中美网络安全战略博弈：现状与展望

朱启超

内容提要：随着中美国家利益在网络空间不断拓展，两国在网络空间利益交叠而又相互依赖的趋势愈加明显，在网络安全相关问题上也处于既相互冲突又有限合作的复杂局面。本文回顾了中美网络安全合作的现状，分析了中美网络安全合作存在的矛盾问题，并结合构建新型大国关系提出中美网络安全合作增进中美战略互信的思路与建议。

关键词：网络安全　战略博弈　中美合作

2010年以来，随着中国综合国力快速上升和国家利益在网络空间不断扩展，网络安全问题开始成为影响中美关系的重要问题之一。网络自由、网络主权、黑客攻击、知识产权窃取、网络空间行为准则等网络安全话题频频被中美智库学者和政府官员提及，并相互指责。从2013年6月5日美国前情报人员爱德华·斯诺登在英国《卫报》爆出美国政府“棱镜门”监控丑闻，到2014年5月19日美国司法部以所谓“网络商业窃密”为由宣布起诉5名中国军人，近一年来中美之间关于网络安全问题的“隔空骂战”更是进入白热化状态，处于国际舆论的风口浪尖。正如美国布鲁金斯学会的李侃如（Kenneth Lieberthal）和彼得·辛格（Peter W. Singer）在《网络安全与中美关系》研究报告中所述：“在未来的国际政治中，或许没有比中美关系更重要的国际关系了。而在两国关系中，没有什么问题像网

朱启超　国防科技大学国家安全与军事战略研究中心主任、副研究员。

络安全问题一样，如此迅速地冒出来，并引发了很多摩擦。”[1] 除了摩擦外，中美之间围绕网络安全问题也展开了有限度的对话与合作，对于缓解双方紧张态势、增进中美战略互信起到了正面的作用。总体来看，中美在网络安全问题上处于既冲突又合作的复杂局面，两国在网络安全问题上的博弈将作为两国关系中一个越来越重要的变量，对于未来的中美关系将产生深远影响。本文从中美两国在网络安全领域的互动实践出发，分析中美网络安全合作现状与存在的主要问题，并试就如何推进构建新型大国关系、把握对美网络安全博弈的战略主动提出对策思考。

一、中美在网络安全问题上的主要分歧

中美在政治制度、意识形态、发展阶段和历史文化等方面存在显著的差异，在对待网络安全相关问题上也必然存在分歧。归纳来说，分歧主要表现在网络自由与网络主权、网络黑客、互联网国际治理权、网络军控与网络空间国际行为准则等方面。

（一）网络自由与网络主权

随着互联网以及新媒体技术的发展，人们对互联网和社交媒体（如脸谱、推特等）对国家安全和社会稳定的影响有了越来越多的认识。美国前国务卿希拉里2010年和2011年关于“互联网自由”的演说以及美国政府2011年《网络空间国际战略》，均明确表达了美国关于网络自由和网络主权的主张。美国认为，网络空间的基本自由应得到保障，互联自由和信息流通自由不应受到限制，中、俄等国不应搞“互联网内容过滤与技术审查”。但另一方面，美国希望借助网络外交和网络“巧实力”来达到其干涉甚至颠覆别国政府的企图，这种行径在伊朗大选、“谷歌事件”以及阿拉伯“茉莉花革命”中不断暴露。在中方看来，网络空间不存在绝对的自由，各国应遵守《联合国宪章》和公认的国际关系基本准则，包括尊重各国主权、领土完整和政治独立，尊重人权和基本自由，尊重各国历史、文化和社会制度的多样性等。网络空间应坚持主权原则、信息自由流动与安全流动相统筹的原则，避免信息网络成为干涉别国内政的新工具，尤其不能以“网络自由”为名，行“网络强权”之实。[2] 根据美国兰德公司2013年9月公布的《互联网自由与政治空间》研究报告，美国国务院民主、人权与劳工局在“谷歌事件”发生一年后曾委托兰德公司开展一项关于“互联网自由对民选政府的影

1 Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, The 21st Century Defense Initiative at Brookings and the John L. Thornton China Center at Brookings report, February 23, 2012,p.1.

2 奕文莉：《中美在网络空间的分歧与合作路径》，《现代国际关系》，2012年第7期，第28—33页。

响评估”的专题研究，研究对象涉及埃及、叙利亚、俄罗斯和中国，研究内容包括互联网领域的舆论自由怎么影响现实政治、哪些国家影响效果比较显著以及如何使美国推行互联网自由倡议取得最大效果，等等。这一报告与美国前国务卿希拉里·克林顿对中国的批评言论一起，被中国政府和学界专家视为美国政府以互联网自由为名影响干涉别国政治的有力佐证。[1]

（二）网络黑客

由于网络防护易攻难守的特点，黑客攻击事件近年来越来越猖獗，已成为国际公害。根据美国智库战略与国际研究中心（CSIS）2013年发布的研究报告，美国每年因网络犯罪导致经济损失近1600亿美元，约占美国国内生产总值（GDP）的1%。[2] 中国互联网安全形势也不容乐观。根据中国计算机网络应急技术处理协调中心2013年7月发布的《2012年中国互联网网络安全报告》，窃取经济利益成为黑客攻击的主要目标之一，中国2012年有5000多万条用户信息被售卖，境内被篡改网站数量16388个，被暗中植入后门的网站达52324个。[3] 中国国务院新闻办公室主任蔡名照2013年11月5日在第四届全球网络空间合作峰会上指出，80%以上的中国网民受到过网络侵害，每年经济损失达数百亿美元。而西方国家遭受网络攻击后，倾向于将“脏水”泼向中、俄等国。美国政府、智库和媒体公开指责中俄黑客盗取其技术及商业秘密，并借美国曼迪安公司等炮制的所谓APT1报告诬称中国军方也参与其中。2013年，美国前国家安全局雇员斯诺登陆续向媒体披露了美国国家安全局对网络进行大规模监控的“棱镜”计划，以及美国政府通过技术手段对中、德、法等国的国家领导人进行监听、对别国机构进行黑客渗透的行为。这一被称为“棱镜门”的事件打击了美国在黑客问题上对别国一味指责的气焰，但是美国政府仍坚称上述做法是为了国家安全而搜集情报的行为，并没有将商业情报转给美国企业。

2014年3月24日，中国国家主席习近平在荷兰海牙参加核安全峰会期间会见美国总统奥巴马时，就美国国家安全局入侵中国华为公司服务器和监听中国前国家领导人一事提出批评。奥巴马则辩称，美国的监视计划是为了国家安全而不是为商业利益服务。2014年5月19日，美国司法部部长霍尔德和联邦调查局官员主持新闻发布会，宣布以所谓“网络商业窃密”为由对5名中国军官提起网络黑客罪控告，再次招致中国政府官员和社会舆论对美国“贼喊捉贼”做法的猛烈抨击。对于中国方面的强烈反弹，美国政府官员、国会议员甚至社会舆论倾向

1 Oleseya Tkacheva, Martin C. Libicki, et al., *Internet Freedom and Political Space*, RAND Corporation report, September 2013,p.iii.

2 CSIS and McAfee Report, *The Economic Impact of Cybercrime and Cyber Espionage*, Center for Strategic and International Studies, July 2013,p.5.

3《国内信息安全态势》,《中国信息安全》，2013年第8期，第14页。

性地认为，美国以国家安全为目的进行的网络间谍活动比所谓中国以经济利益为目的而进行的网络间谍活动要高尚得多。[1] 这种苍白的辩解不仅在中国不能服众，反而更加侵蚀双方本就脆弱的互信基础。从中国国务院互联网新闻研究中心在美国宣布起诉中国军人一周后发布的《美国全球监听行动纪录》来看，在中国官媒历数美国打着维护国家安全的幌子在全球范围内大搞信息监听和网络监控的字里行间，包含着对美国凭借信息技术绝对优势地位谋求其霸权私心的强烈不信任。[2] 在打击网络犯罪问题上，中美立场也不尽一致。美国加入《布达佩斯网络犯罪公约》后要求各国签署该公约以合作打击网络犯罪。中国同样坚决反对任何形式的网络黑客攻击行为，但由于该公约个别条款规定不符合中国现实而暂未加入。中国倾向与俄罗斯等国在联合国框架内协调立场，呼吁各国加强合作打击非法滥用信息技术。

（三）互联网国际治理权

以国际互联网为基础的网络空间被认为“全球公域”，对于增进国际信息交流、技术创新和经济全球化等起到了重要的推动作用。然而，随着世界各国对互联网的依赖日益加深，网络安全问题逐渐成为全球性挑战，人们对互联网的国际治理权问题也给予了越来越多的关注。美国作为互联网的发源地和信息技术强国，垄断着全球互联网的运行管理和战略资源。目前，全球互联网根服务器有13台，其中唯一的主根服务器和9台辅根服务器都设在美国。所有根服务器均由美国商务部国家电信和信息局掌控的互联网域名与地址分配公司（Internet Corporation for Assigned Names and Numbers，简称ICANN）统一管理，为全球互联网提供域名解析和IP地址管理服务。20世纪90年代以前，由于各国对互联网依赖程度较低，互联网国际治理的矛盾尚未凸显。进入21世纪，由于美国不断利用对互联网的垄断管理以实现其政治和战略目的，引起了国际社会的警觉。例如，在2003年伊拉克战争期间和2004年利比亚在顶级域名管理问题上与美国发生争执过程中，美国终止了伊拉克和利比亚顶级域名“.iq”、“.ly”的申请和解析工作服务，导致两国相关网站在互联网消失了数天；2009年，微软公司也曾一度停止了古巴、朝鲜、苏丹等国的MSN即时通信服务。随着各国政治、经济和社会对互联网的依赖日益加深，中、俄等国甚至欧盟部分发达国家都认识到互联网域名管理关系国家主权与安全，纷纷建议在联合国设立一个类似国际电信联盟的机构取代ICANN对国际互联网域名与地址分配进行管理。[3] 虽然美国商

1 SShane Harris, “Our Spying Is Better Than Your Spying, ” May 31, 2014, http://www.foreignpolicy.com/articles/2014/05/31/our_spying_is_better_than_your_spying,2014-06-03.

2 中国互联网新闻研究中心：《美国全球监听行动纪录》，新华网，2014年5月26日，http://news.xinhuanet.com/2014-05/26/c_1110865223.htm，2014年6月2日登录。

3 奕文莉：《中美在网络空间的分歧与合作路径》，《现代国际关系》，2012年第7期，第28—33页。

务部下属的国家电信和信息局2014年3月14日宣布，美国政府有意愿将关键的国际互联网域名管理职能移交给全球多边利益攸关方组织，不过美国政府在声明中也预设了一个前提条件，即要求召集全球各利益攸关方提出一个获得“广泛国际支持”的移交方案，以作为到2015年移交管理权的第一步。同时声明还强调，方案应遵循保持互联网开放性原则，并且不会接受“由政府或政府间机构主导的解决方案”。美国商务部国家电信和信息局这一声明是对由于斯诺登事件所造成的国际舆论压力的妥协性回应，但距离美国政府真正移交国际互联网域名管理职能还有很长的路要走。从技术上讲，移交ICANN关于互联网域名的部分管理权，只是保持互联网开放性的一种举措，不能认为美国要放弃对互联网的控制权；[1] 从美国“棱镜”计划和在信息技术领域的未来投资重点来看，美国将竭力保持信息技术领域的全球领先地位，从而保持对于国际互联网的利用与控制优势。从互联网国际治理改革走势看，美国政府将会继续以国家安全、“难以形成广泛的国际支持”等理由来迟滞这一进程。2010年以来，中国网民人数尤其是使用移动互联网的网民人数激增，国家利益对网络空间的依赖日益加重，中国正越来越成为国际互联网的一个举足轻重的利益攸关方，如何在国际互联网治理改革中体现中国声音、中国分量、中国责任，将是未来中美之间不可回避的话题之一。

（四）网络军控与国际行为准则

信息网络技术推动了社会信息化和经济全球化的发展，不仅使金融证券信息系统、电网、交通管理信息系统、大型工业控制系统等国家关键基础设施日益依赖网络，还使得军事活动也更加依赖网络空间。美国在其2010年新版的军事战略中将网络空间定义为一个新的独立的作战空间。为适应世界新军事革命的发展趋势，各军事大国纷纷出台网络安全战略，成立网络战部队，网络空间军备竞赛持续升温。为确保美国在网络空间的绝对优势和“行动自由”，2013年年初国防部批准大幅扩编其网络司令部编制规模，在2015年前从目前的900人增加到4900人。2014年3月30日，美国国防部长哈格尔再次表示，到2016年美国网络司令部将扩编至6000人。与此同时，美军还加紧研发“震网”病毒、“火焰”病毒等2000多种病毒武器，持续开展以实战为目的的“网络风暴”、“施里弗”等系列演习。为配合网络扩军行动，美国海军战争学院的迈克尔·施密特教授领衔北约成员国专家于2013年3月组织撰写了《塔林手册：适用于网络战的国际法》，公布于北约网站。该手册的主要观点有：承认网络空间存在国家主权和管辖权；超过一定规模和影响的网络攻击属于“武装攻击”；个人或组织的网络攻击行为等同于国家行为；针对网络攻击可以使用传统武力进行回击报复；军事盟友间的集体自卫行动在网络空间依然适用；网络攻击禁止针对医院、儿童福利院等重

1 李国敏：《美国移交ICANN管理权不等于移交互联网控制权》，《科技日报》，2014年3月24日。

要的民用目标或设施；“中立法”适用于网络空间。[1]《塔林手册》的出台，表明美国及北约组织试图主导网络空间国际行为准则的制定，为在网络空间发动战争奠定法理基础。美国本来就拥有十分强大的网络战能力，为网络战立法、定规则的举动必然进一步加剧中、俄等“金砖国家”以及广大发展中国家的疑虑。早在2011年，中、俄、塔、乌等上合组织国家代表广大发展中国家立场向联合国提交《信息安全国际行为准则》倡议书，西方国家尤其是美国对此却并未给予足够的理睬与回应。

美国及北约组织试图主导网络空间国际行为准则的制定，为在网络空间发动战争奠定法理基础。

二、中美关于网络安全问题的对话与合作现状

为了减少冲突与对抗，维持中美关系大局，中美两国自2009年以来进行了多种形式的网络安全对话与合作，主要分为民间与政府两个层面。

（一）民间层面的网络安全对话

中美关于网络安全问题的民间对话主要表现为各类学术机构之间的网络安全学术研讨会和政府授权下“第二轨道”（以下简称“二轨”）层面的网络安全对话。网络安全学术研讨会注重学术交流，议题相对灵活，研讨内容涵盖网络安全的基本术语、网络安全对国际关系的影响、中美对黑客问题的态度以及中美未来网络安全合作的展望等。以国防科技大学自2009年开始举办的“国家安全与科技发展战略国际研讨会”为例，每次都邀请美国智库或大学的专家参会，就网络安全、跨域安全等问题进行研讨交流。由于定位为学术研讨，研讨会给双方较大的讨论空间，既有助于增进双方相互了解，也在一定程度上担当了学术外交的角色。[2]

2009年以来，中美双方至少建立了三个“二轨”层面的对话交流机制。第一个是由中国现代国际关系研究院和美国智库战略与国际研究中心共同发起的“中美网络安全对话”，至今已经举办了8次。双方学者和以观察员身份与会的两国政府主管部门官员围绕中美网络空间互信机制、网络空间国际准则制定、中美打击网络犯罪执法合作以及应对网络空间新的安全威胁等问题进行了持续讨论。

1 Michael N. Schmitt ed, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Center of Excellence, Cambridge University Press, 2013.

2 朱启超、黄长云、张煌：《第三届国家安全与科技发展战略国际研讨会综述》，《现代国际关系》，2013年 第8期， 第64—65页；Qichao Zhu, *Cross-domain Security and Cross-domain Deterrence: An Analytical Framework to understand the Cyber-related Issues in the Information Age*, The 3rd International Seminar on the Strategy of National Security and the Development of Science & Technology (the 3rd ISST), Changsha, China, June 17-18, 2013。

第二个是美国智库布鲁金斯学会组织中美学者开展的网络安全对话研讨活动，对话交流的成果主要体现在李侃如、辛格合作的研究报告《网络安全与中美关系》和李侃如、王缉思合作的研究报告《中美战略互疑：解析与应对》[1] 中。第三个是中国国际战略基金会和美国战略与国际研究中心太平洋论坛之间开展的定期研讨对话活动，近年来关于网络安全的话题也不断增多。通过这些双边对话活动，可为双方决策部门传递积极的、富有建设性的信息，使中美双方能够增进对彼此目标和担忧的理解，推动建立网络行为规范，从而有助于建立互信合作的基础。

（二）政府层面的网络安全对话与合作

随着网络安全问题在中美关系中不断升温，两国政府对于网络安全问题都给予高度重视，并开展了越来越多的合作。这个方面的对话也主要反映在三个层面：一是中美政府高层之间的对话。除了在两国元首会晤中谈及网络安全议题，中美领导人自2009年始启动了中美政府间的战略与经济对话，并于2011年在第三次中美战略与经济对话的框架下设立了中美战略安全对话，在历次对话活动中都对网络安全问题给予了较多关注。二是中美职能部门之间的沟通合作机制。目前，中美双方通过中美执法合作联合联络小组就打击网络犯罪、知识产权执法、司法协助等开展了卓有成效的合作。2011年8月，中美警方联手破获了全球最大的中文淫秽色情网站“阳光娱乐联盟”，就是双方合作打击跨国网络犯罪的一个范例。2013年4月，两国政府决定成立网络工作小组，以协调双方立场和分歧。2013年7月8日，中美政府在战略安全对话框架下举行第一次网络工作组会议，双方就网络工作组机制建设、两国网络关系、网络空间国际规则、双边对话合作措施等问题进行了坦诚交流。然而，2014年5月19日，工作组仅成立一年后便发生了美国司法部以所谓“网络商业窃密”为由起诉5名中国军官的事件。中国政府认为，美国此举严重违反了国际关系基本准则，损害了中美之间的合作和互信，且美方缺乏通过对话合作解决网络安全问题的诚意，遂决定中止中美政府间网络工作组的相关活动并启动针对外国IT企业的网络安全审查制度进行报复。三是联合国框架下双方专家之间的合作。2013年6月，中美等国专家在联合国框架下就网络主权、网络空间行为准则等问题进行了多边研讨，虽然就承认网络主权达成了一些共识，但是对于网络主权和网络空间行为准则的内涵仍存在较大分歧。

（三）中美网络安全对话与合作的局限

从现实情况看，中美网络安全对话有如下特点：一是美方进攻性姿态明显，中方处于守势。美方在网络自由、网络黑客、知识产权保护、网络空间行为准则

1 王缉思、[美]李侃如：《中美战略互疑：解析与应对》，北京：社会科学文献出版社，2013年版。

等方面往往主动抛出话题，企图占据道德制高点，而中方往往被动接招，坚守底线。二是对于术语定义的讨论较多，涉及实质问题的讨论较少。即便中美学术界之间开展了多次的交流，但就网络空间相关术语的理解仍然不相一致，且由于双方社会信息化发展水平不同，对于网络安全问题的认识也存在不少差异。三是对于彼此战略意图相互探底的讨论较多，尤其是美方近年来将网络安全与空间安全、核安全话题相提并论，双方在这些高技术领域互信的基础依然脆弱。美方倾向于认为中国空间技术、网络技术的发展已经到了能切实对美国构成较大威胁的程度，而中方则认为美方在网络、太空和核领域拥有强大的技术优势，对自身在上述领域的安全有着更大的忧虑。

恩格斯在《1852年神圣同盟对法战争的可能性与展望》一文中揭示，人类以什么方式生产，就以什么方式作战。[1] 从这个意义上尤其是对于大国来说，当国家利益不可避免地在网络空间扩展，捍卫国家在网络空间的安全与发展利益就成为国家安全的重要内容，发展网络军事能力、构筑网络国防也就成为主权国家的必然选择。但对于中美两个大国来说，美国作为先发国家，自20世纪90年代开始就重视逐步完善国家层面的网络空间安全战略，目前已形成了涵盖网络空间国际战略、国家安全层面的网络空间战略和军事层面的网络空间行动战略的战略体系，将网络空间的国家利益视为美国国家安全和经济繁荣的基石；[2] 而中国作为快速崛起的发展中大国，与国家利益对网络空间的依赖增长速度相比，应对网络空间安全挑战的战略准备相对滞后，2013年11月12日中国共产党第十八届三中全会决议宣布成立国家安全委员会和2014年2月27日中央网络安全和信息化领导小组宣布成立，标志着中国真正将网络安全提升到国家安全的层面加以系统应对。从国家安全决策的角度看，中国网络安全战略应对能力准备总体上落后美国十余年甚至二十年。何况网络安全问题往往被裹挟在影响中美关系的地缘政治、海洋争端、经济贸易、知识产权等问题中，使得双方就网络安全问题建立互信的难度和复杂性大大增加。尤其是在太空和网络空间，这些领域目前仍存在着许多技术与管理能力上的空白，要消除双方的误解其实比传统领域更加困难，而未来的网络空间将会成为中美两国在安全、军事、情报、科技甚至意识形态方面展开竞争的主要战

未来的网络空间将会成为中美两国在安全、军事、情报、科技甚至意识形态方面展开竞争的主要战场。

1 参见《马克思恩格斯全集》第七卷，北京：人民出版社，2005年版，第557页。

2 比如美国小布什政府于2008年1月颁布了《国家网络安全总体倡议》(The Comprehensive National Cybersecurity Initiative)，奥巴马政府先后于2009年5月发布了《网络空间政策审查报告》(Cyberspace Policy Review)、于2011年5月颁布了《网络空间国际战略》(International Strategy for Cyberspace)，美国国防部于2011年7月颁布了《网络空间军事行动战略》(Department of Defense Strategy for Operating in Cyberspace)。

场。[1] 由于网络安全已扩展到中美关系的经济与贸易、政治与外交、军事与国防等各个领域，集中凸显了中美关系中竞争与对立的一面，其重要性的上升或将挑战“9·11”事件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的影响。[2] 正是由于上述局限，使得中美网络安全合作还处于初步阶段。

三、影响中美网络安全合作的障碍

随着中美在网络空间的利益进一步扩展，两国对网络安全的合作需求将日趋强烈，这种良性合作对于塑造中美新型大国关系将起到有力的促进作用。但是也必须清醒地认识到，中美网络安全合作也存在一些障碍性因素。这些障碍性因素除了两国长期存在的经济贸易领域的结构性矛盾（如贸易逆差、人民币汇率问题）和台湾问题等，近期需要给予重点关注的有以下三个问题：

第一，美方如何处理其“亚太再平衡”战略给中美战略关系造成的负面影响。美国自2009年以来高调重返亚洲，提出了“亚太再平衡”战略。该战略主要涵盖经济上的“跨太平洋伙伴关系协定”（Trans-Pacific Partnership Agreement，TPP）、军事上以中国为假想敌的“空海一体战”（Air-Sea Battle Concept）构想等内容。就具体军力部署而言，美国近期决定把其全球军事力量的60%部署到亚太地区，将“全球鹰”无人机、F-22隐形战机等一批先进的武器装备部署到中国周边；就作战想定来说，美军未来将网络战视为其“空海一体战”构想的重要组成部分。[3] 这些举措必然增加中国的国家安全压力和安全忧虑，对中美未来网络安全合作蒙上挥之不去的阴影。[4]

第二，美国是否会心甘情愿地接受中国提出的“新型大国关系”主张。中国领导人近年来提出“新型大国关系”主张，其内涵为“不冲突、不对抗，相互尊重，合作共赢”。这是中国基于公认的国际关系准则提出来的新构想，体现的是中国作为发展中大国的责任义务与处事风格。但是，对信奉实力原则的美国而言，维持全球霸权是其国家安全战略的基础，美国是否愿意接纳中国作为其平等的合作伙伴而不是潜在的战略对手，前景还不是十分乐观。从美国总统奥巴马2014年4月23日至29日访问亚洲四国力挺军事盟友与中国对抗的举动来看，美国未来不会放弃对华防范遏制的冷战思维。基辛格曾用“克劳学派”（Crowe school of thought）一词来指代美国国内一批坚信中国崛起将会与美国国家利益冲

1 金灿荣、段皓文：《当前中美关系的困境与出路》，《国际观察》，2014年第1期。

2 汪晓风：《中美关系中的网络安全问题》，《美国研究》，2013年第3期。

3 Jan Van Tol, Mark Gunzinger, Andrew Krepinevich, and Jim Thomas, *Air-Sea Battle: A Point-of-Departure Operational Concept*, Report of the Center for Strategic and Budgetary Assessments, 2010.

4 Qichao Zhu, “Obama's Pacific-Pivot: The Coming Arms Race,” *The World Defence Systems*, Vol.1, 2012, pp.10-11.

突的思想界精英，这些精英的观点当前在美国政界、商界和学界拥有一定市场。“克劳学派”源于第一次世界大战前英国外交官艾尔·克劳（Eyre Crowe）就德国崛起向英国外交部撰写的一份秘密报告，史称“克劳备忘录”，认为无论“崛起国”的言行如何表现，其本身能力的发展必将导致“崛起国”与现有霸权国家生存发展互不相容。[1] 因此，中美对于“新型大国关系”的理解有可能“一词各表”，影响两国战略互信的发展，影响中美在网络安全问题上的交流与合作。

第三，美国在网络军备建设上是否会主动地自我克制。美国是世界上军事力量最强大的国家，也是网络军队规模最大、最具威力的国家。美军网络司令部2013年以来高调扩军备战的姿态，将是世界各国发展网络力量的参照。对于中、美、俄等大国而言，网络空间的军备竞赛，加剧的将是国家之间的战略互疑。虽然美国学者戴维·戈帕特（David C. Gompert）和孙飞近年来提出“战略克制”（Strategic Restraint）的概念，呼吁美国与俄罗斯、美国与中国之间在核、太空和网络领域进行相互的战略克制，但是作为实力最强大的美国如果不能自我克制，其他国家的不安全感将会更加强烈。[2] 近年来，一些美国专家也开始认为推动亚洲地区军备竞赛的不是中国，而是美国。[3] 这就表明，美国如果不调整其亚太安全战略与政策，带来的将是该地区无止境的军备竞赛，继续侵蚀中美之间本就脆弱的战略互信。

第四，中美在网络安全问题上的认知错位。虽然中美两国在网络安全问题发酵或产生影响的各个领域都开展了一定程度上的沟通对话，但由于双方社会信息化发展程度、法律制度、政治体制等方面存在差异，使双方的沟通对话实际上不仅处于较浅的层次，同时也存在某种程度上的认知错位。一是关于信息技术优势的认知错位。由于中国是具有后发优势的最大发展中国家，中国一直认为美国拥有全世界无可匹敌的高技术尤其是信息和通信技术（西方语境中将 information and communication technology 简称为 ICT）优势，思科、谷歌、甲骨文、微软等常被提起的 IT 产业“八大金刚”在技术上处于垄断地位，因而与美国相比总是自叹弗如，甚至担心中国的网络安防在美国强大的技术优势面前“形同虚设”；美国方面则认为，ICT 技术扩散快、创新门槛低，中国华为、中兴等 IT 企业已发展壮大甚至在某些领域具有相对优势，美国担心自己的网络安全已不再绝对可

1 尹树广：《“克劳备忘录”不合时宜》，香港《文汇报》，2014年4月1日。

2 David C. Gompert and Philip C. Sunders, ***The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability***, Institute for National Strategic Studies, National Defense University, 2010; Greg Austin and Franz-Stefan Gady, ***Cyber Détente between the United States and China,*** Report of East West Institute, June 2012.

3 Stephen Harner, “U.S. Policy, Not China, Is Driving the Asian Arms Race,” April 6,2014,http://www.forbes.com/sites/stephenharner/2014/04/06/u-s-policy-not-china-is-driving-the-asian-arms-race/,2014-4-24.

靠。二是关于网络黑客与网络间谍的认知错位。基于斯诺登的爆料，中国认为美国的信号监听与网络监控能力登峰造极，信息情报收集范围涵盖政治、经济、科技和军事等各个领域，试图保持各领域的霸权优势；而美国虽承认对别国实施间谍手段，但主要用于国家安全目的，并且美国国会议员、退役高官最为担心的是中国依靠网络间谍手段窃取美国企业商业秘密和知识产权，长此以往，不仅美国国家财富将持续遭受巨大损失，美国霸权赖以存在的高技术优势也将不保。[1] 三是关于网络安全立法与执法的认知错位。斯诺登事件以来，中国舆论主要致力于揭露美国的道德伪善，而美国官、产、学、研各界着力的方向则是企图运用法律手段对中国网络黑客犯罪形成制约。从美国智库不断煽风点火、曼迪安公司等咨询机构精心搜集证据链到美国司法部对5名中国军人提起诉讼，都说明美国在网络安全问题上试图将网络犯罪从网络间谍行动中剥离开来，通过其擅长的经济领域的立法与执法行动对中国进一步制造压力。中美两国关于网络安全问题的这些认知错位，将会继续深刻影响两国网络安全战略与政策的走向，也将为未来两国间的网络安全冲突埋下伏笔，对进一步的对话与合作造成认知障碍。

四、推进对美网络安全务实合作的政策建议

虽然中方因美国司法部起诉5名中国军人的事件暂时中止了两国政府间网络工作组活动，但由于两国之间日益加深的相互依赖，“斗而不破”依然是处理两国关系的一种默契。美国很可能在即将召开的新一轮战略与经济对话期间，主动缓和双方紧张的网络安全关系，继续与中方保持沟通、对话与合作。总的看，中美关于网络安全合作既面临诸多的制约因素，同样也面临很多的机遇条件。展望未来，美方如能真正视中方为平等合作伙伴，接受中方提出的构建新型大国关系主张，必将有助于双方通过务实合作逐步增强互信的基础，破解影响网络安全合作的障碍。应当指出的是，中美在网络安全问题上的竞争是基于实力的竞争，而合作也应是基于实力的合作。如果两个大国应对网络安全挑战在战略决策能力、

1 成立于2000年的美国国会美中经济与安全审查委员会每年推出年度报告，大肆渲染中国威胁论，2010年以来更是将网络黑客问题与知识产权挂钩，不断批评甚至污蔑中国政府支持网络黑客偷取美国知识产权，详见其于2012年3月委托诺斯罗普·格鲁曼公司发布的报告“Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage”；美国前驻华大使洪博培、前国家情报总监丹尼斯·布莱尔、前国防部副部长威廉·林恩等人还专门成立反知识产权偷窃调查组织（The Commission on the Theft of American Intellectual Property），重点将矛头指向中国，就中国黑客知识产权盗窃活动开展调查评估，详见其于2013年5月发布的调查报告“The IP Commission Report”；此外，美国智库战略与国际研究中心、加州大学全球冲突与合作研究所（IGCC）等机构的专家也纷纷加入针对中国黑客知识产权犯罪的调查研究活动，加大渲染中国黑客知识产权盗窃犯罪的严重性，参见美国加州大学全球冲突与合作研究所 Jon Lindsay 和 Tai Ming Cheung 2013年7月发布其网站的文章“The Greatest Transfer of Wealth in History? Exploring the Relationship between Chinese Cyber Espionage and Technological Innovation”。

信息技术实力和网络国防实力方面相差悬殊，将难有真正平等的双边合作。主权国家打造网络安全实力的过程，同时也是追求网络权力的过程，网络安全虽然已渗透到大国关系的各个方面和领域，但本质上可以分为基于网络空间行动规则的程序性权力、基于网络空间影响力的资源性权力和基于网络信息基础设施掌控权的结构性权力。[1] 对中国来说，应结合中美网络安全对话与合作交流的基础，从以下方面增进网络安全实力建设，善加运用大国网络权力，进一步增强未来中美网络安全博弈的战略主动。

（一）增强中方在网络安全问题上的话语权

如前所述，在中美网络安全相关话题的双边研讨中，中方总体上话语权较弱，主导相关议题的能力不强。这一方面反映了两国因信息化水平不同对网络安全问题存在认知差异，另一方面也反映出中方对网络安全相关问题研究还有待深入、网络安全政策传播机制还不完善。比如，早在2008年6月，中国就颁布实施了《国家知识产权保护战略纲要》，通过完善制度和立法来保护知识产权，打击知识产权违法犯罪，但中方对于近年来美方关于中国知识产权盗用的指责回应较弱，这就说明中国尚不善于及时向国际社会宣传自己的网络安全相关政策。因此，中国应进一步整合政府、企业界和学术界的研究力量，围绕网络安全的相关概念（术语）、网络安全战略、网络安全法律法规、网络安全行业政策、网络安全基础设施等方面的问题展开持续研究；树立网络安全的“大人才观”，破除“一谈到网络安全就是技术人员的事”的认知偏见，采用多种灵活措施培养网络外交、网络管理、网络技术、网络法律、网络传播等各领域人才，使网络安全相关问题的研究体现专业素养，提升专业水准；利用政策白皮书、双边对话机制、智库间学术交流等多种形式展示中国在网络安全问题上的战略、政策与合作诚意；切实增强中方关于网络犯罪的立法与执法能力，设立政府和社会层面相结合的网络安全犯罪调查机构，开发新一代网络行动溯源技术，针对美国境内发起的针对中国的各类网络犯罪活动建立证据链，对美方今后可能再次出现的“起诉中国军人黑客犯罪”等行动进行“以眼还眼以牙还牙”的应对。

（二）共同推动国际信息安全行为准则的制定

爱德华·斯诺登对美国国家安全局大规模网络监控计划的爆料至今仍在发酵，引起了包括美国重要盟友在内的国际社会的广泛不满。“棱镜门”事件重创了美国在世人面前的国家形象与道德信誉，表明美国政府对本国公民及他国目标的黑客间谍行为远远超出人们想象，凸显美国为追求和巩固其霸权地位而对信

1 黄长云、朱启超、张煌：《云计算视阈下的网络威慑》，《国防科技》，2013年第4期。

息技术的滥用，也为国际社会改善网络安全国际治理机制提供了合作契机。[1] 为此，中国应把握当前有利的国际舆论环境，与广大发展中国家和包括美国在内的国际社会一起，在联合国框架下共同推动具有一定公信力、凝聚相当范围共识的网络信息安全国际行为准则的制定，避免将网络空间导向无限度军备竞赛的不归路。实际上，随着中国国家利益对网络空间的依赖越来越大，中国不可避免地成为网络安全全球公域中一个分量越来越重的利益攸关方，应在网络安全国际合作话题上展现更多的责任宣示并积极承担相应的国际义务。

“棱镜门”事件凸显美国为追求和巩固其霸权地位而对信息技术的滥用，也为国际社会改善网络安全国际治理机制提供了合作契机。

（三）敦促美方对中国信息产业企业开放市场

近年来，美国动辄以国家安全为借口，阻挠中国华为、中兴等高科技信息企业进入美国市场，但思科、IBM、谷歌、高通、英特尔、甲骨文、微软、苹果等美国高科技公司却在中国电信、金融、能源、交通运输等关键行业的信息基础设施中占有了相当大的市场份额。这种极度不对称的现象既是美国国会人为地干预国际信息技术市场竞争的结果，也体现了美国对待中国信息技术产品不对等、不公平的防范心理。各国对国际互联网的使用参与越多，自然会增加各国之间的相互依赖，而中美之间这种建立在信息基础设施资源不对称基础上的相互依赖，却成了双方相互防范的重要壁垒，造成双方尤其是中国方面的安全困境。这种状况如不能得以缓解，将加剧中国政府和企业界对美国在网络安全问题上的不信任。对中国而言，要增进两国在网络安全合作问题上的互信，一方面要加强对国外高科技产品的供应链安全审查制度，另一方面应采取切实措施促使美国尽快对中国企业平等开放信息技术市场。否则，双方关于信息技术产品渗透的安全担忧和贸易冲突将会恶化双边互信与合作。

（四）继续保持双边多层次对话与合作

中美在共同打击网络犯罪方面已经进行了尝试性的合作，未来在这一领域还应继续深化技术取证与执法协作。这将有助于中国尽快完善相应的法律体系和执法力量建设，更好地与国际社会一起打击网络黑客犯罪，塑造中国负责任的大国形象。截至目前，中美已经在政治、经济与军事领域形成近百个多层次的专业化磋商与对话机制，成为降低中美直接冲突、促进中美合作的宝贵制度资源。这些对话与磋商机制形成的一般路径是，首先是“二轨”层面民间试水、智库推进，沟通相对成熟以后再由政府职能部门主导“一轨”层面的对话，但往往上升到“一轨”层面对话磋商之后，“二轨”层面的对话就会终止。因此，今后仍有必要

1 朱启超：《“棱镜门”事件的棱镜效应》，《科技日报》，2013年9月10日。

继续拓展多层次的对话磋商与合作，形成多轨并存、多层次持续并进的对话局面，使得中美网络安全问题在“一轨”层面的对话与合作之前或在“一轨”层面的对话暂时中止期间，仍能有持续充分的沟通和理解。