中美新型大国关系研究报告（第15期）

网络安全博弈
与中美战略关系稳定

复旦大学
中美新型大国关系协同创新中心
2016年3月

中美新型大国关系研究报告

网络安全博弈与中美战略关系稳定

第 15 期

2016 年 3 月

作者简介

沈逸，副教授，2005 年复旦大学国际政治系博士毕业，现任复旦大学网络空间治理研究中心副主任，中国网络空间研究院特约研究员。主要研究方向为国家网络安全战略、网络外交与网络空间国际治理。专著有《美国国家网络安全战略》。

网络安全博弈与中美战略关系稳定

自 2013 年以来，以美国曼迪昂特公司发布《高级可持续攻击（Advanced Persistent Attack，缩写为 APT）报告 1 号》，中央情报局前雇员斯诺登披露美国国家安全局“棱镜”系统监控全球网络、美方起诉中国人民解放军五名军官涉嫌对美国企业进行商业窃密攻击、美国威胁就网络商业窃密起诉中国相关企业等事件为标志，网络安全问题正式成为中美战略关系中的新议题。2015 年初，美国总统奥巴马邀请中国国家主席习近平 9 月对美国进行国事访问，在前期磋商过程中，美方提出网络安全、南海问题、人权问题作为中美是次首脑峰会的三大焦点议题；其后围绕美国相关公司、企业以及以人事局办公室（Office of Personnel Management，缩写为 OPM）等遭遇大规模黑客袭击等问题，中美双方就如何构建网络空间行为准则，在中美战略关系框架开内建设完善网络安全对话机制，妥善处理网络安全威胁以保持战略关系稳定，如何看待和认识中方倡导的网络治理理念等议题，展开了全方位的沟通、交流与博弈。

网络安全议题成为贯穿 2015 年中美战略关系始终的重要问题，成为中美战略博弈的新领域，并一度由于矛盾和摩

擦的激化，导致中美走向摩擦乃至有限对抗的危险境地。最终，由于中美战略决策层均保持了高度的理性与克制，借助特使互访、二轨对话以及首脑峰会等方式，在 2015 年 9 月重建了被临时中断的对话机制，初步就稳定网络安全战略关系达成了合作协议，重新启动了两国网络安全政府间对话机制，网络安全战略议题重新趋于稳定。

从全球发展态势看，中美战略关系框架内网络安全议题重要性的提升与凸显，是全球面临的网络安全威胁冲击和挑战的缩影和标志。自冷战结束后高速扩展的网络空间最终不可避免的要求现存的国际体系对此问题作出相关的回应。各国在利用网络空间获取、扩展和保障自身重大利益的同时，又面临如何在网络安全议题上寻找共同利益基础，应对共同安全威胁挑战的新任务和新挑战。2015 年联合国框架下政府间专家组就网络安全相关问题达成的框架性文件，凸显了国际社会应对网络安全相关挑战的努力；以互联网名称和地址分配当局监管权限转移方案的形成为标志，全球共同治理网络空间的努力正在朝向更加公正、公平、合理的方向迈出重要的步伐，在此过程中，中美之间的网络安全战略博弈不仅对双边战略关系产生了显著的影响，也对全球治理互联网的多边努力产生了深远、重要而微妙的影响。

本章节将分四个部分对此问题展开论述：其一是对 2015

年影响中美网络安全关系的重要问题进行梳理和分析；其二将对中美两国政府围绕网络安全的战略互动进行描述；其三是分析和介绍影响中美网络战略博弈的关键议题；其四简要分析评价 2015 年中美两国在网络安全问题上达成的成果进行评估，并初步预测两国网络安全战略关系发展的趋势和特点。

一、2015 年中美网络安全关系中摩擦显著提升

指责中国在网络空间实施的窃密活动有损美国的商业利益，威胁美国国家安全，是美国政要和智库圈自 2013 年开始的新动向。[1]这一动向主要受三个因素的影响：其一，是中美整体战略力量对比中持续出现差距缩小的态势，中方缩小与美国的力量差距引起美各方系统的战略焦虑；[2]其二，是美国对网络关键基础设施的战略依存显著提升，网络的正常运行已经成为美国国家利益的重要组成部分；[3]其三，美方研判中方在网络空间的情报获取活动对中国提升整体实力具有战略意义，并认为美方在此问题上仍然具有对华施压的空间和能力。[4]

相比 2013 年和 2014 年，2015 年中美在网络安全关系中的摩擦一度呈现显著提升态势，具体来说表现如下三个方面：

第一，美方持续指责所谓得到中国资助或者支持的黑客

组织对美国的公司和政府部门实施大规模网络攻击。2015 年 2 月至 8 月间，美方先后指责中国黑客组织“深度熊猫”（Deep Panda）入侵全美第二大医疗保险公司安森（Anthem）；中国黑客入侵美国人事局网络系统，窃取 2000 万美国政府雇员或承包商的数据和信息；中国黑客入侵美国联合航空公司（American Airlines）的数据库，窃取大量数据。

第二，美国政府开始提升在网络安全议题上对华施加的压力，威胁实施经济制裁，甚至暗示可能对华实施网络战进行报复。2015 年上半年，美国政府多次通过智库报告以及匿名官员向媒体“放话”的方式，直接或间接的表示，将就网络安全问题对华施加压力，制裁被美国认为从网络攻击中直接获益的中国公司；威胁考虑以网络攻击方式瘫痪部分中国关键基础设施以报复所谓中国对美实施的网络攻击行动。

第三，美国政府开始在战略规划、政策文件以及财政拨款等方面以中国网络安全威胁假想敌，落实并强化有针对性的网络攻击能力建设。2015 年 5 月，美国国防部发布新版的《国防部网络空间行动战略》，明确宣布将使用网络司令部的防御力量用于防御针对美国关键基础设施的可能造成严重后果的网络攻击，同时宣布将为美国总统和国防部长提供用于危机管理的网络攻击能力；美国国会在讨论新财政年度的《国防授权法案》中，明确要求美国参谋长联席会议在 2016

年建设完善针对俄罗斯、中国、伊朗、朝鲜等国网络攻击的“战棋推演”能力；2015 年 7 月美国政府匿名官员向《纽约时报》的记者承认，美国已经在中国大陆的计算机网络中“植入数以千计的系统”，用于“预警中国向美国发动网络战”。[5]

2015 年中美网络安全关系一度呈现出摩擦高速提升的态势，这一方面是由中美整体力量对比和战略态势改变在网络安全问题上的投影所导致的，另一方面，网络安全对中美两国来说，都是一个全新战略领域，两国仍然在摸索构建完善自身的国家网络安全战略，对于如何正确识别和评估威胁，构建完整、完善的政策工具，仍然存有相当的不确定性。由此带来的结果，是 2015 年在个别时期和个别议题上，中美两国在网络安全议题领域表现出来的摩擦和争议，至少在公开媒体的层面，显示出了某种令人非常担忧的趋势。

缺乏战略信任，是导致中美网络安全关系在 2015 年一度趋于恶化的核心原因。美国的网络安全战略决策与政策制定，深刻的受到决策者认知理念的影响。自冷战时期遗留下来的刻板的意识形态认知框架，深刻的影响了美国在处理网络安全议题时的政策选择。受技术条件限制，目前对网络攻击的“溯源”，也就是查找源头的能力，有了长足的进步，但仍然无法通过技术手段最终确定发起攻击者的真实动机。

用美国国务院官员的话来说，最终确定真实动机和身份的工作，远比想象中复杂，无法单纯依靠技术完成，必须结合国家情报力量来完成。但值得关注的是，2015 年相当一段时间里，在公开媒体环境中，“中国”通常被默认为头号候选嫌疑人。

判别标准模糊不清，是导致中美网络安全关系中摩擦显著上升的关键原因。国家可以在网络空间做些什么？哪些事情可以做？哪些事情不可以做？迄今为止，至少在中美之间，还处于探索和完善的阶段。而美国的问题在于，过于自觉地使用了完全基于美国国家利益的双重乃至多重标准，试图要求中国完全以符合美国国家利益的方式采取行动。一个简单的例子，就是 2015 年一度被炒得沸沸扬扬的美国人事局数据遭遇中国黑客攻击的事件。当美国政府、安全公司、智库和媒体大肆讨论美国人事局遭遇中国黑客攻击威胁美国国家安全的时候，给人的印象是：这种行为是美国所不能接受的。但美国国家情报总监克拉伯在国会听证会上给出的回答却与此截然不同：对美国人事局数据的攻击就是一起传统的被动情报搜集活动，“和我们做的没有差别”。换言之，对人事局数据的攻击，不是商业窃密，只是正常的情报搜集活动。但美国借用了在媒体传播中的影响力，将对人事局数据的攻击和所谓“商业窃密”混为一谈，在美国国内恐吓美国

民众，进而谋求美国政府更容易在美国国会获得网络安全领域的授权；在中美关系中对华施加压力，迫使中国做出本无需做出的让步，挤压中国在网络空间的行动自由。

国内政治干扰，是影响中美网络安全关系走向的重要原因。特别值得关注的是，美国网络安全战略决策与政策制定的过程，具有相当显著的官僚部门竞争的色彩，整个国家网络安全战略的制定和运行，包括对威胁的认知与识别，并非在最高决策者的单一控制下严格遵循理性决策的模式展开，而是在国务院、国防部、国土安全部、司法部（联邦调查局）、商务部等部门彼此竞争的关系中展开。美国国防部长卡特将“预防性防御”的战略理念用于网络空间，大幅强化和提升了美国网军司令部在网络安全战略中的影响力，也使得美国国家网络安全战略更具“先发制人”的攻击性。各个部门彼此竞争，加上 2015 年美国国内政局因为两党竞争继续趋于极化等因素，在整个网络安全议题上，美方通常会经过不同的渠道、平台和方式，同时向中方发出自相矛盾的信号，这进一步干扰了本来就充满了不确定性的中美网络安全关系。总体来看，美国国务院、国土安全部、商务部更加倾向于采取交流和对话的方式，来解决中美之间的网络安全问题，即使提及中国对美国构成网络安全的威胁，也更多的是作为施加压力的筹码；国防部、司法部因为职能分工的原因，更倾

向于将网络安全议题升格为传统国家安全问题，更关注中美网络安全关系中的摩擦和分歧，强调用对中国施加压力的方式来解决问题。

二、2015 年中美两国努力重建政府间网络安全对话机制

2014 年 5 月 19 日，美国司法部以所谓涉嫌对美实施网络商业窃密为由，起诉中国人民解放军 5 名军官，中方对此举做出强硬回应：中断中美政府间网络安全对话机制。自那时开始，中美两国一直努力试图重建政府间网络安全对话机制。中方此前始终坚持美国必须撤销对五名军人的指控，然后才能恢复对话；美方则在 2014 年至 2015 年上半年多次通过第二轨道知会中方，称美方无意采取任何导致事态升级的后续行动，起诉主要是美国司法部的决定而美国行政当局无权干涉，希望中国能够采取更建设性的态度来重启对话。

进入 2015 年之后，中美两国各自继续采取努力以重建政府间网络安全对话机制，并在绕开僵局方面表现出了相当程度的灵活性：

首先，中美首脑之间围绕网络安全的对话和沟通事实上从未中断。中美两国最高领导人均非常重视网络安全，在多次的直接通话中均涉及网络安全问题，并达成了相关的共识。这些共识构成了推动两国政府在实践层面积极探索跨越障

碍的关键动力。2015 年 9 月，在对美国首次进行的正式国事访问时，中国国家主席习近平与美国总统奥巴马就网络安全议题达成了系列合作成果，分别涉及网络安全审查、商业领域加强信息通讯技术网络安全的一般措施、恶意网络活动提供信息及协助、反对网络窃取知识产权、制定和推动国际社会网络空间国家行为准则以及建立两国打击网络犯罪及相关事项高级别联合对话机制。这一系列成果的达成，扭转了中美网络安全议题摩擦持续上升的态势，为推进两国在网络安全领域的合作，奠定了扎实的基础。

其次，中美之间围绕网络安全问题的第二轨道以及业界合作始终处于较为通畅的阶段。美国战略与国际研究中心与中国智库之间的第二轨道对话机制已经形成了惯例；中美互联网产业论坛以及在论坛框架下举行的闭门论坛，构成了重要的产业界和研究者对话的渠道，2015 年 9 月 23 日，在国家主席习近平抵达华盛顿之前，他参加了在西雅图微软公司总部举行的第八届中美互联网产业论坛，并与出席该论坛的中美互联网企业代表合影，这张合影不仅构成此次国事访问最大的亮点之一，而且普遍被舆论解读为体现了中国作为全球最大网络市场对美国网络企业巨头所具有的吸引力。

截止目前的经验观察显示，几乎没有任何美国企业可以抗拒这一市场的吸引力，无论是被媒体捕捉到的脸谱公司创

始人努力向中国市场示好的举措，还是没有被媒体捕捉到的谷歌公司用各种方式展开的争取重新进入中国市场的游说，都在反复证明这种巨大吸引力的存在。从战略视角来看，这一吸引力可以转化为促进中美两国在网络问题有效维持战略稳定的重要资产。

再次，中美两国政府间围绕网络安全议题的危机管控与突发事件协作机制正在发育完善。2015 年 9 月中美首脑峰会之前，中美两国已经形成较为完善的特使互访机制。8 月底，美国总统特使国家安全事务顾问赖斯首先访华，就网络安全等相关议题向中方进行情况通报，并较为详细的阐释了美方行动的意图和可能的后续行动；9 月初，中方派遣孟建柱国务委员率公安、网信、国安、工信等相关部门成员出访美国，与外交部相关工作组一道，就美国人事局数据遭遇黑客攻击等问题向美方有关部门进行情况通报，并就中国遭遇来自美国黑客攻击等问题向美方提出协查要求。从实际效果看，相关沟通机制起到了增加信任，缓解紧张态势的作用，并初步产生了一定的积极效果。

作为最终的年度成果，2015 年 12 月中美双方仅用了 3 个月不到的时间，就举行了第一次打击网络犯罪及相关事项的部长级对话，初步实现了跨越僵局，实质性的就网络安全相关事项，再度启动了两国间有关网络安全的政府间对话机

制。尽管仍然存在诸多有待完善之处，但这种对话机制的存续，已经并且将继续成为中美两国在推进网络安全领域合作的重要机制保障。

2015 年中美两国网络安全战略的博弈，经历了从冲突摩擦剧增到显著缓和的转变，在此过程中，促成中美两国在网络安全领域合作的三项主要因素也梯次浮现：

其一，战略因素。中美两国战略决策层无意在网络安全议题上进行彻底的摊牌，管控分歧，促进合作，成为双方共同努力的方向。尽管存在诸多矛盾、分歧、猜忌、摩擦，但中美两国战略决策层均无意在网络安全议题上进行一场彻底的摊牌，无意在网络安全领域展开一场传统大国权力转移的较量。管控分歧，促进合作，避免网络安全议题的摩擦和分歧最终扩散到中美战略稳定的全局，构成中美两国最高领导人共同努力的方向。这一默认的战略性共识的存在，是维系网络安全议题，以及其他中美两国诸多战略、安全议题保持相对稳定的关键所在。

其二，利益因素。中美两国在全球网络空间的产业链和价值链已经形成牢固的利益-命运共同体，无法以传统的零和思维与模式来解决彼此间的分歧和摩擦。中美两国都希望从全球网络空间的稳定与健康发展中获益。对两国来说，从网络空间获益，无论是获取战略与安全领域的收益，还是获

取经济与社会文化领域的收益，保障各方，尤其是中美双方自愿、顺畅、便捷的接入全球网络空间，都是至关重要的前提。因此，这决定了中美双方必须有效尊重对方的核心关切，以一种照顾对方核心利益关切和基本舒适度的方式，推进实施自身的网络安全战略与政策。这最终导致中美之间网络安全领域的战略关系会趋于稳定。

其三，体系因素。与冷战时期人们熟悉的中美苏三角关系等战略博弈相比，中美两国在网络空间的战略博弈受全球体系因素的影响更多，中美双方都必须关注和考虑自身行为带来的系统影响，保障全球网络空间的战略稳定，供给满足全球网络空间发展趋势的秩序安排等，是中美两国共同面临的历史使命。同时，这构成了维持和保障中美网络安全战略关系稳定的体系因素，中美两国都无法超越这种体系性因素滥用自身的优势和实力来追求短期收益。在 2015 年，美国政府尽管多次威胁要制裁中国所谓涉及网络商业窃密的企业，通过《金融时报》等媒体以匿名放话方式予以公开点名，甚至通过总统特使直接向中国进行情况通报，但最终由于担心制裁可能导致中方强烈的报复性措施，以及由此带来的对全球网络安全生态体系的不良影响，美国最终还是没有采取相关的行动和措施。

整体来看，2015 年中美两国在网络安全领域重新启动、

建设、完善沟通对话机制的努力，仍然是非常清晰的。尽管在媒体传播中更引人瞩目的是冲突、对抗和摩擦，但在战略规划和政策实践中，两国战略层确实表现出了谋求务实合作的灵活、机动与弹性。务实谋求合作的努力，也最终取得了相应的成果。

三、网络主权的边界、网络情报活动的限度与国家网络安全的实践方式成为三大焦点

纵观 2015 年的中美两国在网络安全战略领域的博弈，整体上正在形成三大焦点议程，分别可以概括为：网络主权的边界之争、网络情报活动的限度之争与国家网络安全的实践方式之争。

网络主权的边界之争折射的是中美两国有关网络安全议题的指导原则之争。一般认为美国不倾向于承认主权原则适用于网络空间，而中国则倾向于强调网络主权。[6]但公开资料、“1.5 轨”与 2 轨的交流以及在联合国政府间专家组进行的多边磋商均显示，美方在言论和实践中并不真的拒绝或否认网络主权。[7]具体来说，美方有关网络主权的主张和认知大体上可以概括为如下要点：主权原则适用于网络空间，但这种适用不能阻碍跨境数据流动等关系全球网络空间有效互联的活动；主权原则的适用通过对领土范围内关键信息基

础设施的管辖以及对从事相关服务和活动的企业的司法管辖得到体现；美国有权在全球网络空间追求最大限度的行动自由，同时应该适度考虑其他国家的主权反应。

中方有关网络主权的主张和认识在经历了一段时间的发展和完善之后，于 2015 年 12 月经由国家主席习近平在第二届乌镇世界互联网大会上进行了比较系统和完善的阐释，其特点是：同样强调主权原则适用于网络空间，优先关注的是技术处于相对弱势的一方有权通过立法等非技术方式，实施对领土范围内网络活动的有效管辖；中方强调网络主权原则的至高性，认为跨境数据自由流动等应该服从网络主权的需求，不能以跨境数据自由流动削弱网络主权；在全球网络空间的治理和关键资源共享问题上，中方认为应该基于主权平等原则，确保弱势行为体平等享有利用网络资源促进发展的权利。

网络情报活动的限度之争是中短期内中美两国网络安全议题中最敏感和微妙的争议领域。尽管中美两国之间围绕互联网和网络空间的相关议题从 1994 年就开始了各种互动，但真正使得网络安全问题成为中美两国战略框架中焦点议题的，就是网络情报活动，具体来说，就是美方指控中方所谓“国家黑客”对美国系统展开网络商业窃密，以及斯诺登披露美方“肆无忌惮”通过“棱镜”系统实施全球网络空

间监控。坦率的说，这是一个迄今为止没有得到有效处置的敏感议题。美方过于随意以自我利益为核心构建解释框架，以及用一种含糊而不负责任的方式在公开媒体渲染中国黑客威胁，导致问题进一步趋向于复杂和敏感。

2015 年美方对美国人事局遭遇黑客攻击事件的处理，就是一个典型的案例：尽管美国情报总监克拉伯在国会听证会上公开承认这种黑客攻击就是传统的情报搜集活动；但美国政府在媒体上仍然将对人事局的黑客攻击与网络商业窃密混为一谈，用人事局大量数据遭到泄露作为新闻噱头和政治动员的工具，通过煽动对华网络安全恐惧心理的方式，来谋求扩展在网络安全领域的行政权力，谋求对华战略优势。而被过度渲染的中国网络黑客威胁，反过来又助长了对华网络安全的强硬派主张，并无助于以合作方式来解决中美网络安全问题。

未来对中美两国的考验是，如何以理性、务实的态度，尽快为网络空间的情报活动建立一套行之有效的行为准则，从而实现对分歧和矛盾的有效管控，避免因为个别案例影响中美网络安全关系全局乃至中美战略关系稳定。

国家网络安全的实践方式之争将在较长时期内影响中美网络安全战略关系的发展与走势。中美对于保障国家网络的实践方式存在不同偏好，美国偏好采取的是具有显著单边

主义、预防性防御色彩的行动，中国则偏好更加传统的主权国家自我防御的方式。2015 年 4-5 月，美国国防部通过的新版《网络空间行动战略》，反映了美国谋求国家网络安全的最新实践方式。这份战略文件的最重要特色就是“跨界”，即跨越军民两分的界限。一般认为，冷战结束以后，受制于冷战时期的传统实践，以及美国国内自由主义等理念的制约，美国政府，尤其是美国军方，在网络安全领域的基本实践有比较显著的“军民两分”特色，对民用网络空间的关键资源和基础设施保障，基本上处于司法机构、安全机构、情报机构的业务范围，并且美国国防部较少用军事力量介入民用关键基础设施。以对网络关键基础设施的攻击来实现危机管理和不战而屈人之兵，则更多停留在具体的情报安全机构的秘密行动实践，停留在国防部内部机密报告，停留在假想的作战场景，而较少出现在公开战略文件之中。但从这份战略文件的内容来看，这种区分正在被打破，由此所带来的后果，不仅是美国国防部的军事力量大规模涌入，而且还无法避免国防部对美国国家网络安全战略实践的主导。

在跨越“军-民”分界的同时，网络战略文件也进一步强化了威慑地位和作用，明确指出要通过国防部科学理事会有关网络威慑的任务力量、美国网军司令部、美国参谋长联席会议，以及美国国防部部长办公室等机构的协调运作，评

估国防部对特定国家与非国家行为体的网络威慑能力。施加威慑的对象，是那些能够对美国造成严重后果的网络攻击，包括造成人员伤亡、财产严重损毁，以及对美国外交和经济政策利益构成严重影响的行为。

因为跨越“军民两分”的界限，所以这份战略高度呼应参谋长联席会议正在研究的“全球公域介入与机动联合”概念，美国军方所拥有的资源和能力，将更加自如地在外空、海洋、网络空间等美军认定的行动作战领域内自由活动。被美国认定为是这些领域内的攻击方，或者潜在攻击方的国家、行为体，或者是被认定为威胁、限制美国在这些领域内行动自由的行为体，亦或者是被认为是美国主要战略竞争对手的行为体，将面临来自美国国防部的行动。

中方保障和实现网络安全的方式，受到技术、观念、体制与历史遗产等多种因素的影响，与美国存在显著的差异。从 2015 年前后的实践来看，完善立法，强化基于网络主权的政府管辖，谋求实现双边与多边的跨境合作，构成中国的主要选择。预计未来围绕中国颁布落实《网络安全法》等文件，中美还将展开新一轮的战略博弈。

四、中美网络安全战略领域短期趋于谨慎务实合作但仍面临艰巨考验

综上所述，2015 年，中美在网络安全领域关系一度趋于紧张，主要驱动力来自四个方面：其一，美国国内产业集团因遭遇黑客攻击或者对我网络安全政策制定持有疑虑，因此对政府进行游说施压；其二,美政府决策者对华战略焦虑增加；其三，美国人事管理局（OPM）遭遇空前规模的数据泄露刺激美国国内普通公众情绪；其四，自 2014 年起中美之间没有正式官方渠道就网络安全议题进行有规律的磋商。四股压力合流促成美对华战略施压。

2015 年 9 月，国家主席习近平对美国事访问，以及 12 月中美网络安全高官会首次实施之后，上述四个方面的压力均得到不同程度缓和，具体表现为：

其一，中美首脑峰会达成网络安全协议以及高官会召开提供了满足美方需求的对话渠道。2015 年 9 月中美首脑峰会达成网络安全协议，仅不到三个月时间，即在 12 月举行了首次高官对话，贯彻落实安全协议。此举被认为体现了中国政府通过对话解决网络安全议题的诚意。

其二，美国国内政治逐渐进入选举季节，总统选举而非应对中国战略威胁成为美政府相关部门、国会，以及智库和研究机构关注的焦点。美国国内政治的发展在 2015 年提前

进入了选举季，执政的奥巴马政府重心转向政治遗产的塑造，无意与中国继续在网络安全议题上深入纠缠。

其三，美国人事局遭遇黑客攻击的事件等失去新闻价值，被恐怖主义以及黑客攻击电网等基础设施的新威胁掩盖。2015 年 10 月之后，ISIS 在全球发动的恐怖袭击、在网络实施的宣传攻势以及黑客在圣诞节前后对乌克兰电网实施的攻击等新闻，取代美国人事局遭遇黑客攻击等“旧”新闻，成为各方关注的焦点。

基于上述发展，初步研判，在 2016 年的多数时间，除非出现重大突发事件，否则中美在网络安全领域将进入一个相对平稳发展的时期，但这种平稳是相对的，短暂的，脆弱的。预计在 2017 年美国新任总统产生之后，窗口期就可能趋于压缩乃至彻底关闭。

窗口期不会长期持续存在的本质原因，是影响中美网络安全趋于紧张的深层矛盾没有消失，而且还将长期存在：

其一，最主要的矛盾是实力趋于成长的中国需要在网络空间获得更多的行动自由，而占据优势乃至霸主地位的美国试图限制中国在网络空间自由行动的空间。网络空间是陆地、海洋、大气、外空之外的人类活动第五空间，在网络空间获得必要的行动自由，投射力量，捍卫利益，是所有大国，包括中国，的客观需要。尊重网络主权的本质，除了尊重各国

独立制定并执行网络管理政策的权利之外，还包括尊重各国在网络空间的合理行动，比如在网络空间开展情报搜集的行动，发展完善必要的网络攻击和防御能力的行动等。美国目前解决中美网络安全关系中矛盾和冲突的基本预期，是“（美国）施压-（中国）让步”。如何在管控分歧，避免“擦枪走火”的同时，有效的变革美方的战略预期，是中方在中短期内面临的首要战略挑战之一。

其二，最本质的矛盾是中美两国在网络领域的实力分配继续呈现不对称、不平衡，美国战略决策层始终面临在网络领域强势牵制中国整体崛起的巨大冲动。从中美两国在网络安全相关的技术、产业、制度和战略能力比较看，美国具有综合性的优势，相关实力在中美两国之间的分配不对称、不平衡；对美国来说，在不考虑网络领域时，面对综合国力不断接近美国的中国，除了直接动用军事手段进行打压之外，没有可行的战略选择；但现在美国决策者多了所谓“网络选项”，即通过网络空间对华施压有效的牵制中国的战略崛起。这种认知，是美国战略决策者根据其固有的思维逻辑和惯性，依据中美两国实力对比做出的选择，是冷战思维在网络领域的投射，短期内不太可能出现实质性的变化。

因为上述矛盾的存在，预计中美之间未来还将继续在网络安全领域展开复杂而微妙的互动，如何有效的管控分歧，

有效维持和保障中美两国在网络安全议题上的稳定与缓和，将日趋成为影响中美战略关系稳定的重要议题。

---

[1] 吴心伯主编：《中美关系战略报告 2013》，时事出版社，2014 年版，第 13 页；吴心伯主编：《中美关系战略报告 2014》，时事出版社，2015 年版，第 6 页

[2] Nguyen, Hang Thuy Thi. "Robert G. Sutter. The United States and Asia: Regional Dynamics and Twenty First Century Relations." *European journal of American studies* (2016).

[3] Kuehn, Andreas. *Extending cybersecurity, securing private internet infrastructure: The US Einstein Program and its Implications for Internet Governance.* Springer Berlin Heidelberg, 2014.

[4] Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and cybersecurity: espionage, strategy, and politics in the digital domain.* Oxford University Press, USA, 2015.

[5] David Sanger, "U.S. Decides to Retaliate Against China's Hacking", *New York Times*, July 31st, 2015, 来源：http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0 (最近访问：2016 年 2 月 1 日)

[6] Yuen, Samson. "Becoming a Cyber Power: China's cybersecurity upgrade and its consequences." *China Perspectives* 2 (2015): 53.

[7] 相关材料参见 CSIS-CICIR Dialogue，来源：http://csis.org/program/china-institute-contemporary-international-relations-cicir