过程，更是一个数据化（Datafication）的进程。① 数字化将文字、图像、音频、视频等内容换为二进制代码，提高了计算和处理的效率，也扩展了传输的速度和范围。数据化则是人类生活各个方面转化为可量化分析的数据以及网络活动直接产生数据的进程。美国调查机构的一份报告指出，互联网上的数据每年将增长50%，每两年便翻一番，目前世界上90%以上的数据是最近几年才产生的。② 近年来云处理、社交媒体等互联网应用快速发展，更是促使网络数据以惊人速度增长，网络空间逐渐成为一个储量巨大并持续自我增值的数据矿藏，蕴含着人类生产要素新变革的"大数据"（Big Data）时代已经到来。③ 2008年9月，《自然》（Nature）刊出了一组探讨"大数据"的文章。④ 时隔五年，《外交》（*Foreign Affairs*）首次刊载一篇关于大数据的论文，认为"大数据的管理可能成为国家间新的角斗场。"⑤这表明信息化变革已从自然科学领域向社会科学领域及外交领域扩展。特别是那些包含金融、能源、商贸、国防等高价值数据的应用平台或对国家经济社会运行意义重大的网络系统，各国政府已逐渐从战略高度和国家安全的角度予以重点关注。

2.复合相互依赖：世界经济社会运行与网络空间日益密不可分。

罗伯特·基欧汉和小约瑟夫·奈曾指出，信息革命极大地扩展了社会联系渠道，使国际体系更接近于复合相互依赖。⑥ 作为信息革命最重要的成果之一，以互联网为代表的网络技术和应用最近二十年来迅速发展，全面渗透到世界经济、政治、军事

---

① Kenneth Neil Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think about the World," *Foreign Affairs*, May/Jun, 2013, p.28.

② 张意轩、于洋：《大数据时代的大媒体》，载《人民日报》2013年1月17日。

③ "大数据"是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长和多样化的信息资产。参阅网页：http://www.gartner.com/it-glossary/big-data.

④ 这组文章包括：Joi Ito, "Big Data, The Next Google"; Cory Doctorow, "Big Data: Welcome to the Petacentre"; Mitch Waldrop, "Big Data: Wikiomics"; Clifford Lynch, "Big Data: How Do Your Data Grow? "; Felice Frankel, "Big Data: Distilling Meaning from Data"; Sue Nelson, "Big Data: The Harvard Computers"; Doug Howe, Maria Costanzo, "Big Data: The Future of Biocuration"; *Nature*, Vol. 455/No. 7209, Sept. 4, 2008.

⑤ Kenneth Neil Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think About the World," p.35.

⑥ Robert O. Keohane, Joseph S. Nye, Jr., "Power and Interdependence in the Information Age," *Foreign Affairs*, Vol. 77 Issue 5, Sept. Oct. 1998, p.82.

等各个领域，进一步加强了人类社会的相互依赖。自美国政府1993年推出国家信息基础设施计划、[①]1994年发出全球信息基础设施倡议以来，持续20年的全球信息基础设施建设已经铺设了超过10亿公里的光纤网络，连接数以百亿计的固定和移动终端设备。1990年只有25万人使用互联网，2013年全球互联网用户将达27亿。[②]2012年全球电子商务销售额已超过1万亿美元。[③]世界范围的生产、贸易、金融、商业、交流等已经与网络空间高度融合，全球信息基础设施的互联互通已经成为世界经济社会运行的重要基础，一旦发生故障或中断运行，整个国际社会的正常运转都会受影响。从这个意义上讲，网络安全已经成为绝大多数国家、私营部门以及个人必须面对的一个全球性公共问题。

3.从冗余到安全：网络空间整体安全和综合防护需求。

这主要是指以互联网为核心的网络空间安全设计上的缺失，以及国家和社会管理能力的不足。冷战时期美国国防部高级研究计划署（Advanced Research Projects Agency）设计阿帕网（ARPANET）时重点考虑的是以“冗余”（Redundancy）保证连通性，是确保指挥和控制命令能够到达目标而非其具体路径，是整个系统的正常运转而非单个节点的安危。当以阿帕网为雏形的互联网发展成为各国经济社会运行重要基础的网络空间时，单个节点已经不再是可以忽视的因素，一些节点甚至事关国家重大利益。由于开放和匿名的设计理念，网络安全一直是伴随网络空间发展而日益增长的难题。美国情报界的一份报告曾指出美国决策者面临两大难题：“一是如何明确网络攻击的实时归属，即知道谁实施了攻击以及实施者的位置；二是如何管理网络信息技术供应链中的大量脆弱性。”[④]因此，美国、欧盟和中国规划下一代互联网时，都将安全保障列为首要考虑因素。如中国强调在商用部署阶段要确保安全可信，“在公众网络中建立网络与信息安全防护体系，完善国家数字证书管理体系，提升网络安全可信水平”，[⑤]美国国家标准与技术局在一份未来互联网发展的指导意见中着重强调网

---

① 1993年克林顿政府宣布实施国家信息基础设施（National Information Infrastructure，NII）计划，计划用20年时间、耗资2000～4000亿美元，作为美国发展政策的重点和产业发展的基础。

② International Telecommunication Union，“The World in 2013：ICT Facts and Figures，” Feb. 27，2013，available at：http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf，p.2.

③ “Ecommerce Sales Topped $1 Trillion for First Time in 2012，” Feb. 5，2013，available at：http://www.emarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649.

④ “Current and Projected National Security Threats to the United States，” Hearing before the Select Committee on Intelligence of the United States Senate（One Hundred Twelfth Congress Second Session，Jan. 31，2012，available at：http://www.gpo.gov/fdsys/pkg/CHRG-112shrg74790/pdf/CHRG-112shrg74790.pdf，p.14.

⑤ 中国国家发展与改革委员会：《关于下一代互联网“十二五”发展建设的意见》，2012年3月27日，详情参见网址：http://www.sdpc.gov.cn/zcfb/zcfbtz/2012tz/W020120329402141091330.pdf，第8页。

络行为归属的问题，并考虑在下一代网络的基础协议中加入身份识别功能。①

二 中美双边关系中的网络安全问题

目前，中美双边关系中的网络安全问题主要体现在围绕经贸关系中的市场准入和窃取商业机密、政治外交关系中的信息传播和网络控制、军事安全关系中的网络空间进攻与防御能力建设等一系列政策和事件而产生的争议和冲突。

（一）嵌入与窃取：中美经济贸易关系中的网络安全问题

1.中美都担忧对方企业在本国的经营活动可能危及国家安全而加以市场准入限制。

对中国而言，20世纪90年代以来中国互联网的发展吸引了许多美国知名信息技术公司来华投资，开展硬件设备制造、软件产品研发、电子商务运营等业务，其中有“八大金刚”之称的思科、IBM、谷歌、高通、英特尔、苹果、甲骨文、微软等一度占据网络设备、操作系统、数据平台、个人终端、搜索引擎等产品和服务市场的主要份额。近年来中国市场和政策的变化对美国企业形成了挑战：一方面，随着中国本土企业的崛起，市场竞争日趋激烈，2010年谷歌将其搜索业务退出中国，很大程度包含竞争失利的因素。② 然而谷歌却归咎于中国的网络审查政策，美中经济与安全评估委员会认为“中国的网络审查实际上是一种贸易壁垒，削弱了美国企业开展业务的能力。”③美国政府多次就谷歌事件指责中国，还向世界贸易组织起诉，称中国的互联网政策违反贸易规则。④ 另一方面，随着思科网络设备、微软操作系统等被发现存在产品漏洞及后门问题，以及谷歌和微软等企业被披露依据《爱国者法案》(PATRIOT Act)向美国

---

① Tanya Brewer, “Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop,” *U.S. National Institute of Standard and Technology*, Feb. 2013, available at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7916.pdf.

② 2009年7月，中国搜索引擎市场上，各搜索品牌的首选份额百度占77.2%，谷歌占12.7%（同比下降3.9%）。同期全球搜索引擎市场上，谷歌的市场份额为67.5%，百度为7.0%。数字对比清晰显示了谷歌在中国市场上的失利。见中国互联网络信息中心：《2009年中国搜索引擎用户行为研究报告》，2009年9月，第16、30～31页。应当指出，谷歌仅是将其搜索引擎业务退出中国，迄今仍在中国市场开展诸如地图、翻译、工具栏、移动操作系统等业务，因此，笼统的说“谷歌退出中国”并不严谨。

③ USCC, “2010 Report to Congress of the U.S.-China Economic and Security Review Commission,” Oct. 29, 2010, available at: http://origin.www.uscc.gov/sites/default/files/annual_reports/2010－Report－to－Congress.pdf.

④ “Promoting Global Internet Freedom,” Hearing before U.S. House Committee on Foreign Affairs, Dec. 8, 2011, available at: http://www.gpo.gov/fdsys/pkg/CHRG－112hhrg71621/pdf/CHRG－112hhrg71621.pdf, p.18.

政府提供用户信息，[①]这引起了中国对关键基础设施过于依赖国外产品的警觉和对发展自主知识产权及本土信息技术产品的重视，并明确提出未来中国信息基础设施建设要以本土企业和产品为主导。[②] 2013 年 6 月美国中央情报局前雇员爱德华·斯诺登(Edward Snowden)曝光美国国家安全局通过"棱镜计划"接入一些美国互联网公司的数据服务器，对全球网络空间进行长期和系统性的网络监控和入侵活动，而中国是其重点目标。这进一步显示了中国建立自主可控的网络基础设施和发展有效管辖的信息网络平台的必要性和紧迫性。

美国政府则以网络安全为由，认定中国企业的产品有代码嵌入风险，并通过立法或行政措施，限制中国企业在美国市场的经营活动。如联想集团、华为、中兴在个人电脑市场、通信设备、网络设备等产品与服务市场与 IBM、思科等美国公司展开竞争，扩展了市场份额。美国众议院情报委员会竟认为中兴和华为进入美国市场的意图可疑，这些公司与中国政府联系过于紧密，可能为中国政府从事间谍活动和网络窃取提供帮助，从而对美国国家安全产生威胁，故建议美国政府禁止这两家公司获得任何美国敏感网络的接入权，并禁止其收购美国资产。[③] 奥巴马政府《2013 财年综合继续拨款法案》(*Consolidated and Further Continuing Appropriations Act, 2013*)第 516 条款规定"未经联邦调查局或相应机构许可，美国航天局、司法部、商务部、国家科学基金会等部门不得购买中国相关企业生产、制造或组装的信息技术设备"。[④] 尽管世界贸易组织政府采购协议允许缔约方出于国家安全需要采取特定的针对供应商的限制条件，但该条款把矛头指向所有中国企业，美国对中国企业的疑虑和担忧可见一斑。

2.美国确信中国政府和企业合谋窃取其企业机密而蒙受巨大经济损失。

近年来美国频频指责中国政府参与或支持针对美国企业的网络攻击和窃密活动，并将获取的商业机密和知识产权资料交给中国企业，提高了中国企业的竞争能力，由此造成美国巨大的经济损失。根据网络司令部的估算，美国企业每年因网络窃

---

① Zack Whittaker, "Google Admits Patriot Act Requests," *ZDNet*, Aug. 11, 2011, available at: http://www.zdnet.com/blog/igeneration/google-admits-patriot-act-requests-handed-over-european-data-to-u-s-authorities/12191.

② 苗圩：《我国互联网行业的发展与管理——在互联网行业发展与管理研讨班上的讲话》，2012 年 11 月 22 日，参见网页 http://www.miit.gov.cn/n11293472/n11294464/n14835886/15025545.html。

③ U.S. House Permanent Select Committee on Intelligence, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," Oct. 8, 2012, available at: http://intelligence.house.gov/press-release/investigative-report-us-national-security-issues-posed-chinese-telecommunications.

④ "U.S. Public Law 113～116: Consolidated and Further Continuing Appropriations Act, 2013," Mar. 26, 2013, available at: http://www.gpo.gov/fdsys/pkg/PLAW-113publ6/pdf/PLAW-113publ6.pdf, p.273.

密造成的损失达3000亿美元,[①]而"中国是最积极和顽固的网络入侵者"。[②] 2013年2月,美国网络安全公司曼迪昂特(Mandiant)的一份报告详尽描述了中国黑客发起针对美国一百多家企业的网络入侵和窃密行动,并断定中国军方参与了这些行动。[③]在美国政府和公众看来,曼迪昂特报告包含比较完整的证据链,有较高可信度。其后,美国政府公开指责中国政府参与和支持针对美国企业的网络窃密活动。美国贸易代表办公室《特别301报告》(*Special 301 Report, 2013*)引用曼迪昂特报告,称中国入侵美国的商业系统的主要目标是窃取工业秘密。[④] 指责中国的同时,美国坦承自己也从事广泛的网络间谍和网络攻击活动,但并不认为有何不妥,因为"美国从不窃取商业或技术秘密。"[⑤]

经贸关系一向被喻为中美关系的"压舱石"和"稳定器",近年来随着中国经济规模的发展和结构的变化,中美经贸关系的互补性逐渐下降,而在汇率、知识产权保护、市场壁垒等方面的竞争性正在上升。网络安全问题增加了中美在经贸领域发生摩擦的机率,"已经成为对两国经济关系日益严重的挑战",[⑥]这一定程度上侵蚀了经贸关系在中美关系中的稳定器作用。

(二)塑造与控制:中美政治外交关系中的网络安全问题

中国实行安全与自由相平衡的网络空间管理政策,坚持境内互联网的主权管辖。而美国指责中国限制互联网自由,试图通过互联网途径影响中国社会政治进程,并支持技术手段突破中国对互联网访问的限制。

1.美国强调不受限制的互联网自由,试图通过互联网途径影响中国社会舆论,对中国社会政治稳定构成威胁。

美国向来强调"开放社会"对于塑造有利国际环境的作用,"作为一个最主要的民

---

① Dutch Ruppersberger, "Opening Statement at Hearing on Chinese Telecommunications Investigation," U.S. House of Representatives Permanent Select Committee on Intelligence, Sept. 13, 2012, available at: http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/09122012DutchOpening.pdf, p. 2.

② U.S. Office of National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009~2011*, Oct. 2011, available at: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf, p.5.

③ Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," Feb. 19, 2013, available at: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

④ Office of the United States Trade Representative, "2013 Special 301 Report," May 1, 2013, available at: http://www.ustr.gov/about-us/press-office/reports-and-publications/2013/2013-special-301-report.

⑤ Richard McGregor, "U.S. Says China Is Stepping up Cyber War," *The Financial Times*, May 7, 2013.

⑥ Tom Donilon, "The United States and the Asia-Pacific in 2013," *Remarks at The Asia Society*, Mar. 11, 2013, available at: http://iipdigital.usembassy.gov/st/chinese/texttrans/2013/03/20130314144171.html.

主国家，美国一直在努力打开各个封闭社会”。[①] 互联网兴起之初，约瑟夫·奈(Joseph Nye)就认为信息网络为民主国家间安全对话提供有效工具的同时，也为与非民主国家和地区的民众进行直接沟通以培养民主意识提供了有力工具。[②] 冷战结束后，意识形态差异不再是中美关系发展的主要障碍。但美国坚持中国尽管不再是一个封闭社会，但仍是一个信息不自由及须以美国价值观“塑造”的社会，故试图通过信息传播来改变中国社会的价值观。互联网可以提供多样化、快捷、低成本的信息传播功能，自然成为美国“塑造”中国社会的重要途经。美国将其倡导的开放社会、自由表达等理念引入网络空间，指责中国的互联网管理政策，并通过支持网络技术公司开发突破网络防火墙的软件并分发给中国网络用户。当社交媒体显示其在引导和塑造舆论、参与和吸引互动等方面的公共外交价值时，美国国务院及其驻华使领馆加入中国主要社交媒体，积极发布信息及与网民互动，展开各种形式的网络公共外交活动。这些行为引起了中国的警觉，尤其2010年中东北非颜色革命中，社交媒体等互联网途径在引导公众舆论、组织政治参与和反政府运动中的巨大影响力，形成对社会稳定和政治制度的威胁，中国进一步加强了网络内容管理。

2.中国强调互联网管理主权，美国认为对网络空间自由和全球可连通性造成破坏。

中国政府认为境内互联网属于主权管辖范围，中国的互联网主权应受到尊重和维护。中国实行互联网信息安全流动基础上的自由流动，主张“合理运用技术手段遏制互联网上违法信息的传播，发挥技术手段的防范作用，遏制违法信息对国家信息安全、社会公共利益和未成年人的危害。”[③]基于这些认识，中国制定了一系列互联网内容发布和管理的政策，[④]设置了内容审查及防火墙系统，对非法信息进行过滤，限制访问一些国际网站。对此美国从互联网自由和网络空间的可互通性两方面加以指责，并认为这实质上损害了美国在网络空间自由行动的权利。如为加强提供互联网信息发布平台企业的主动性，中国实行严格的行业自律政策，[⑤]对此，尽管美国也承认各国有独立制定互联网公共政策的主权，但仍然认为中国“扩大政府权力，由政府

---

① John Arquilla, David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND, 1998, p.472.

② Joseph Nye and William Owens, "America's Information Edge," *Foreign Affairs*, Mar/Apr, 1996, pp.20～36.

③ 国务院新闻办：《中国互联网状况》，北京·人民出版社2010年版，第16、20页。

④ 这些法规如《全国人大常委会关于维护互联网安全的决定》(2000年)、《中华人民共和国电信条例》(2000年)、《全国人大常委会关于加强网络信息保护的决定》(2012年)等。

⑤ 如2002年10月131家互联网企业签署《中国互联网行业自律公约》。2011年11月39家网站和互联网企业负责人一致同意加强“自我管理、自我约束、严格自律”。华春雨：《发展健康向上的网络文化》，载《人民日报》2011年11月7日。

为互联网制定条例规范，不仅会损害人权和信息自由流通，而且会破坏网络的互通性。"①

（三）拒止与威慑：中美军事安全关系中的网络安全问题

中美都在认真考虑网络空间发生冲突及战争的可能性，发展网络空间作战和防御能力，但均表示要避免网络空间军事化。

1.发展网络空间作战能力。

根据美国国防部《军事及相关术语词典》的定义，网络空间作战（Cyberspace Operations）是"在网络空间或通过网络空间运用网络能力达成军事目的，包括运行和保护全球信息网格的计算机网络作战和行动。"②早在克林顿政府时期，隶属军方的情报机构就开始筹划网络攻击能力。③ 小布什政府时期美军又将网络空间列为与陆、海、空、太空同等重要的战略空间，④并在"先发制人"军事战略指导下，开发网络作战武器，加强网络进攻能力。奥巴马政府进一步将网络空间纳入作战领域，在此基础上加强军事力量的组织、训练和装备，以确保国防部充分运用网络空间的潜力，以及采取有效军事行动的能力。⑤ 迄今，美军各军种都建立了各自的网络空间作战力量，并由网络司令部统一负责协调。⑥ 美军网络司令部行政上隶属于战略司令部，表明美军将网络空间视作全球性的作战行动领域。但美国仍没有在网络空间作战对象的界定和作战方式的选择方面取得实质性突破，迄今可见到的最主要进展是美国空军正式将六类网络工具列为武器。⑦ 而是否将对电力、供水、电信等基础设施的网络攻击视作战争行为仍存在争议。

中国总体上是以信息化和网络化促进军队训练水平和作战能力。自 1998 年迄今中国共发布了七份国防白皮书，1998 年首份白皮书未出现信息网络相关内容，2000～2008 年五份白皮书主要强调依托国家信息基础设施、综合运用各种信息技术

---

① Hillary Rodham Clinton, "Remarks at Freedom Online Conference," Dec. 8, 2011, available at: http://www.state.gov/secretary/rm/2011/12/178511.htm.

② U.S. Department of Defense, *Dictionary of Military and Associated Terms*, Nov. 8, 2010, p.93.

③ Jeffrey T. Richelson, Malcolm Byrne, "When America Became a Cyberwarrior: A Secret Document Shows the NSA Has Been Planning Attacks Since the Clinton Years," *Foreign Policy* Website, Apr. 26, 2013, available at: http://www.foreignpolicy.com/articles/2013/04/26/when_america_became_a_cyberwarrior_nsa_declassified.

④ U.S. Department of Defense, *The National Defense Strategy of the United States of America*, Mar. 2005.

⑤ U.S. Department of Defense, *Strategy for Operating in Cyberspace*, Jul. 2011.

⑥ 美军各军兵种的网络部队包括陆军网络司令部、海军第十舰队、空军第二十四航空队、海军陆战队网络司令部、海岸警卫队网络司令部。

⑦ Andrea Shalal-Esa, "Six U.S. Air Force Cyber Capabilities Designated 'Weapons'," Apr. 8, 2013, *Reuters*, available at: http://www.reuters.com/article/2013/04/09/net－us－cyber－airforce－weapons－idUSBRE93801B20130409.

手段，加强网络化训练水平，提升军事训练科技含量。2010 年白皮书首次提出要密切关注其他大国的网络作战能力。这几份白皮书都没有发展网络空间作战能力的表述，是否表明中国军事发展规划中不包含网络作战内容？由于外界对中国军事透明化的疑虑，及美国对中国发展网络作战能力的渲染，如曼迪昂特报告指中国军方参与或支持多项网络黑客行动，[①]其后美国政府多份正式文件引用该报告对中国军队涉及网络攻击的内容，显然美国确信中国是在大力发展网络空间作战能力。从另一个角度看，中国军方学者自 20 世纪 90 年代以来对信息战、心理战、网络战等非对称作战进行了大量深入研究，包括从网络空间打击敌方的脆弱性等，也说明中国军方重视网络空间作战的研究和运用。

2.发展网络空间防御能力。

美军网络空间的防御范围涵盖了整个网络空间。美军强大的作战和指挥能力很大程度上依赖于全球信息基础设施的稳定、连通和自由进入。美军在全球几十个国家运行着 1.5 万个网络和 700 万台计算机，[②]利用网络空间开展军事、情报、商务活动以及各种军事行动的指挥控制。《网络空间行动战略》(2011 年)着重指出美军负有保护军事网络、国家信息基础设施和全球信息基础设施的职责，该战略将网络空间界定为作战领域，国防部以此为基础进行组织、培训和装备，以应对网络空间的复杂挑战和巨大机遇。美军将变被动防御为主动防御，更加有效地阻止、击败针对美军网络系统的入侵和其他敌对行为。加强与其他政府部门及私人部门的合作，在保护军事网络安全的同时，加强国家重要基础设施的网络安全防护。同时还要加强与美国的盟友及伙伴在网络空间领域的国际合作。[③] 美国国防部常务副部长威廉·林恩(William J. Lynn III)称美军在网络空间的任务重在防御而非进攻，目的是打掉因攻击获得的利益，而前参谋长联席会议副主席詹姆斯·卡特赖特(James Cartwright)则批评该战略“过于防御性，过于可预知性”。[④]

中国认识到网络空间的国际军事竞争正在形成，因此将发展网络空间防御作为军队建设的重要任务。2010 年国防白皮书指出，一些大国制定网络空间战略，发展包括网络空间在内的全球快速打击能力，增强网络作战能力，抢占新的战略制高点。中国应将网络空间安全利益纳入新时期中国国防的目标和任务，以全面维护国家主

---

① Mandiant Intelligence Center, "APT1: Exposing One of China's Cyber Espionage Units," Feb. 19, 2013, available at: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

② U.S. Department of Defense, *Strategy for Operating in Cyberspace*, Jul. 14, 2011, available at: http://www.defense.gov/news/d20110714cyber.pdf, p.7.

③ U.S. Department of Defense, *Strategy for Operating in Cyberspace*, pp.5~9.

④ Ellen Nakashima, "U.S. Cyber Approach 'Too Predictable' for One Top General," *Washington Post*, Jul. 15, 2011.

权、安全、发展利益。[①] 2013 年《中国武装力量的多样化运用》白皮书再次重申上述主张。[②] 这显示中国军方着重发展网络防御能力，而美国军方认为信息封锁(Information Blockade)和信息控制(Information Dominance)是中国网络防御能力的核心。[③] 但中国军方并没有将公共网络安全纳入军事保障任务，这是与美军一个很大的区别。

军事关系是中美关系中最敏感和最脆弱的环节。近年来中国军力的持续增长引发了美国的担忧，如何继续维持总体军力和各领域的绝对优势是未来美国军事战略的重点。在网络空间，美军认为并没有绝对优势，因而以防范、威慑及规制等方式限制中国网络空间作战能力的增长就成为其重要目标。然而美国并不愿意通过平等对话解决网络空间军事化的共同担忧，有观点认为中美网络空间的竞争和冲突可能导致中美网络空间安全困境的产生，并可能会引发网络军备竞赛，美国网络战研究专家约翰·阿奎拉(John Arquilla)甚至断言中美已进入所谓"凉战"(Cool War)网络冲突状态。[④]

三 网络安全国际治理与中美竞争

国际上，中美围绕网络安全国际治理的多边互动角力正在展开，包括网络空间基础资源的控制和分配、网络安全治理规则的制定等。中美原则立场的差异和国际社会的阵营分化将对网络安全治理的未来走向产生决定性影响。

(一) 资源与控制权之争

当前网络安全国际治理的制度化水平较低。基本原则和准则存在分歧、权力分配高度不均的领域难以形成国际制度，这是国际机制研究的一个基本判断。[⑤] 网络空间正是利益主体多元化、权力分布高度不均的国际共享领域。美国控制了根服务器、地址资源等最重要的网络空间资源。如 IPv4 架构下可分配约 43 亿个 IP 地址，美国有 15.67 亿个，中国仅有 3.3 亿个。[⑥] 不仅拥有最多的基础资源，美国还掌握关

---

① 国务院新闻办公室：《2010 年中国的国防》白皮书，2011 年 3 月。

② 国务院新闻办公室：《中国武装力量的多样化运用》白皮书，2013 年 4 月。

③ U.S. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China of 2013*, May 2013, available at: http://www.defense.gov/pubs/2013_china_report_final.pdf, p.32.

④ John Arquilla, "Cool War: Could the Age of Cyber Warfare Lead Us to A Brighter Future?" *Foreign Policy*, Jun. 15, 2012, available at: http://www.foreignpolicy.com/articles/2012/06/15/cool_war.

⑤ Stephen D. Krasner, "Global Communications and National Power: Life on the Pareto Frontier," *World Politics*, Vol. 43 Issue 3, Apr. 1991, p.337.

⑥ 中国互联网信息中心：《互联网发展信息与动态》，2013 年 3 月。参见网页 http://www.cnnic.org.cn/hlwfzyj/hlwfzzx/qwfb/201304/W020130424624101060588.pdf，第 4 页。

键资源的分配权。目前整个互联网域名及地址分配由“互联网名称与数字地址分配机构”(ICANN)管理,“互联网名称与数字地址分配机构”名义上是一个由全球商业、技术及学术专家组成的国际组织,各国政府可委派人员参与政府咨询委员会,但关键性权力如域名控制和否决权仍由美国商务部通过与“互联网名称与数字地址分配机构”的协议保持,“从某种意义上而言,‘互联网名称与数字地址分配机构’就是美国对互联网实施控制的工具”。①

美国占有网络空间基础资源和控制分配权,经济收益之外,还能够获得广泛的安全收益。其一,作为网络空间的全球枢纽,美国可以在其境内通过国内立法监控全球数据流动,获取情报信息,应对通过网络途径发起的敌对行动,美国还可以将这些情报与同盟和伙伴分享,加强其在网络安全和其他安全领域的主导权;其二,拥有域名解析的控制权,美国可以令对其国家安全构成威胁的机构、组织的网站甚至整个国家的网络无法访问,如伊拉克战争期间,美国以伊拉克局势动荡为由,敦促“互联网名称与数字地址分配机构”终止其国家顶级域名的解析,伊拉克因此从网络空间消失。②其三,美国还可以通过操作根服务器,封锁特定 IP 地址,对抗网络攻击。如 2008 年俄罗斯和格鲁吉亚冲突期间,技术专家通过瑞典的根服务器有效阻截了针对格鲁吉亚互联网的大规模拒绝服务式攻击。

中国认为各国都有平等参与国际互联网基础资源管理的权利,应在现有管理模式的基础上,建立一个多边透明的国际分配体系,合理分配互联网基础资源。③ 国际社会对美国独揽互联网控制权也多有不满,要求美国将部分控制权移交国际机构。美国政府也面临国内要求维持控制权的压力,2005 年 11 月信息社会世界峰会期间,国会以 423 票对 0 票通过决议要求总统反对任何将互联网控制权移交给联合国或其他国际组织的举措。④ 2012 年 12 月国际电信世界大会期间,国会再以 397 票对 0 票通过决议反对由外国或国际组织管理互联网。⑤ 面对内外压力,美国政府在保持实质控制的基础上作出有限让步,如赋予 ICANN 更多自主权。

(二)治理模式之争:多利益攸关方与政府间合作

---

① Kenneth Neil Cukier, “Who Will Control the Internet?” *Foreign Affairs*, Vol.84, No.6, Nov./Dec. 2006, p.7.

② 朱伟、王珏:《域名解析:一个需要破解的安全瓶颈》,载《解放军报》,2006 年 4 月 4 日。

③ 国务院新闻办公室:《中国互联网状况》,第 25 页。

④ U.S. Senate, 109th Congress, “S.Res.316-A Resolution Expressing the Sense of the Senate that the United Nations and Other International Organizations Shall Not Be Allowed to Exercise Control Over the Internet.” Nov. 18, 2005, available at: http://beta.congress.gov/bill/109th-congress/senate-resolution/316.

⑤ U.S. Senate, 112th Congress, “S.Res.446-Bill Aimed at Preventing Foreign Regulation of Internet.” Dec. 5, 2012, available at: http://beta.congress.gov/bill/112th-congress/senate-resolution/446.

美国一直强调理想的网络安全治理模式是维持现有基本架构不变，即多利益攸关方(Multi-Stakeholder)模式，这些利益攸关方包括各国政府、私营部门和国际组织。美国认为，互联网天生具有国际特性，不能由各国政府控制，政府的权威限于其边界，政府的作用应限于国内公共政策的制定。互联网发展的主要动力来自全世界私营部门，包括服务器和网络的所有者和操作者、域名注册商、地区 IP 地址分配组织、标准制定组织、互联网服务提供商和互联网用户，这些私营部门理当在互联网治理方面发挥主要作用。而政府间组织如"互联网名称与数字地址分配机构"政府咨询委员会、互联网治理论坛(Internet Governance Forum，IGF)、国际电信联盟、世界知识产权组织、经济合作与发展组织(OECD)并没有直接管理或控制互联网的权力，只能对未来互联网的国际政策方面发挥影响。① 可见美国的多利益攸关方模式中发挥核心作用的是私营部门，而互联网领域最有影响力的私营部门主要来自美国，所以本质上仍然是要维持美国对互联网的有效控制。

中国对于治理主体的多元化并无异议，但希望国际组织获得更多的主导权，即将网络空间的资源分配和政策协调置于一个或多个政府间机构之下，从而为国家在网络安全治理中谋求更大的作用。中国认为各国网络空间彼此相连，分属不同的主权管辖范围，没有一国可以独善其身，更不能靠一国之力确保本国的信息和网络空间安全，需要通过加强国际交流与合作共同应对。制定信息和网络空间国际规则，是当前维护各国信息和网络空间安全的紧迫课题，而"作为最具普遍性和权威性的国际组织，联合国是制定上述规则的最合适平台"。② 联合国也认为"互联网已发展成为一个全球性公共设施，互联网的国际管理应是多变、透明和民主的，由政府、私营部门、民间团体和国际组织的全面参与"，③并积极推动国际电信联盟获得互联网治理的主导权。但无论是联合国还是中国的主张，都遭到了美国政府的坚决反对。

2011 年 9 月，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦四国共同向联合国大会提交了一份《信息安全国际行为准则》议案，中国提出互联网治理应遵循"和平、主权、统筹协调信息自由流动与安全流动、合作、公平发展"五大原则，强调"主权国家是有效实施国际信息和网络空间治理的主体"，"充分尊重各利益攸关方在信息和网络空

---

① Lennard G. Kruger, "Internet Governance and the Domain Name System: Issues for Congress," Jan. 2, 2013, p.6, available at: http://www.fas.org/sgp/crs/misc/R42351.pdf, p.3.

② 王群：《中国特命全权大使在联大一委关于信息和网络空间安全问题的讲话》，2011 年 10 月 20 日，参加中国外交部网页 http://www.fmprc.gov.cn/mfa_chn/wjdt_611265/zwbd_611281/t869443.shtml。

③ WSIS, "Building the Information Society: A Global Challenge in the New Millennium," Dec. 12, 2003, available at: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!! PDF-C.pdf, p.6.

间的权利和自由”，[①]希望联合国大会就此展开讨论。美国对该议案反应冷淡，国会众议院甚至要求美国直接予以否决，因为“该行为准则为政府排它性地控制互联网资源寻求国际合法性，并反对当前确保互联网繁荣的多利益攸关方模式，对互联网信息自由流动构成威胁，将损害自由表达的权利，有利于政府控制互联网内容，试图在违反国际法的情况下保持政治稳定”，“美国常驻联合国代表应当反对该议案”。[②] 可见虽然中美都强调多利益攸关方的网络安全治理模式，但对各利益攸关方作用和地位的认识存在根本差异。

（三）国际阵营的分化

由于美国坚持控制网络空间基础资源，对多利益攸关方模式的理解与各国政府及国际组织存在差异，其在网络空间安全上的政策主张也面临获取国际支持的压力。为此，美国提出要建立网络空间国际战略上的“志同道合”（Like-minded）的伙伴关系，团结传统盟国、联合在基础资源分配、信息内容管理、网络空间安全等议题上立场一致的伙伴、胁迫或诱使利益诉求不明的中小国家。“美国需要制定一项战略，以塑造有利的国际环境，聚集在领土管辖权、主权责任及武力使用规则等问题上持有共同立场的国家。”[③]美国“将与‘志同道合’的国家一起，努力建立一个人们所期望的环境或相关行为准则，这种环境将符合我们的外交与国防政策并能指导我们的国际伙伴关系。”“我们将通过外交和联盟关系，寻求将尽可能多的利益攸关者纳入这一网络空间构想，因为这将产生巨大的经济、社会、政治和安全效益。与国内外的私营部门开展富有成效的合作，将对我们的努力起到支撑作用。”[④]在互联网基础资源的分配上，美国得到了英国、日本和瑞典三家拥有根服务器的国家的支持。美国还与日本举行网络安全综合对话，商谈应对网络入侵，并建立网络空间行为准则，以争夺网络空间安全的国际规则的主动权。

中国则以握有较大发言权和主动权的国际平台为主展开凝聚共识的努力。迄今中国已在东南亚国家联盟（ASEAN）、上海合作组织（SCO）、金砖国家（BRICS）等国际组织框架内就网络安全问题进行多边磋商，协调政策，签署了《中国-东盟电信监管理事会关于网络安全问题的合作框架》（2009 年）、《上合组织成员国保障国际信息安

① 王群，前引文。

② U.S. House, 112th Congress, “H.RES.628-Expressing the Sense of the House of Representatives That the United States Should Preserve, Enhance, and Increase Access to An Open, Global Internet,” Apr. 19, 2012.

③ U.S. White House, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” May 29, 2009.

④ U.S. White House, “International Strategy for Cyberspace: Prosperity, Security, and Openness in ANetworked World,” May 2011.

全政府间合作协定》(2009 年)。2012 年 9 月,中国、俄罗斯、巴西、南非互联网主管部门共同举办首届新兴国家互联网圆桌会议,议题涉及"互联网发展及治理"、"网络空间安全"、"新兴国家互联网领域的交流与合作"。2012 年 12 月还举办了中韩互联网圆桌会议,双方表示要加强国际互联网治理立场协调。中国在这些双边和多边的渠道中逐渐积累了一些政策共识,同时以这些共识为依托,在更广泛的国际平台如联合国大会、国际电信联盟、世界知识产权组织等政府间国际组织中寻求国际支持。

2012 年 12 月,国际电信世界大会就国际电信联盟新电信规则进行讨论,网络安全和互联网治理也在议题之列。会议之前,美国即表示反对任何对互联网带来更大监管的提案,反对新电信规则包含任何有关互联网的条款,不支持任何有利于内容审查或阻止信息和思想自由流动而拓宽电信规则范围的努力。① 中俄等国希望推动国际电信联盟获得互联网治理更大的权力,为各国政府管理互联网内容争取合法性。突尼斯代表则提请增加保护在线言论自由的内容。在国际电信联盟提供讨论的初稿中,包含了互联网、信息安全、网络犯罪等条款。由于美国坚决反对,新电信规则条约文本未出现互联网条款,并强调"条约并不针对电信涉及内容的方面",大会另通过决议案表示"各国政府都应该在国际互联网管理中发挥同等作用、承担同等责任"。也由于一些国家反对,新电信规则未包含保护网络言论自由的内容。尽管如此,新电信规则出台后,中俄等 89 个主要发展中国家予以签署,而美、加、英、澳等 55 个西方国家拒绝签署。这次大会可谓中美在网络安全等议题上所持立场的一次国际对决,国际阵营的分化也得到充分展现。

四 网络安全问题对中美关系的影响

网络安全问题在中美关系中快速升温,其潜在影响将不亚于九一一事件对中美关系的影响。不同的是,九一一之后美国因反恐需求重新定位其全球战略,促使中美关系合作的一面占据主导,而网络安全问题凸显了中美关系竞争和冲突的一面,将对中美发展新型大国关系形成新的障碍。

(一)对中美关系的影响

目前网络安全问题对中美关系的影响仍然是有限的和局部的,但由于国家利益和原则立场的差异,网络安全问题有可能产生全面和深远的影响。

1.网络安全问题将会促使美国国家安全战略转型,冲击当前中美关系的战略

① Terry Kramer, "on International Telecommunications Conference," Nov. 29, 2012, available at: http://translations.state.gov/st/english/texttrans/2012/11/20121129139303.html.

基础。

美国的政治领导人往往愿意强调甚至夸大国家安全威胁，以获取公众支持，这种现实主义偏好在美国决策圈长期存在。历史上美国国家安全战略的重大转折都是基于对战略威胁改变的判断，换言之，美国国家安全战略转变的过程即是发现新威胁和新敌人的过程。冷战后传统大国军事威胁减弱，国际经济竞争及分配性冲突增加，国家安全概念的模糊性越发明显。① 美国也不断更新国家安全的涵盖范围，经济、环境、恐怖主义等非传统领域纷纷进入其国家安全战略考虑，将网络安全上升到国家安全高度正是这种趋势和思维的结合，也隐含了美国重新定义核心利益和战略威胁的可能性。近年来，“美国对网络安全忧患已经到了白热化的程度”。②

网络安全问题加深了美国对本土安全的担忧。珍珠港事件、九一一事件都是外部力量对美国本土的直接打击，造成了重大人员伤亡和经济损失。“正如第二次世界大战战将美国从孤立主义中唤醒，九一一恐怖袭击再次打碎了美国本土无懈可击的想法。”③美国国内迅速形成共识，促成国家安全战略的重大转变。九一一事件后，美国的战略重心迅速转移至应对国际恐怖主义威胁，对中国实力增长的担忧和改变中国的意愿都降低了，从而加大了中美的合作空间。中美关系的后续发展也印证了这一点，双方务实地看待双边争议和矛盾，妥善地处理台湾、西藏、人权、贸易等敏感问题。但网络安全问题与珍珠港事件、九一一事件的最大差异在于美国对威胁来源的判断。一个严峻的现实是，美国政府和社会公众已经形成一个印象，网络安全是美国国土安全的严重威胁，而中国的网络攻击是这些威胁的主要来源。如前所述，网络安全问题对中美经贸、外交和军事关系都产生了重要的负面影响，这势将冲击当前中美关系稳定发展的战略基础。

2.网络安全问题将促使美国调整对华政策的优先次序，改变当前中美关系的议程。

近年来，中美战略竞争态势日趋明显，各领域矛盾和冲突不断增多。随着网络安全问题越来越受关注，美国行政部门将出台一系列网络安全相关政策，国会也将通过一些网络安全相关立法，这些政策和立法很可能从技术、贸易、政治和安全等方面添加“中国网络威胁”内容。美国情报界《安全威胁评估报告》每年都会对美国国家安全

---

① 罗伯特·基欧汉、约瑟夫·奈：《权力与相互依赖》（第三版，门洪华译），北京大学出版社 2001 年版，第 6～8 页。

② Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations* (Brookings Institute, 2012), p.3.

③ Paul R. Viotti, Michael A. Opheim, Nicholas Bowen eds., *Terrorism and Homeland Security: Thinking Strategically about Policy* (New York: CRC Press, 2008), p.69.

的威胁进行分类排序，2011 年该报告列出的威胁来源榜单为恐怖主义和大规模杀伤性武器的扩散，[①]2012 年该报告中的前三位为恐怖主义、武器扩散、网络威胁，[②]2013 年报告中的前三位为网络威胁、恐怖主义与跨国有组织犯罪、武器扩散。[③] 这种次序的变化必将在中美双边对话机制和议程中得到体现。

近年来，中美处理双边关系的机制不断发展，中美关系正常化以来陆续建立各种层级和形式的双边对话机制已达九十多个，涉及经贸、防务、安全、人权等多个方面。可以预料，随着网络安全热度不断升高，网络安全议题将"嵌入"多个重要的双边对话机制，如中美商贸联委会、战略与经济对话、防务磋商、人权对话等。中美国家元首会晤、官员互访也都回避不了网络安全问题。特别是作为最高层级的双边对话机制，中美战略与经济对话已将网络安全问题纳入议程，并专设中美网络事务磋商小组，[④]意味着网络安全问题已上升到双边关系的战略高度。

（二）对中国的启示

网络安全问题已经与中国国内经济社会运行和发展中美关系密不可分，中国为阐释原则立场进行了大量的努力，但外界对中国的意图和政策仍有很多疑虑。反观美国，全方位的网络安全战略清晰可见，各项政策稳步推进。中国可从中获得有益的启示。

1.重视国内政策的公共支持。

在网络安全问题上，中国偏重于国内经济发展和社会政治稳定的需求，对争取国内和国际共识的关注度不够。网络空间与太空、海洋等全球公共空间相比一个重要的区别是参与主体的多样性，太空及海洋秩序国际治理的主体是各国政府和专业机构，协调国际公共政策涉及面相对较窄。而迄今推动网络空间迅速发展的主体是私营部门，他们在技术、规则和应用方面保持持续创新能力，与网络空间可提供一个政府干预较少的宽松环境密切相关，广大网络用户的参与也是网络空间发展不可或缺的推动力。美国政府强调私营部门的主体地位、反对政府或政府间国际组织管理互联网、坚持互联网的自由访问、保护个人隐私，这些原则立场在美国国内和国际上都

---

① U.S. Intelligence Community, *Worldwide Threat Assessment of the U.S. Intelligence Community*, Feb. 16, 2011, available at: http://www.dni.gov/files/documents/Newsroom/Testimonies/20110216_testimony_sfr.pdf.

② U.S. Intelligence Community, *Worldwide Threat Assessment of the U.S. Intelligence Community*, Feb. 2, 2012, available at: http://www.dni.gov/files/documents/Newsroom/Testimonies/20120202_testimony_wta.pdf.

③ U.S. Intelligence Community, *Worldwide Threat Assessment of the U.S. Intelligence Community*, Apr. 18, 2013, available at: http://www.intelligence.senate.gov/130312/clapper.pdf.

④ John Kerry, "Solo Press Availability in Beijing," Apr. 13, 2013, available at: http://www.state.gov/secretary/remarks/2013/04/207469.htm.

有着较高的支持度。如奥巴马政府虽然认为网络盗版对企业造成了巨大损失，但仍反对国会通过旨在保护网络知识产权的《禁止网络盗版法案》和《保护知识产权法案》，因为这两个法案可能伤害更为重要的个人隐私和整个互联网行业的发展。① 中国拥有最大的互联网和移动通讯用户群体，中国企业的应用创新和竞争能力已开始展现，如电子商务领域的阿里巴巴、社交网络与移动网络相结合的微信、微博等。因此，中国政府要鼓励企业和个人参与网络安全治理的非政府组织，并从培育网络空间国际竞争力的角度给中国信息技术企业和产品以更坚定的支持。

2.有效应对美国就网络安全问题对中国的施压与指责。

一方面要善于利用美国在网络安全问题上的内外矛盾。如美国惯常指责中国政府参与或支持攻击其政府、企业和机构的网络系统，窃取技术和商业机密、军事和战略情报等。然而，2013 年 6 月曝光的"棱镜计划"显示美国对世界各国进行长期和系统的网络监控和情报获取活动，不论是敌对国家、竞争对手还是联盟伙伴概莫能外，面对国际社会的指责，美国以反恐需要、符合国内法律和范围可控等理由加以辩解，还特别强调其网络监控性质不同于中国的技术和商业机密窃取活动。对此，中国可从国际社会的共同关切入手，就"棱镜计划"的国际合法性对美提出交涉，同时将在华美企将属中国管辖范围的网络数据提供给美国政府界定为侵权行为。② 再如美国政府以网络安全为由对中国企业加以市场准入限制，从而在实质上对本国企业予以支持。2012 年美国国会众议院情报委员会发布了有关华为和中兴通讯威胁美国国家安全的报告，③有评论认为思科参与了游说国会对华为展开审查的活动，思科随即发表声明，声称自己并未游说国会，还称与另一家中国企业中兴通讯是合作伙伴而非对手。④ 这反映了美国企业的矛盾心理，既期待中国的市场机会，又希望政府帮忙打压竞争对手，还害怕遭致中国的报复。这种矛盾心理在谷歌、微软、雅虎及未能进入中

---

① 《禁止网络盗版法案》(*Stop Online Piracy Act*，SOPA)和《保护知识产权法案》(*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*，PIPA)得到美国众多知识产权组织和国会议员的支持，但多数互联网企业和网民坚决反对。2012 年国会讨论期间，维基、谷歌、脸谱、优兔、美国在线等互联网企业进行了各种形式的抗议活动，奥巴马也明确表态不支持这两个法案。

② 根据已披露的信息，美国国家安全局"棱镜计划"的依据是《爱国者法案》和《外国情报监视法案》(The Foreign Intelligence Surveillance Act，FISA)，情报部门向外国情报监视法庭提出调查申请，获得许可后，再要求相关互联网公司开放数据服务器访问接口或直接提供数据。因此美国政府一再强调该计划的目标、程序和结果都合法。但如果美国公司将从其他国家获得的用户信息和运行数据交给美国政府，就存在侵犯个人财产权甚至它国主权的问题。

③ U.S. House Permanent Select Committee on Intelligence, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," Oct. 8, 2011.

④ Cisco, "What Cisco Did Was Not Lobbying," *Washington Post*, Oct. 10, 2012, available at: http://articles.washingtonpost.com/2012-10-20/opinions/35500947_1_huawei-cisco-house-intelligence-committee.

国市场的脸谱、推特等公司那里都有所体现。

另一方面要寻找并积累中美之间的共识。中美不仅是世界两大经济体，也是两个最大的互联网国家。中美之间就网络安全治理的原则达成共识，建立共同遵守的网络行为规范是实现网络安全国际治理最重要的基础，一个不包含中美共识的网络安全制度安排必定是不完整的，必将破坏网络空间的统一性并造成国际分裂。应当看到，中美都表示要建立共同遵守的网络空间行为规范，应从双方已形成共识的原则或领域着手，推动更广泛的政策协调。目前中美在共同应对网络安全问题已经有一些机制，取得了一定成效，如2012年国际电信世界大会召开之前，美国代表团团长泰里·克雷默(Terry Kramer)到北京与中国工信部协调立场，着重在网络安全与网络流量管理等问题上交换意见。再如共同打击网络犯罪方面，2012年10月，中国国家互联网应急中心接美国国家互联网应急中心通报，称中国境内一些主机被恶意程序控制正在参与针对美国一家银行和一家大型公司的拒绝服务攻击，中国方面对位于中国境内的IP地址进行了及时处理。[①] 这些合作对于积累中美在网络安全问题上的共同利益和合作共识，有着长期和积极的意义。策略上，曼迪昂特报告也是一个启示，中国应对重要目标受到的网络攻击和相应损失进行跟踪调查，尤其是对来自境外的一些系统性和长期性的网络攻击进行取证分析，形成完整的证据链，在中美有关网络安全问题的争议中，拿出有说服力的证据。

总之，美国提升网络安全问题层级，并以此对中国进行指责和施压，有其国内政治的因素，也有夸大的成分。但毫无疑问，美国有着无可匹敌的国际影响力和强大的问题塑造能力，正如九一一以来，美国迅速将恐怖主义规划成整个国际社会的议程，中美的经贸、军事、外交关系也都增添了反恐内容。美国对网络安全问题的高度关注也将改变国际关系和中美关系的运行轨迹。“世界上没有哪个双边关系比美中关系更能深刻影响未来国际政治。而在这个双边关系中，没有哪个议题像网络安全一样快速升温，并且在很短的时间内造成了种种摩擦。”[②]因此，中国应从战略高度认识和定位网络安全问题，重视其对中美关系的长期影响。2013年6月中美元首加州会晤就网络安全问题达成重要共识，即要在合作共赢的新型大国关系的目标框架下构建国与国之间新的合作模式，共同应对包括网络安全在内的各种全球性挑战。[③] 这就

---

① 中国国家互联网应急中心：《2012年中国互联网网络安全态势综述》，2013年3月20日，参阅网页 http://www.cert.org.cn/publish/main/upload/File/20130321012CNCERTreport.pdf，第12页。

② Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, p.vi.

③ 《跨越太平洋的合作——国务委员杨洁篪谈习近平主席与奥巴马总统安纳伯格庄园会晤成果》，2013年6月9日，参阅外交部网站 http://www.fmprc.gov.cn/mfa_chn/wjdt_611265/gjldrhd_611267/t1048973.shtml。

将中美网络安全问题上的利益差异和政策分歧纳入共同管控范畴，为避免中美在网络空间的对抗和冲突奠定了战略基础。

汪晓风：复旦大学美国研究中心助理研究员

（本文责任编辑：魏红霞）