美国网络安全战略调整与中美新型大国关系的构建

汪晓风

[内容提要] “斯诺登事件”引发美国国内和国际社会对美网络安全战略的广泛批评和质疑，奥巴马政府一方面调整网络情报活动的监视范围和获取方式，另一方面积极争取国内和国际社会的理解和支持，包括突出对私营部门的网络安全保护，促进政企间网络安全信息共享，加强法律和经济手段的运用，为网络空间国际行为确立规则，在同盟和伙伴体系中推动网络安全合作等。这些调整包含防范和规制中国的内容，中国应将网络议题纳入中美新型大国关系战略框架，塑造合作共赢的氛围，设置切实有效的议程，积极引导中美网络安全关系的走向。

[关键词] 美国 网络安全战略 中美新型大国关系

[作者介绍] 汪晓风，复旦大学美国研究中心、中美新型大国关系协同创新中心助理研究员、博士，主要从事美国政治与外交、网络安全与网络外交研究。

2015 年以来，美国政府陆续推出多项有关网络安全的重要措施。2 月，发布《国家安全战略报告》，提升网络安全战略地位，规划综合运用法律、经济、外交和军事手段预防和反击网络攻击，①白宫发起促进私营部门与政府共享网络安全信息的倡议。②4 月，奥巴马签署行政命令，对网络攻击实行经济制裁，③随后国防部推出新《网络战略》，突出积极防御、主动进攻和全面威慑战略；④国会众议院也推动“网络安全增强法案”，加强网络安全信息共享和隐私及公民权利保护；⑤新修订的《美日防卫合作指针》也正式纳入网络防御合作的内容。⑥ 这一系列政策调整反映出美国进一步寻求网络空间绝对安全和维持网络空间优势地位的意图，也包含了“棱镜计划”等网络情报项目曝光后修复关系和重建信任的努力。值得注意的是，美国政府既将所谓中国窃取网络商业机密等威胁作为政策调整的动因之一，也将遏制中国网络空间能力增长作为政策调整的一个目标。本文拟对近期美国网络安全战略调整的重点、防范和规制中国的政策措施及其影响进行分析，并探讨如何在中美新型大国关系框架下进行有效应对。

一、美国网络安全战略的调整

2011 年奥巴马政府推出《网络空间国际战略》，全面勾画了美国综合运用外交、军事、经济、司法和

① U. S. White House, “National Security Strategy of 2015”, February 2015, p. 13, http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf. (上网时间: 2015 年 4 月 15 日)

② Barack Obama, “Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing”, February 13, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari. (上网时间: 2015 年 4 月 15 日)

③ Barack Obama, “Executive Order: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities”, April 1, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m. (上网时间: 2015 年 4 月 15 日)

④ U. S. Department of Defense, “The Department of Defense Cyber Strategy”, April 15, 2015, http://www.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf. (上网时间: 2015 年 4 月 18 日)

⑤ U. S. House of Representatives, 114 Congress, “H. R. 1731: National Cybersecurity Protection Advancement Act of 2015”, April 13, 2015, https://www.congress.gov/114/bills/hr1731/BILLS-114hr1731ih.pdf. (上网时间: 2015 年 4 月 18 日)

⑥ “Guidelines for U. S.-Japan Defense Cooperation”, April 27, 2015, http://www.defense.gov/pubs/20150427_--_guidelines_for_us-japan_defense_cooperation_final&clean.pdf. (上网时间: 2015 年 4 月 28 日)

情报手段在网络空间促进国家利益及保护安全、开放和可信网络空间的战略。这一战略成为指导美国国务院、国防部、司法部、商务部、国土安全部等联邦职能部门制定网络空间运行和保护政策的纲领性文件。① 在该战略指引下,美国外交上积极倡导网络开放和网络自由,通过社交媒体等网络传播干预他国社会政治进程;军事上由网络司令部统领网络部队攻防能力建设,通过以劝阻和威慑为核心的预防性防御以应对各类网络威胁;国际上构建志同道合的伙伴关系,推动网络行为规范和网络冲突国际法的讨论和制定等。

2012 年底迪拜国际电信世界大会促使奥巴马政府重新审视其网络安全战略的国际支持度。对于网络空间的国际治理,美国一直坚持多利益攸关方模式,认为互联网不能由各国政府控制,政府作用应限于国内公共政策的制定,也反对政府间国际组织介入互联网事务。② 迪拜大会争议焦点之一为是否将互联网治理纳入国际电信联盟议程,会议结果显示美国已沦为少数派,特别是多数互联网普及率较低的发展中国家出乎意料地站在了对立面,这令美国意识到它并不具备单边主导网络空间国际事务的能力,国会对于美国的政策主张失去国际支持非常不满,一些国会议员因而敦促政府设法寻求更广泛的国际共识。

美国网络情报活动的曝光使奥巴政府面临更大的国内外压力。2013 年 6 月斯诺登揭秘美国情报部门长期、大规模和系统性地入侵和监控全球互联网和各国通讯网络,显示美国政府在网络安全问题上的自私任性及对它国网络空间主权、安全和发展权益的漠视,这就使得美国网络空间守护神的光环褪色。国际社会纷纷质疑美国主张网络开放和网络自由的真实意图,一些国家开始加强网络防御措施和进行网络安全审查,美国主要互联网企业的海外业务大受影响。美国国内舆论也要求限制情报部门获取网络数据的方式和范围,加强个人隐私保护。这些都促使奥巴马政府对其网络安全战略进行调整,转向重视多方合作,选择切实可行的手段,以达成较为务实的目标。

首先,突出保护私营部门利益和重建政企信任。美国绝大多数网络基础设施和网络应用服务由私营部门构建和运营,美国企业也参与建设许多国家的关键信息基础设施和通信系统,美国众多高科技公司是推动全球网络空间迅速发展的活跃主体,在互联网及移动通讯领域的技术、规则和应用方面保持领先地位和持续创新能力,这些公司拥有全球最大的互联网用户群体,管理着最大规模的用户信息和运行数据,因而获取私营部门的支持就成为美国网络安全战略的关键依托和重要保障。而美国私营企业特别是互联网企业对与政府合作持复杂心态:既希望政府帮助其在国际市场获得平等竞争机会,协助其在国内市场上打压外来竞争对手,又担忧与政府过从甚密会影响其海外业务。"斯诺登事件"使美国政府与私营部门的默契合作出现裂痕,一些互联网企业刻意与政府保持距离,与网络情报项目撇清关系,谷歌、雅虎、脸书等公司高管拒绝参加 2015 年白宫网络安全与消费者保护峰会即是最新一例。③ 奥巴马政府因而将重建政府信任与改善政府及互联网企业之间的合作置于优先地位,④加强私营部门应对网络安全威胁的指导,同时通过立法和行政命令要求私营部门分享更多网络威胁信息,因为这些信息对于防范网络攻击和获取网络情报都至关重要。在白宫网络安全峰会上,奥巴马呼吁企业领导人和政府机构更密切合作以应对网络攻击,同时签署了一项建立企业与政府共享网络信息框架的

① U. S. White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World", May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. (上网时间:2015 年 4 月 15 日)

② Lennard G. Kruger, "Internet Governance and the Domain Name System: Issues for Congress", January 2, 2013, p. 6, http://www.fas.org/sgp/crs/misc/R42351.pdf. (上网时间:2015 年 4 月 15 日)

③ 美国白宫网络安全与消费者保护峰会(White House Summit on Cybersecurity and Consumer Protection)2015 年 2 月 13 日在斯坦福大学举行,峰会由美国总统奥巴马主持,美国主要互联网巨头均接到与会邀请,但谷歌、雅虎和脸书的高管拒绝与会。参见:http://www.bloomberg.com/news/articles/2015-02-11/three-of-tech-s-biggest-ceos-to-skip-obama-cybersecurity-summit. (上网时间:2015 年 4 月 15 日)

④ U. S. White House, "National Security Strategy of 2015", February 2015.

行政命令。[①] 出于缓解私营部门担忧的考虑，也是迫于国内呼吁保护个人隐私的压力，奥巴马政府对情报部门获取网络数据进行了一些限制，如将数据保存在运营商的服务器、提高情报监视活动透明度、进行更严格的情报授权审核、[②]删除确认无情报价值的美国公民信息等。[③] 国防部新《网络战略》也将建立与私营部门和研究机构更紧密合作的新机制作为网络部队建设的重点，“必须吸引来自私营企业的优秀人才、创意和技术”。[④] 白宫网络安全峰会和国防部新《网络战略》发布会均选择在硅谷发源地的斯坦福大学召开，就凸显了美国政府向私营企业示好的姿态。

其次，注重应用法律、经济手段遏制外部网络攻击。近年来，针对美国政府部门、私营企业和非政府组织的网络攻击事件持续增多，其攻击源来自其它国家的政府、网络犯罪组织和个人。美国政府宣称运用技术手段侦测到一些网络攻击源，如索尼影业事件中将侵入索尼公司网络窃取内部资料者锁定为朝鲜政府支持的黑客，但如果没有相关国家配合，就既无法最终确认攻击源和攻击者，也无法通过政府间合作有效阻止类似攻击。在网络安全国际治理问题上，美国政府不希望联合国等政府间国际组织获得主导权，其原因主要是担忧一国一票决策方式对其不利，也不愿意与其他国家进行平等对话。单边的法律和经济手段逐渐成为美国政府应对外部网络攻击的重要选项，即针对其所认定的网络攻击者提起刑事诉讼和实行经济制裁，如美国司法部 2014 年 5 月以网络窃密为由起诉五名中国军人和 6 月以网络欺诈和洗钱为由起诉俄罗斯黑客，2015 年 1 月美国总统奥巴马签署行政命令对朝鲜数个实体和个人实施制裁，以回应朝鲜“对索尼影娱的破坏性和胁迫性网络攻击”。[⑤] 新《国家安全战略报告》称美国将依据本国法律和国际法，通过司法行动提高攻击者代价，防范与应对网络攻击。报告还强调对网络攻击行为溯源的重要性，并指出由于一些政府、犯罪组织和个人试图阻止溯源，美国政府将同国会合作推出高水平的立法框架，制订更有效的网络安全标准。[⑥] 2015 年 4 月奥巴马签署行政命令，授权财政部对实施恶意网络活动、对美国国家安全、外交政策、经济安全和金融稳定构成显著威胁的个人和组织实施制裁，从事网络攻击的个人或组织资产将被冻结，禁止入境美国、禁止与美国公民或公司进行商业往来。[⑦]

第三，强调领导国际规则制定和主导网络安全治理。奥巴马政府将塑造国际秩序作为国家安全战略支柱之一，在处理国际事务时越来越多地强调规则，一则是由于美国总体实力优势和国际影响力非比往昔；二则是出于奥巴马自由主义的世界秩序观；三则是因为该领域的秩序有待形成和规则远未完善，美国欲占得先机将其政策选择确定为国际规则。如斯诺登揭秘国家安全局棱镜计划后，奥巴马政府的第一反应是为其辩护，继而刻意将网络监控及网络窃密以商业获益和国家安全目的进行区分，试图赋予基于反恐及国家安全目的的网络情报活动以国际合法性。新《国家安全战略报告》强调美国致力于塑造网络安全全球标准，[⑧]具体措施包括在现有各种网络治理国际平台推动机制化合作、为双边和

---

① Adam Gorlick, “Obama at Stanford: Industry, Government must Cooperate on Cybersecurity”, January 13, 2015, http://news.stanford.edu/news/2015/february/summit-main-obama-021315.html. (上网时间: 2015 年 4 月 15 日)

② 美国总统奥巴马 2014 年 1 月 17 日发布情报改革政策指令，包括对收集通话记录等情报活动加强监管，提高情报监视活动透明度、限制情报部门拦截国际通讯信息的权限、提高联邦调查局使用国家安全密函的透明度、不再由政府保存通话记录等措施。参见: “PPD-28: Signals Intelligence Activities”, January 17, 2014, https://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf. (上网时间: 2015 年 4 月 15 日)

③ 美国政府 2015 年 2 月 3 日宣布修改 PPD-28 指令部分内容，要求情报分析人员删除没有情报目的美国公民个人信息，并在 5 年内删除类似外国公民个人信息。参见: https://www.whitehouse.gov/the-press-office/2015/02/03/statement-assistant-president-homeland-security-and-counterterrorism-lis. (上网时间: 2015 年 4 月 15 日)

④ U.S. Department of Defense, “Fact Sheet: the DoD Cyber Strategy”, April 23, 2015, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf. (上网时间: 2015 年 4 月 26 日)

⑤ Barack Obama, “Executive Order: Imposing Additional Sanctions with Respect to North Korea”, January 2, 2015, https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea. (上网时间: 2015 年 4 月 15 日)

⑥ U.S. White House, “National Security Strategy of 2015”, February 2015, p. 13.

⑦ Barack Obama, “Executive Order: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities”, April 1, 2015.

⑧ U.S. White House, “National Security Strategy of 2015”, February 2015, p. 2.

多边国际网络安全合作提供专业支持。美国政府还支持东西方研究所、战略与国际研究中心等智库发起和组织各种网络安全国际会议，邀请网络安全和国际法领域专家参与二轨对话，指导一些国家的网络安全战略设计，规划各类国际网络安全合作议程。这些措施旨在有效扩展美国网络安全战略的国际影响力，寻求国际社会对美国价值理念和政策主张的理解、认同和支持。

第四，加强盟国伙伴政策协调及多方网络安全对话。此前美国政府自恃其创建和繁荣互联网的独特贡献、技术领先优势和对核心网络资源的控制，提出建立“志同道合者伙伴关系”，[①]期待其盟友伙伴自觉支持其战略目标和政策主张。在迪拜国际电信世界大会上，美国不仅未获多数发展中国家的支持，一些传统盟友也未与其统一立场，一些国会议员则对失去众多潜在支持者深感不满并要求改进。其后奥巴马政府开始把重点转向与其老盟友及新伙伴的实质性合作及政策协调，意图将网络安全议题纳入既有军事同盟体系中，包括在北约框架下加强网络安全立法和网络防御合作；在美日安全磋商机制中增加网络安全内容并将网络防御纳入新修订的《美日防卫合作指针》，规定美军和日本自卫队将密切协商和采取行动共同应对网络威胁；[②]美韩、美澳等双边网络安全合作也不断充实。

与此同时，美国也日益重视与竞争对手或秉持中立立场的国家进行对话与合作，相继与俄罗斯和中国等建立网络事务对话机制，倡议与印度合作制定网络安全国际标准。对那些互联网应用水平较低、对网络安全关注度不高的国家，美国也吸取国际电信世界大会的教训，希望它们在关键时刻能站在美国一边，如利用东盟－美国领导人会议提升双方网络安全合作、与非洲国家合作设立网络安全与网络犯罪工作组等。

总体上，奥巴马政府网络安全战略的调整主要体现在政策层面，目标是继续维持美国的实力优势和主导地位，仍坚持美国对于网络空间国际秩序的领导权和网络空间核心资源的控制权。对于美国网络安全战略的上述调整，可以从两个方面理解：其一，美国并未放弃单边主义的网络安全理念，无论是加强经济、外交、军事、司法等政策工具的使用，还是推动以联盟体系为基础的网络安全国际合作，其核心都是在以美国主导和自身安全和利益最大化的前提下展开的；其二，美国提升网络安全战略地位既有网络环境风险和网络攻击威胁不断增强的客观现实，更是基于国家安全战略的总体考虑，如国防部新《网络战略》将未来五年网络作战的重点放在中东、亚太和欧洲，并将中国、俄罗斯、伊朗和朝鲜等列为构成网络威胁的重点国家。[③] 美国网络作战的重点与其国家安全战略的地缘政治重心基本一致，这并非巧合，而是美国不断寻找新威胁、塑造新敌人的思维定势和决策逻辑使然。

二、对中国的防范、规制与合作

由于中国在网络空间的利益、能力和影响力持续增长，近年来中美在网络安全问题上的矛盾和冲突也逐渐增多，美国的网络安全政策调整也就具有相当多针对中国的考虑。在美国的网络安全战略中，中国既是可以为美国企业带来巨额利润的合作伙伴，也是日益挑战美国网络空间领导地位和网络治理主导权的竞争对手，中国还被美认定为窃取其商业机密及攻击其网络系统的威胁来源。因而美国逐步明确在网络安全议题上对中国防范、规制与合作的多手策略。

首先，加强对中国的防范和遏制能力。基于意识形态、政治制度和发展模式的差异，美国对中国的防范意识和遏制政策不会改变，在网络安全领域，其对中国的防范、遏制则有不断强化的趋势。美国认定中国对其构成现实和潜在的网络安全威胁，必须构建防御不确定的网络攻击的能力及应对与中国发生网络冲突的局面。就防范意识而言，美国认为中国政府和私营部门长期为商业利益窃取美国企业和贸易机密，中国网络攻击能力发展迅速，并已可通过

① U. S. White House, “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”, May 2011, p. 21.

② “Guidelines for U. S. – Japan Defense Cooperation”, April 27, 2015.

③ U. S. Department of Defense, “The Department of Defense Cyber Strategy”, April 15, 2015, p. 9.

网络瘫痪美国电网,[①]美国防部新《网络战略》也明确点名称中国对美国网络安全构成“关键威胁”。[②]这些认知增强了美国将与中国发生网络冲突的担忧,新《国家安全战略报告》表示美方将从实力立场出发管控中美之间的竞争,并再次把网络窃密的矛头指向中国政府,称“就网络安全问题而言,我们将采取必要措施,保护我们的商业企业及维护我们的网络,以对付窃取贸易机密以获取商业收益的网络窃贼,不论是个人行为者还是中国政府”。[③]

针对中国管控互联网的技术和政策不断成熟,及美国军方认定中国进行信息封锁和信息控制的网络防御能力的不断增强,[④]奥巴马政府逐步确立以实力地位和管控预防为导向的在网络空间遏制中国的政策措施,一方面加强遏制中国互联网和通讯技术的技术进步和产业发展,保持对中国网络空间攻防能力的优势,美国限制加密算法和高性能芯片对中国出口[⑤]、阻止中国企业在美国市场上销售网络通讯产品等都是美在网络安全领域加强遏制中国的具体措施;另一方面是构建以美国及其盟国为核心的国际网络安全合作体系。美国及其盟友间的网络安全合作往往将中国作为重要的防范和遏制对象,如《美日新防卫合作指针》中间报告提出美日将加强网络合作,包括“平时和应急状态下共享网络威胁和安全漏洞信息,以及加强作战时的网络安全保证”,[⑥]作为美日从平时、有事到战时任何阶段进行“无缝合作”的关键环节,其中显然包含针对中国的意图。

其次,规制中国网络空间政策和行为。在中美综合实力和国际影响力此长彼消的趋势下,美国认识到无论在经济、政治和军事领域对中国实行对抗和遏制政策都会形成斗则两伤的局面,因而规制中国成为奥巴马政府的现实选择。新《国家安全战略报告》要求中国在海上安全、贸易、人权等问题上维护国际规则和准则,[⑦]在网络安全问题上也同样要求中国遵守规则,但规则选取和评判标准须以美国国家利益和战略目标而定,如美国刻意对商业机密和政治军事情报进行区分,以维持其监控全球网络及侵入各国网络系统的合法性,这种选择性守规矩的做法自然无法得到中国认同。另外,美国还致力于建立符合其利益和战略目标的行为规范和国际法框架,包括倡导以布达佩斯《网络犯罪公约》[⑧]作为打击网络犯罪的国际法文本,推动以北约卓越合作网络防御中心的建议性文件《塔林手册》[⑨]作为网络战的国际法规范,从而掌握网络空间国际规则的制定权和主导权,意图规制包括中国在内的世界各国网络安全相关政策和立法。

对于中国倡导和主张的网络空间国际行为准则,美国则采取排斥和反对的态度,如 2011 年中俄等国提请联合国大会讨论《信息安全国际行为准则》,美国政府反应消极,美国会众议院甚至要求其常驻联合国代表反对该议案,其理由是美国认为“该行为准则为政府排它性地控制互联网资源寻求合法性,否定确保互联网繁荣的多利益攸关方模式,对信息自由流动构成威胁”。[⑩] 2015 年 1 月中俄等

---

① 美国国家安全局局长兼网络司令部司令迈克尔·罗杰斯(Michael Rogers)2014 年 11 月 20 在众议院情报委员会听证会上的证词,http://intelligence.house.gov/hearing/cybersecurity-threats-way-forward.(上网时间:2015 年 4 月 15 日)

② U.S. Department of Defense, “The Department of Defense Cyber Strategy”, April 15, 2015, p.9.

③ U.S. White House, “National Security Strategy of 2015”, February 2015, p.24.

④ U.S. Office of the Secretary of Defense, “Military and Security Developments Involving the People's Republic of China of 2013”, May 2013, http://www.defense.gov/pubs/2013_china_report_final.pdf, p.32.(上网时间:2015 年 4 月 15 日)

⑤ 据《华尔街日报》网站 2015 年 4 月 9 日报道,中国与超级计算机“天河二号”有关的四个技术中心被列入美国政府的一个禁止出口名单,名单上的实体被认定从事违反美国国家安全或外交政策利益的活动。参见:Don Clark, “U.S. Agencies Block Technology Exports for Supercomputer in China”, April 9, 2015, http://www.wsj.com/articles/u-s-agencies-block-technology-exports-for-supercomputer-in-china-1428561987.(上网时间:2015 年 4 月 15 日)

⑥ “The Interim Report on the Revision of the Guidelines for U.S.-Japan Defense Cooperation”, October 3, 2014, http://www.defense.gov/pubs/20141003_interim_report.pdf.(上网时间:2015 年 4 月 15 日)

⑦ U.S. White House, “National Security Strategy of 2015”, February 2015, p.23.

⑧ 《网络犯罪公约》(Cybercrime Convention)是 2001 年 11 月由欧洲委员会 26 个欧盟成员国以及美国、加拿大、日本和南非等 30 个国家在布达佩斯共同签署的国际公约,是世界上第一部针对网络犯罪行为制订的国际公约。截至 2015 年 1 月,已有 53 个国家加入了该公约,其中 44 个国家签署了公约。参见 http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.(上网时间:2015 年 4 月 15 日)

⑨ Michael N. Schmitt ed, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.

⑩ 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”, April 19, 2012.

国提交该准则的新版本，美国政府再次表示“关注”和“担忧”，理由仍是“使政府控制网络资源合法化和限制网络基本自由”。①

对于中国政府加强国内网络治理的政策措施，美国也指责中国设置国家级网络防火墙和进行广泛的内容审查，要求中国遵守不受限制的网络言论自由等所谓全球通行规则。美国国务院认为中国主导制订的贸易协议在保护网络开放等方面不能达到美国推行的高标准，如针对谷歌搜索引擎和邮件服务进行的封锁致使中国的公司可以从中获利，而美国公司则因而无法进入中国市场。②

美国还罔顾美方长期以信息安全产品审查制度限制中国企业在美投资和经营活动的事实，指责中国的反市场垄断执法和将美国一些企业的产品移出政府采购名单是贸易保护行为和包含政治目的，要求中国遵守国际贸易规则和双边贸易承诺。奥巴马虽然曾表示美国不能要求它国遵守规则而自己却置身事外，言下之意是要建立共同遵守的标准，但总体上，美国仍意图以其制定或认可的规则来约束中国。

第三，维持与中国开展网络安全合作的意愿。现在美国上下比较一致地将中国视为对美国网络基础设施和网络商业机密形成威胁的主要国家。即便如此，美国也认识到在没有中国参与和认同、中美在网络主权和网络治理等原则问题上立场对立的情况下，不可能建立有效的网络空间秩序和美国需要的网络安全。奥巴马政府第一份《国家安全战略报告》曾表示中美两国不可能在每个问题上都达成共识，但意见不同不应该妨碍美中双方在共同利益领域进行合作，中美之间发展务实有效的关系是应对 21 世纪主要挑战的关键。③ 新《国家安全战略报告》也强调美中两国虽然面临竞争，但冲突并非不可避免，美国将寻求与中国发展建设性关系，这将给中美两国人民带来好处，并促进地区和世界的安全和繁荣。④ 这表明，美国政府认为发展与中国各领域的建设性与互利性合作关系符合其国家利益和战略目标。

自从 2013 年“曼迪昂特报告”指称中国军人窃取美国商业机密以来，美国政府通过各种渠道对中国施压，造成了中美网络安全关系的紧张局面。但美在成立中美网络工作组、促进双方合作打击网络犯罪、加强两国互联网应急中心协调与合作、建立中美网络空间国际规则对话等问题上仍持积极姿态。2015 年 2 月中美元首通电话时，奥巴马呼吁两国努力尽快缩小双方在网络安全问题上的分歧。⑤ 美国政府还通过各种渠道要求中国同意恢复中美网络工作组接触。

对于中国《反恐怖主义法》草案要求包括中国境内的电信业务经营者、互联网服务提供者在电信和互联网的设计、建设和运行中预设技术接口，将密码方案报主管部门审查等，美国总统奥巴马认为这将伤害美国在中国运营企业的商业利益，并要求中国更改，同时也表示美国“仍然致力于扩大与中国政府就网络安全方面的合作”。⑥ 美国国防部新《网络战略》也提出要通过双边防务磋商等渠道，增进中美之间在网络空间军事原则、政策、角色和人物等的理解和透明度，以保证战略稳定，降低误解和误判风险，避免冲突升级。⑦ 这些都显示与中国加强网络安全领域的对话与合作仍然是美国网络安全战略的重要选项。

总之，美国在网络安全问题上采取对中国防范、规制和合作的多手策略，既是基于其对中美关系发展方向的整体考虑，也是基于对中国网络能力增长和安全战略选择的综合判断和应对，特别是中国成

① 美国国务院副发言人玛丽·哈夫(Marie Harf) 2015 年 3 月 2 日记者会回答关于中俄《信息安全国际行为准则》问题，http://www.state.gov/r/pa/prs/dpb/2015/03/238132.htm.（上网时间：2015 年 4 月 15 日）

② 美国国际通讯和信息政策协调官、助理副国务卿丹尼尔·塞普尔韦达(Daniel Sepulveda) 2015 年 2 月 11 日关于“促进贸易和维护互联网开放”的讲话。见 http://www.state.gov/e/eb/rls/rm/2015/237436.htm.（上网时间：2015 年 4 月 15 日）

③ U.S. White House, “U.S. National Security Strategy of 2010”, May 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf. p43.（上网时间：2015 年 4 月 15 日）

④ U.S. White House, “U.S. National Security Strategy of 2015”, February 2015, p.23.

⑤ “习近平应约同奥巴马通电话，推动中美新型大国关系建设”，《人民日报》(海外版)，2015 年 2 月 12 日。

⑥ 美国国务院副发言人玛丽·哈夫(Marie Harf) 2015 年 3 月 2 日记者会回答关于中国《反恐怖主义法》草案要求在华企业预设技术接口及向主管部门提交密码方案对美国企业的影响及美国政府的立场。见 http://www.state.gov/r/pa/prs/dpb/2015/03/238132.htm.（上网时间：2015 年 4 月 15 日）

⑦ U.S. Department of Defense, “The Department of Defense Cyber Strategy”, April 15, 2015, p.28.

立中央网络安全和信息化领导小组并提出与“两个一百年奋斗目标”同步推进的网络强国战略之后，美国对中国的防范意识更为突出。美国外交关系委员会的一份报告认为，美国现有将中国的经济和政治发展纳入美国主导的国际秩序的做法不利于美国长期的战略利益，“美国应平衡崛起的中国的力量，而非协助其已有优势”。报告建议在网络安全问题上采取“更加强硬的对抗中国在网络空间行为的措施”。①

近年来美国在处理中美网络安全关系时对抗性日益明显就体现了美国在网络安全领域针对中国的这种平衡主义思维，其结果是中美在网络安全问题上的相互疑虑不断加深，一方加强自身网络安全的一举一动往往会被对方理解为针对自己的限制性甚至对抗性措施而引发指责，而近期两国推出的网络安全相关战略、政策、措施和立法又都比较密集，从而形成两国网络纷争一波未平一波又起的局面。因此，促使中美在网络安全关系上建立相对清晰的战略认知、战略定位和机制保障，就显得尤其重要。

三、如何在新型大国关系框架下推进中美网络安全合作?

中国正在积极推进构建中美新型大国关系，这是着眼中美关系长期稳定发展的战略举措。新型大国关系适用于中美关系各个领域，“不冲突、不对抗，相互尊重，合作共赢”的理念也应作为处理中美间网络安全议题的指导原则。维护和发展开放、稳定和安全的网络空间，符合中美两国共同利益，中国应积极推动两国在网络安全的理念、利益和政策上形成契合点。

首先，建立避免网络冲突与对抗的共识和机制。新型大国关系意味着客观理性看待双方战略意图，以对话合作而非对抗冲突的方式处理矛盾和分歧。中美网络安全关系的现状是共识不足和机制缺失，因此一方面要增进共识，倡导基于共同安全的网络安全观，中美间网络安全领域的相互疑虑已经形成但应避免继续加深及防止新的冲突，充分交流及增加透明度有助于更准确认知对方的战略意图和政策选择。还应认识到中美对网络安全的认知都有一个动态发展的过程，并非完全不可调和，如针对中国主张的网络主权，美国也有观点认同国家主权适用于网络空间。美国战略与国际研究中心的詹姆斯·刘易斯(James Lewis)就曾表示“国界确实存在，正是因为有了国界，所以各国的主权在网络空间上仍然是适用的”、“需要一个针对全球的、适用于各国主权的新治理模式”。对于网络安全问题上的大国合作，刘易斯也认为“需要各国达成共识，尤其是需要一些主要大国达成共识”。② 中美应肯定并扩展此类共识。另一方面要建立机制，规制各自网络空间的活动和行为，包括重大事项通报机制、重要政策协调机制、危机防范预警和应急处理机制等。网络安全议题涉及科技、经贸、军事、司法等多个领域，机制建设也应从多个职能部门间展开。针对不同领域的网络安全问题，可利用已有双边机制，或创设新的机制。

其次，尊重对方网络领域核心利益和重大关切。新型大国关系意味着切实尊重双方价值理念和制度选择，以兼容并行和求同存异的认知促进共同发展。中美在网络安全问题上的理念、利益和目标均存在差异甚至对立，但对于维持开放、和平、有序、安全的网络空间仍有基本共识，以网络互联互通促进各自经济社会进步是双方不断增长的共同利益，而不断增长的网络攻击和网络恐怖主义是需要双方合作应对的共同威胁。因此，中美之间一方面要有相互尊重之心，中国对美国创建国际互联网及发展全球网络基础设施的历史贡献应予以充分肯定，对美国在网络空间已形成的主导地位或特殊利益给予适当尊重，对美国强化网络情报活动应对恐怖主义威胁的政策表达应给予必要理解。同时，美国也应切实尊重和理解中国在治理主权范围内加强网络事务管控的正当性和必要性。另一方面中美要有相互照顾之行，双方应各自限制针对或涉及对方的网络攻击和

① Rober D. Blackwill, Ashley J. Tellis, *Revising U. S. Grand Strategy toward China*, Council on Foreign Relations, March 2015, http://i.cfr.org/content/publications/attachments/China_CSR72.pdf, pp. 26 – 27. (上网时间: 2015 年 4 月 15 日)

② 美国战略与国际研究中心战略技术项目主任詹姆斯·刘易斯 2014 年 11 月 19 日在乌镇世界互联网大会网络空间安全和国际合作分论坛上的发言，http://www.wicnews.cn/system/2014/11/19/020368252.shtml. (上网时间: 2015 年 4 月 15 日)

网络情报活动，不扩散可能损害对方网络安全和国家安全的软件和应用，就中国在联合国的相关呼吁达成共识，包括“各国应承诺不利用信息网络技术实施敌对行动，制造对国际和平和安全的威胁，不扩散信息和网络武器及相关技术”，①并妥善处理双方网络安全审查措施与双边市场开放和自由贸易承诺的矛盾，避免各自寻求自身网络安全的政策措施损害对方的主权、安全和发展利益。

第三，以共赢理念促进网络安全领域务实合作。新型大国关系意味着摒弃零和思维，在追求自身利益时兼顾对方利益，促进共同发展。作为世界上两个最重要的国家，中美共同为世界的和平与发展做出贡献、为世界提供公共产品，可以作为发展新型大国关系的一个着眼点。②

网络空间的发展及其与世界经济社会各领域的不断融合，在促进各国经济增长和社会进步的同时，也逐渐形成了一个包含前所未有风险和形形色色威胁的全球共享新领域。中国应促使美国认识到中美促进网络空间安全和发展的共同利益、共同责任和共同使命。国际上任何一个公共领域的规则制定和秩序维护，莫不是由该领域主要大国主导，并由利益攸关方共同参与来达成的。作为两个最大的互联网国家，中美在网络安全问题上的合作空间远大于双方的矛盾和冲突，中美就网络空间安全和发展的基本原则达成共识，建立共同遵守的网络行为规范是实现建立有效的网络空间国际秩序最重要的基础。

鉴于美国司法部起诉中国军人网络窃密案致中美网络工作组活动中断，且双方都难以做出实质性让步，中美两国一方面可利用双方政府职能部门和专业组织间的双边和多边机制拓展网络安全领域务实合作，如中美刑事司法协助协定下的司法合作、中国公安部和美国国土安全部的反恐合作及国家互联网应急中心国际合作伙伴机制下的技术合作；另一方面可主动进行国际多边政策协调，如迪拜国际电信世界大会前美方代表团来华与中方协调立场的做法值得肯定。中美还可提出共同创设国际多边网络安全协调机制，或共同推动将网络安全议题纳入联合国相关议程。

中美新型大国关系是中国倡导推动的大国关系新模式，是为了避免陷入新兴大国和守成大国由于实力变化和利益转移而必然伴随的矛盾、对立和冲突及至以战争方式完成权力格局重建的历史宿命。作为信息时代世界经济社会运行的重要基础，网络空间能否避免重复历史上大国间争夺核心资源控制权的命运，而成为一个和平、合作和共享的新型空间，也将考验新型大国关系在解决更广泛的国际和平与发展问题的适用性。

结语

网络安全议题事关中美新型大国关系的未来，妥善处理将形成正向推动力，处理不好则将成为重大阻力。中美元首加州会晤时就网络安全问题达成重要共识，即，中美两国要在合作共赢的新型大国关系目标框架下构建国际合作新模式，共同应对包括网络安全在内的各种全球性挑战。习近平主席指出，中美双方在网络安全上有共同关切，双方应消除猜忌、进行合作，使网络安全成为中美合作新亮点。③ 但其后局势发展显然偏离了这一期待。中国应积极和坚定地以新型大国关系理念引导和处理中美间网络安全议题，实现中国建设网络强国与构建中美新型大国关系两大战略之间的良性互动。

中美网络安全战略的相互影响、相互塑造是一个长期和渐进的过程，中方应当主动促进中美就网络安全议题展开对话与合作，寻求双方在网络空间的利益和关切的契合点，引导两国网络安全战略和政策相向而行，寻求并扩展两国网络安全相关经贸、政治、军事政策的兼容性，防止中美在网络空间形成新的对立和冲突。而所有这些，都是构建中美新型大国关系的应有之义。○

（责任编辑：沈碧莲）

① 中国特命全权裁军大使王群 2011 年 10 月 20 日在联大一委关于信息和网络空间安全问题的讲话，见中国常驻联合国代表网站“携手构建和平、安全、公正的信息和网络空间”，http://www.china-un.org/chn/zgylhg/cjyjk/ldyw/t869409.htm.（上网时间：2015 年 4 月 15 日）

② 达巍“构建中美新型大国关系的路径选择”，《世界经济与政治》，2013 年，第 7 期，第 70 页。

③ “习近平同奥巴马举行中美元首会晤，在新起点上开展跨越太平洋的合作”，《人民日报》（海外版），2013 年 6 月 10 日。

Abstracts

Establishing a Strategic Consensus and Long – term Stability Framework for Future Sino – U. S. Relations

Da Wei

Abstract: Over the past 35 years, "integration – engagement" has been the axis of Chinese – and U. S. strategies towards each other. China needs to integrate itself into the international system and realize modernization, and the two sides have reached strategic consensus on this point. This consensus, has been gradually diluted over the past 10 years. The recent hot discussions on U. S. China policy in America has clearly reflected this trend. China and the U. S. need to reach a new strategic consensus on "common development within a system", and set up a long – term and stable framework, in which the two countries can coexist and carry out effective cooperation with limited competition. China's initiative of building a new model of major power relations shows that it may undertake this mission.
Keywords: China – U. S. relations, strategic consensus, strategic stability, new model of major power relations

The Adjustments of U. S. Cyber Security Strategy and the Building of a New Model of Major Power Relations between China and the United States

Wang Xiaofeng

Abstract: Snowden's leaks has triggered wide domestic and international criticism of U. S. cyber security strategy. The Obama administration has adjusted the range and the acquisition mode of the cyber intelligence and actively sought the understanding and support of the domestic and the international communities. These adjustments include emphasizing the protection of cyber security of the private sectors, promoting cyber security information sharing between the government and enterprises, broadening the applications of juridical and economic measures, establishing code for international conducts in cyberspace, and promoting cooperation in cyber security among allies and partners. These adjustments indicate its intention to regulate and contain China. China should seek to handle the cyber issues within the framework of China – U. S. New Model of Major Power Relations and create an atmosphere of cooperation, so as to set up effective agenda and effectively guide the China – U. S. cyber – security relations.
Keywords: U. S. cyber security strategy, new model of major power relations, China – U. S. relationship

A Strengthened Japan – US Alliance and Its Impact on China's Peripheral Security

Huang Dahui & Zhao Luoxi

Abstract: The new Guideline for Japan – US Defense Cooperation revised in April 2015 has further clarified the co–