《美国研究》2016 年第 5 期

中美经济网络间谍争端的冲突根源与调适路径①

汪晓风

〔内容提要〕中美经济网络间谍争端的根源在于网络空间发展与经济社会运行深度融合、中美网络战略的结构矛盾，以及两国安全和发展利益的竞争特性。挑起中美经济网络间谍争端是美国寻求绝对安全的国家安全观和网络安全观的体现，也包含平衡中国实力增长的意图。随着对网络安全认知不断加深，相互政策不断碰撞磨合，中美两国管控分歧意愿逐步增强，及至达成各自承诺不从事、不支持经济网络间谍活动的共识。中美关系竞争面的上升，促使网络空间控制权和网络治理话语权的争夺成为常态，因而围绕经济竞争与安全博弈的网络争端仍将不断出现。未来中美能否有效管控分歧，避免引发新的冲突，还在于两个互联网大国网络战略理念的相互塑造和网络空间利益的相互调适，并在网络安全领域展开务实合作。

关键词：美国外交 网络安全 中美关系 经济网络间谍 网络战略

随着社会信息化程度不断加深，网络环境蕴藏的风险和网络活动带来的威胁日益显现。美国私营企业和科研机构频频遭受网络攻击，大量商业机密和技术专利被窃，这本是很多国家都面临的新问题，然而美国政府却将矛头指向中国，指责中国政府参与和支持对美经济网络间谍活动，令美国企业遭受重大损失，进而削弱美国经济

① 感谢《美国研究》匿名评审专家提出的问题和修改意见，文责自负。本文系国家社科基金一般项目“美国棱镜计划的系统分析和综合应对研究”（项目号：15BGJ049）的阶段性成果，本文写作得到清华大学国家战略研究院支持。

的国际竞争力。美国以此对中国进行外交施压、提起司法诉讼,还威胁进行经济制裁、网络打击和军事报复。

经济网络间谍争端对中国外交和中美关系产生诸多不利影响。国际上,中国政府支持经济网络间谍论调盛行,对中国国际声誉造成了伤害,给中国海外投资和经贸活动带来了政治和安全壁垒,为中国参与网络空间国际治理和国际贸易规则制定设置了障碍。中美关系中,经济网络间谍争端已经成为长期干扰和重要阻力。那么,如何认识中美经济网络间谍争端的实质,能否有效化解两国间的认知分歧和利益矛盾,怎样避免中美在网络安全问题上形成新的冲突?本文拟从中美经济网络间谍争端的发展演变、两国的不同认知、美国挑起争端的动因,以及调适路径等方面对上述问题进行分析。

一 争端演变:酝酿、冲突及管控

中美经济网络间谍争端由来已久,在美国政府主导和媒体推动下,美国社会逐渐形成一个根深蒂固的印象:中国政府支持和参与长期、系统、大规模地从美国企业和科研机构窃取商业机密、技术专利和敏感信息。美国政府进而以保护企业利益和维护国家安全为由,不断对中国发起口诛笔伐和外交施压。中国政府则一再声明反对经济网络间谍行为的原则立场,也没有支持和参与经济网络间谍活动的政策和计划,并对美国的指责和施压进行反制。迄今为止,中美经济网络间谍争端的演变大致经历了三个阶段:

(一)酝酿阶段(2007 年至 2013 年 2 月)

这一阶段,美国和西方媒体关于中国窃取美国商业机密和技术专利的报道逐渐增多。政府层面相对谨慎和克制,主要是以各种方式表达怀疑、担忧和不满,但并未上升为针对中国的具体政策行动,也没有引发两国间的直接冲突。

2007 年 8 月,德国《镜报》刊登长篇专题,称中国军方黑客通过网络大量获取德国企业的尖端技术机密,令德国企业遭受巨大经济损失。[①] 随后西方媒体开始追踪报道中国政府支持或参与经济网络间谍活动。2010 年 1 月,英国《泰晤士报》报道,"中国黑客侵入'谷歌中国'系统,窃取知识产权和个人邮件账号信息","至少 20 个公司成为攻击目标,包括防务承包商、金融公司和技术企业等。攻击复杂程度远超一

① Jurgen Dahlkamp, Marcel Rosenbach, Jorg Schmitt, Holger Stark, Wieland Wagner, "Die Gelben Spione: Wie China Deutsches Know-how Ausspaht," *Der Spiegel*, Ausgabe 35, 2007, pp.19~34.

般个人黑客和犯罪组织的水平，是典型的国家行为”。[①] 2011 年 12 月，《华尔街日报》称美国情报机构准确定位了窃取美国公司机密的 20 个中国网络间谍组织，其中 12 个与军方有关，报道还称国家安全局已确认一些网络间谍组织成员的身份，美国政府可以此与中国政府直接对质。[②]

美国政府也开始将“应对中国网络间谍”议题推上日程。2007 年 11 月，美中经济与安全审查委员会向国会提交年度报告，称“工业间谍活动为中国企业提供了获取新技术的新途径”，“中国的工业间谍活动已经对美国技术形成最大威胁”。[③] 2009 年 5 月，奥巴马发表关于保护国家网络基础设施的讲话，称网络犯罪从私营企业窃取大量知识产权。[④] 2011 年 10 月，美国国家情报总监办公室反情报执行办公室向国会提交一份报告，称中国情报机构利用网络间谍手段盗取美国的贸易和技术机密，吞噬大量美国高科技企业的研发数据，这一行为“对美国经济安全造成日益严峻和持久的威胁”，报告将中国描述成“顽固的搜集者”（persistent collector）。[⑤] 同月，时任国会众议院情报委员会主席迈克尔·罗杰斯（Mike Rogers）在一次名为“网络威胁和保护国家的措施”的听证会上指出，“中国的经济网络间谍已经达到无法忍受的水平。”[⑥] 2012 年 6 月，美国前网络司令部司令和国家安全局局长基斯·亚历山大（Keith B. Alexander）称经济网络间谍给美国工业信息和知识产权造成的损失构成了“历史上最大规模的财富转移”。[⑦]

对于美国及西方媒体和政府或明或暗的指责，中国政府一直坚持从未参与或支

---

① Mike Harvey, “China Accused of Cyber Attack on Google and ‘Global Industrial Targets,’” *The Times*, January 16, 2010, available at: http://www.thetimes.co.uk/tto/technology/article1859862.ece.

② Siobhan Gorman, “U.S. Homes In on China Spying: Probe Pinpoints Groups of Hackers and Ties Most to Military, Officials Prepare to Confront Beijing,” *Wall Street Journal Online*, December 13, 2011, available at: http://www.wsj.com/articles/SB10001424052970204336104577094690893528130.

③ U.S.-China Economic and Security Review Commission, “2007 Report to Congress,” November 15, 2007, available at: http://origin.www.uscc.gov/sites/default/files/annual_reports/2007-Report-to-Congress.pdf.

④ U.S. White House, “Remarks by the President on Securing Our Nation's Cyber Infrastructure,” May 29, 2009, available at: https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

⑤ U.S. Office of the National Counterintelligence Executive, “Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009~2011,” October 2011, available at: http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

⑥ Mike Rogers, “Statement to the U.S. House, Permanent Select Committee on Intelligence, Open Hearing: Cyber Threats and Ongoing Efforts to Protect the Nation,” October 4, 2011, available at: http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingRogers.pdf.

⑦ Josh Rogin, “NSA Chief: Cybercrime Constitutes the Greatest Transfer of Wealth in History,” *Foreign Policy*, July 9, 2012, available at: http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history.

持经济网络间谍活动，西方的报道和指责是捏造事实、诬陷和施压中国。如 2009 年 3 月加拿大多伦多大学芒克全球事务研究中心(Munk School of Global Affairs) 发布报告，称中国政府黑客入侵 100 多个国家网络系统，中国外交部发言人回应称该机构无中生有，捏造所谓中国网络间谍的谣言。① 2009 年 10 月美中经济与安全评估委员会发布报告称，中国政府加紧针对美国的网络间谍行动，中国外交部发言人指出，该委员会一向渲染“中国威胁论”，有关报告“捏造事实，充满冷战思维”。② 在这一阶段，中美在经济网络间谍问题上形成了“指责、施压——否认、反驳”的基本互动模式。

(二) 直接冲突阶段(2013 年 2 月至 2015 年 9 月)

这一阶段的突出特点是美国政府、网络安全公司、媒体、研究机构全面渲染中国经济网络间谍威胁，两国分歧不断加深，矛盾不断升级，直至发生正面冲突。

2013 年 2 月 19 日，美国网络安全公司曼迪昂特(Mandiant) 发布一份题为《高级持续性威胁: 揭秘一个中国网络间谍单位》的报告，称上海浦东一家驻军单位的数名军人长期侵入美国企业和研究机构的计算机系统，获取敏感信息和技术文档，报告还详细叙述其中三名军人的个人信息和 2006 年以来的数次网络入侵活动。③ 该报告通过一些片断证据，将 IP 地址来自中国的黑客攻击归因为政府行为，并得出中国军队有一批高水平、专业化的黑客精英的结论。在美国政府和公众看来，曼迪昂特报告证据链完整，有很高的可信度，因而普遍认为中国政府确有经济网络间谍行为。值得注意的是，曼迪昂特报告并没有证明中国政府系统地参与和支持经济网络间谍活动，如从美国企业获取的商业机密如何交给中国企业，有哪些中国企业从中受益，美国企业因而遭受哪些损失。

《曼迪昂特报告》是促使中美网络矛盾向冲突演变的开端，美国政府以该报告为据对中国施压，国会参众两院情报、外交、军事、国土安全相关委员会密集召开听证会探讨中国网络窃密活动，情报机构发布报告渲染中国网络攻击威胁。美国政府从总统、副总统、国务卿、商务部长、国防部长、参联会主席都通过不同方式向中国对应部门和官员施压，网络安全问题迅速上升成为中美关系最显著的冲突爆发点。中国政府迅速回应报告指称，2 月 20 日，外交部发言人称“该报告出于各种目的，进行无端猜测和指责，既不专业，也不负责，无助于解决问题”。国防部发言人也称“曼迪昂特

① 《外交部发言人秦刚就所谓中国网络间谍系统入侵多国电脑事答记者问》，2009 年 3 月 31 日，参见网页: http: //www.fmprc.gov.cn/zflt/chn/fyrth/t555021.htm。

② 《外交部发言人马朝旭就美国会发表报告渲染所谓中国“网络间谍”威胁答记者问》，2009 年 10 月 23 日，参见网页: http: //www.fmprc.gov.cn/ce/cgtur/chn/wjbfyrth/t622154.htm。

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

网络公司所谓中国军方从事网络间谍活动的说法是没有事实根据的”。① 2 月 27 日，《人民日报》发表社评，称报告不专业、不严谨、有偏见，同时指美国是真正的“黑客帝国”。②

2013 年 4 月，美国国务卿约翰·克里(John Kerry)访华，两国外长同意在“战略与经济对话”框架下成立一个网络工作组，作为处理两国网络争端的对话机制。2013 年 6 月，中美两国元首在美国加州会晤，在联合记者招待会上，习近平表示注意到媒体的报道，“这可能给人一种感觉：网络安全威胁主要来自中国，或者中美关系中最大的问题是网络安全问题。”“我们需要密切关注这个问题，研究有效解决方法。这个问题实际上可以是中美以务实方式相互合作的领域。”奥巴马则表示，“黑客攻击和盗版并非美中关系独有的问题，这些是国际关切的问题，一些非国家行为者也进行这类活动，我们在和其他国家就建立共同遵守的行为规则进行磋商。”③

中美元首加州会晤后，如双方遵循经过协商和外交渠道妥善解决各方关切，经济网络间谍问题可望得到缓解。但树欲静而风不止，美国政府决意将网络问题上的矛盾和分歧公开化、扩大化。2014 年 5 月 1 日，美国司法部签署起诉书，在美国宾夕法尼亚州西区地方法院起诉五名中国军人，称他们隶属中国军方在上海的一个情报部门，他们侵入一些美国企业的网络系统，窃取商业机密和敏感信息。5 月 19 日，美国司法部公布起诉书，联邦调查局同时还签发了对五名中国军人的通缉令。

中国政府迅速做出反应，外交部、国防部、国家互联网信息办公室先后发表声明，表达强烈不满和抗议。外交部发言人称“中国政府和军队及其相关人员从不从事或参与通过网络窃取商业秘密活动。美方的指责纯属无中生有，别有用心。”“鉴于美方对通过对话合作解决网络安全问题缺乏诚意，中方决定中止中美网络工作组活动。”④国防部发言人称“中方是网络安全的坚定维护者，美方所谓‘网络商业窃密’等说法无中生有，混淆视听，是别有用心的。”⑤国防部外事办公室官员 5 月 20 日召见美国驻华使馆代理武官，提出严正交涉和抗议。中方表示，美方对中方人员的指责毫无根据，有关霸道行径严重违反国际关系基本准则，严重诋毁中国军队形象。中方

① 《外交部国防部回应“中国黑客威胁论”》，2013 年 2 月 20 日，参见网页：http://www.fmprc.gov.cn/ce/cgfrankfurt/chn/zgyw/t1016047.htm。

② 钟声《美国炒作中国黑客威胁论，把网络当战场损人害己》，载《人民日报》，2013 年 2 月 27 日，第 5 版。

③ The White House Office of the Press Secretary, “Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting,” June 8, 2013, available at: https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china.

④ 《外交部发言人就美国司法部宣布起诉 5 名中国军官一事发表谈话》，2014 年 5 月 19 日，参见网页：http://www.fmprc.gov.cn/mfa_chn/fyrbt_602243/t1157478.shtml。

⑤ 《国防部新闻发言人耿雁生就美司法部起诉中国军人发表谈话》，2014 年 5 月 20 日，参见网页：http://www.mod.gov.cn/auth/2014-05/20/content_4510364.htm。

要求美方立即撤销错误决定，切实维护两军关系发展大局。① 中国国家互联网信息办公室即日公布美国攻击中国网络的最新数据，其发言人称美国才是世界上最大的网络窃密者，也是中国网络的头号攻击国。“美国以所谓网络窃密为由宣布起诉五名中国军官，纯属倒打一耙，贼喊捉贼。”②

中美网络工作组活动的中止，切断了中美在网络事务上进行沟通的渠道。美国通过多种途径尝试恢复中美网络工作组，由于中国方面对恢复工作组开出的条件是“撤销指控”、“停止指责”、“纠正错误”，而按照美国司法相对独立于行政部门的政治体制及相关法律规定，撤销具体刑事诉讼仅限于两种情况：一是司法部作为诉讼提起方主动撤回；二是法院作为案件受理方提出因“嫌疑人无法到场”，为避免滥用司法资源而中断审查。由于该案指控通过大陪审团提出，故不论是宾夕法尼亚州西区地方法院或是司法部，都不可能做出主动撤诉之举。既然美国政府做不到主动撤诉，而中国也不愿意在诉讼和通缉仍然存在的情况下恢复工作组。双方都不能回撤立场而承担国内政治压力，恢复网络工作组之事就此搁置。

按照日程，2015 年 9 月中国国家主席习近平将访问美国，能否妥善处理网络窃密问题就成为访问顺利进行的关键，一些国会议员甚至以中方没有停止经济网络间谍活动为由要求白宫取消习近平主席的访问。7 月，中央政法委书记孟建柱率公安、国家安全、司法、网信等部门负责人访问美国，同美国国务卿、国土安全部部长、总统国家安全事务助理等举行会谈，就共同打击网络犯罪等执法领域进行沟通。孟建柱表示，“中方反对网络攻击和网络商业窃密的立场是坚定的，中美两国开展对话合作、共同打击网络犯罪，符合双方和国际社会的共同利益。”③此次访问缓和了经济网络间谍问题上的紧张气氛，也为解决双边关切探索出新的路径，即将该问题放在打击网络犯罪合作的框架下，这是一个符合双方预期的安排，为两国元首达成共识创造了条件。

2015 年 9 月 10 日，美国国家情报总监詹姆斯·克拉珀（James R. Clapper）在众议院情报委员会作证时表示，美国应该强化针对中国黑客攻击的网络安全措施。克拉珀在习近平访美前说这番话，无疑是向中国施加压力，一些媒体则称奥巴马已签署有关制裁的行政命令，近期对一些中国公司和个人实施制裁的可能性越来越大。种种有违中美元首即将会晤更应塑造合作友好氛围的非常规做法，表明美国政府以经

① 《国防部就美国司法部起诉中国军官向美方提出严正交涉和抗议》，2014 年 5 月 20 日，参见网页：http://www.mod.gov.cn/auth/2014-05/20/content_4510453.htm。

② 《美国攻击中国网络最新数据公布》，载《人民日报海外版》，2014 年 5 月 20 日，第 4 版。

③ 《外交部发言人就中央政法委书记孟建柱访美答记者问》，2015 年 9 月 14 日，参见网页：http://www.fmprc.gov.cn/web/wjdt_674879/fyrbt_674889/t1296439.shtml。

济网络间谍争端捆绑中美关系的意图。9 月 11 日，中国外交部发言人表示，在网络安全问题上，美国应该停止无端指责，在互信基础上启动对话，共建和平与安全的网络空间。[①]通过双方交流，维护中美关系稳定发展的大局成为共识，美国政府软硬兼施的同时，也对如何化解困局提出了一些建设性的方案。

（三）管控调适阶段（2015 年 9 月以后）

这一阶段的特点是冲突管控和政策调适，美国指责中国政府进行经济网络间谍的频度和力度都有所降低，中美管控网络争端及网络安全合作的对话也得以恢复。

2015 年 9 月，习近平主席访问美国，中美元首会晤后举行联合记者招待会，承诺双方政府均不在知情情况下支持和参与以商业为目的的网络窃密，并同意就打击网络犯罪开展合作。奥巴马在中美元首联合记者招待会上表示，“我保证我们政府不支持这些活动（经济网络间谍），一旦我们注意到非政府实体或个人从事这类行为，我们会严肃对待。”[②]习近平主席指出，“中美在网络安全问题领域具有广泛的共同利益，我们应该加强合作，避免引起冲突。中美双方就共同打击网络犯罪达成了许多重要共识，接下来要把这些认识和进展，进一步达成一致并且落实下去。”“双方应该合作，合则两利，斗则双输，我们完全可以开展部门之间、企业之间、专家之间的对话交流，从技术产业标准、打击犯罪多方面加强合作，将网络安全问题打造成中美合作的增长点。”[③]

此后，中美经济网络间谍争端逐渐降温。2015 年 12 月 1 日，中美打击网络犯罪高级别对话在华盛顿举行，中国国务委员郭声琨与美国司法部部长林奇、国土安全部部长约翰逊共同主持会议，双方达成《打击网络犯罪及相关事项指导原则》，并同意建立热线，以处理在响应这些请求过程中可能出现的问题。2016 年 3 月 31 日，两国元首在华盛顿第四届核安全峰会期间会晤，奥巴马表示非常重视保护美国公司的知识产权，但很高兴中美就网络安全问题进行坦诚交流，而习近平主席则表示将积极探索进一步合作的可能。[④] 两国元首在网络安全议题上的气氛已大大和缓，在维护网络安全和保护知识产权问题上的表态也更具建设性。中美打击网络犯罪合作机制也

---

① 《外交部发言人就美国国家情报局总监克拉珀有关中国黑客言论答记者问》，2015 年 9 月 11 日，参见网页：http://www.fmprc.gov.cn/web/wjdt_674879/fyrbt_674889/t1295942.shtml。

② The White House Office of the Press Secretary, “Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference,” September 25, 2015, available at: https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

③ The White House Office of the Press Secretary, “Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference.”

④ The White House Office of the Press Secretary, “Remarks by President Obama and President Xi of the People's Republic of China Before Bilateral Meeting,” March 31, 2016, available at: https://www.whitehouse.gov/the-press-office/2016/03/31/remarks-president-obama-and-president-xi-peoples-republic-china.

部分取代了网络工作组的功能，成为中美间网络事务沟通的新渠道。2016 年 5 月 11 日，中美网络空间国际规则高级别专家组首次会议在华盛顿举行，由中国外交部和美国国务院共同主持，这一新的部际对话机制的建立，意味着美国司法部诉中国军人案后中断的网络安全外交对话得以重新启动。

与中美恢复网络对话相对应的是，美国情报部门和网络安全企业均称来自中国的网络攻击和网络窃密大幅下降。2016 年 3 月，美国国家情报总监詹姆斯·克拉珀（James Clapper）表示，情报部门探测到中方间谍活动有所减少。4 月初，美国国家安全局局长迈克尔·罗杰斯（Michael Rogers）在国会参议院军事委员会作证时表示，当前中国的黑客活动处于较低水平。网络安全公司方面也给出了类似信息，菲德利斯公司（Fidelis）表示“网络间谍活动出现实质性减少。”“明显带有商业动机的网络间谍活动似乎有所收敛。”火眼公司（FireEye）首席执行官戴维·德瓦尔特（David DeWalt）称该公司识别的 22 个中国政府支持的黑客单位中，没有一个仍在对美国企业发起网络攻击，其 4000 余家客户接到的应急事件呼叫显著减少，自去年 9 月以来没有再发现中方利用“零日漏洞”[①]进行攻击。

即便如此，美国仍不乏质疑中美控制经济网络间谍的共识能否得到落实的声音。2015 年 10 月，众击公司（Crowdstrike）称中国并未收敛网络间谍活动。2016 年 4 月 5 日，迈克尔·罗杰斯（Michael Rogers）在国会参议院军事委员会作证时称，尽管去年美中就网络安全议题达成共识，但这项共识没有起到作用，充其量只是活动强度比之前有所降低。[②] 4 月 27 日，美国国防部长阿什顿·卡特（Ashton Carter）在美国海军学院发表演讲时称，“中国黑客违反互联网创建的精神，大规模地窃取美国企业知识产权”。[③] 还有一种观点认为，尽管中国政府可以管控政府支持的网络窃密活动，但阻止大批民间高手自行从事黑客活动的难度较大，这也促使许多人对中美限制经济网络间谍活动的协议能否发挥实质作用表示怀疑。

美国总统大选期间，经济网络间谍无意外地成为参选人谈论中美关系的主要话题。2015 年 10 月 14 日，共和党总统参选人泰德·克鲁兹（Ted Cruz）以经济网络间谍问题攻击中国，“中国在幕后操纵大规模网络战，攻击我们的政府系统和私营系

① 零日漏洞是指被发现后立即被恶意利用的安全漏洞。

② Michael S. Rogers, “Statement before the Senate Armed Services Committee,” April 5, 2016, available at: http://www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf.

③ Ashton Carter, “Remarks at U.S. Naval Academy Commencement,” May 27, 2016, available at: http://www.defense.gov/News/Speeches/Speech-View/Article/783891/remarks-at-us-naval-academy-commencement.

统。”[①]2016 年 2 月 23 日,民主党总统参选人希拉里·克林顿在《波特兰新闻先驱报》发表专栏评论,指责中国“系统地窃取商业秘密,背后得到政府支持,并公然拒绝按规则行事”。[②] 2016 年 4 月 27 日,共和党总统参选人唐纳德·特朗普发表外交政策演说,称“中国通过网络攻击和工业间谍,盗窃美国政府机密和公司信息,奥巴马容忍这一切,让对手和挑战者认为他们可以得到任何东西。”[③]尽管美国总统选举中的议题未必会转换为下一届政府的政策,但不可否认的是,大选议题的高关注度将进一步加深美国公众对于中国政府支持经济网络间谍的印象。

二 争端焦点:认知、技术及合法性

经济网络间谍问题伴随网络空间与经济社会运行日益融合而产生,各国政府都表示反对通过网络窃取商业机密或技术情报,这一点中美的原则立场并无二致,然而概念认知的差异和适用法律的缺失,加上网络攻击活动跨国和隐秘的技术特性,造成中美围绕经济网络间谍的争端不断,美国政府在网络攻击问题上的双重标准,更是成为促使矛盾升级的主要原因。

(一)经济网络间谍的概念及其法律适用

在国际关系中,间谍活动位于灰色地带,绝大多数国家都会从事搜集军事、安全、经济情报信息的秘密间谍活动。经济网络间谍则是传统灰色行为与现代网络技术相结合产生的新问题。从字面上看,经济网络间谍或网络商业窃密[④]是通过网络获取情报、数据、信息,谋求经济收益的活动,包含三个要件:入侵网络、窃取数据、商业受益,经济收益是目的,网络入侵是途径和手段,数据窃取是行为表现。一般而言,窃密在任何国家都是违法行为,属国内法律管辖范畴,当然窃密活动也可能是跨国行为。间谍本身就具有国际或跨国含义,属于国际关系范畴。而经济网络间谍活动发生在网络空间,没有国家边界区分,这就对经济网络间谍行为的法律认定和管辖权形成了挑战。

---

① Matthew Patane, “Cruz Calls for ‘Reciprocal Response’ to China-tied Cyberattacks,” *The Des Moiners Register*, October 14, 2015, available at: http://www.desmoinesregister.com/story/news/elections/presidential/caucus/2015/10/14/cruz-calls-reciprocal-response-china-cyberattacks/73943634/.

② Hillary Clinton, “Level the Playing Field on Global Trade,” *Portland Press Herald*, February 23, 2016, available at: http://www.pressherald.com/2016/02/23/commentary-if-elected-president-ill-level-the-playing-field-on-global-trade-clinton-says/.

③ “Trump Details Foreign Policy of Paradoxes,” *New York Times*, April 28, 2016, available at: http://www.nytimes.com/2016/04/28/us/politics/donald-trump-foreign-policy-speech.html.

④ 美国政府通常会用“网络间谍”(cyber enabled espionage)、“经济网络间谍”(economic cyber espionage)等概念,而中国政府通常使用“网络商业窃密”一词。

从经济网络间谍的认定来看，商业获益是预先的设想和后继的行为，与窃密本身是分离的，因此判别一项具体的网络窃密行为是否构成经济网络间谍，不仅需要确定网络入侵和网络攻击行为已经发生，还要确定窃密者利用所窃商业机密和技术专利获取了经济收益。而网络窃密者所在国未必掌握窃密者的身份、窃密时间和网络路径，而如果网络窃密活动受到政府支持，则该国政府往往不会向受害国提供窃密者互联网接入和服务器访问记录，因而尽管网络间谍非常普遍，但得到调查和确认的经济网络间谍寥寥无几。

管控经济网络间谍活动不仅取决于相关政府的政治意愿和行动能力，法律适用性也是关键条件。目前中美两国都没有直接针对经济网络间谍活动的专门法律法规，在适用法律的选择上均体现了将经济犯罪和计算机犯罪相结合的思路。

按照中国政府的相关表述，“在中国境内实施网络攻击和网络商业窃密都是违反国家法律的，都应受到法律的追究”，显然，未经授权进入企业或科研机构的网络系统获取数据信息是违法行为，但中国现有法律对入侵计算机网络及窃取数据的规定比较宽泛，并无明确规定经济网络间谍具体受哪些法律管辖，以何种形式予以追究。现行刑法以妨害社会管理秩序罪对涉及计算机和网络的犯罪进行认定和处罚，而在侵犯财产罪的相关条款中则未有体现。1997 年《刑法》修订案明确入侵国家和政府部门计算机信息系统系违法行为，“入侵国家事务、国防建设和尖端科学技术领域计算机信息系统的，处三年以下徒刑”。① 2009 年《刑法修正案(七)》增加了侵入其他领域计算机网络系统的条款，并以“非法侵入计算机信息系统罪”、“非法获取计算机信息系统数据、非法控制计算机信息系统罪”定罪。② 此外，拟议中的《网络安全法(草案)》规定“任何个人和组织不得从事入侵他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动”。③ 这些法律明确了中国政府反对包括经济网络间谍在内的一切形式网络窃密行为的立场。

而美国政府的基本立场是“反对将通过情报手段获取的知识产权和商业机密提供给本国企业，从而为本国企业谋取不合理的市场竞争优势”，这显然是基于其科技发展水平高、贸易及商业机密价值大、技术专利数量多的现实。当前美国处理经济网络间谍的法律依据主要是两类立法，第一类是关于经济间谍的，主要是旨在保护私营

① 《中华人民共和国刑法》(1997 年 3 月修订)，法律出版社，2015 年 9 月第 1 版，第 92 页。

② 《中华人民共和国刑法修正案(七)》(2009 年 2 月通过)，载《中华人民共和国刑法》，法律出版社，2015 年 9 月第 1 版，第 166~167 页。

③ 《中华人民共和国网络安全法(草案二次审议稿)》，2016 年 7 月 5 日上网公布，参见网页：http://www.npc.gov.cn/npc/lfzt/rlyw/2016-07/05/content_1993588.htm。

部门经济信息的《1996 年经济间谍法》[①]及加重处罚经济间谍行为的《2012 年外国与经济间谍惩治增强法》。[②] 第二类是关于打击虚假网络身份和网络行为身份识别的，这方面的法律依据主要是《2000 年互联网虚假身份证明防范法》。[③] 在美国，窃取商业机密是一项联邦罪(federal crime)，当机密信息涉及在州际或对外贸易的产品(美国法典第 18 卷第 1832 节)或者当潜在受益人是外国主体时(美国法典第 18 卷第 1831 节)，就涉及经济间谍罪。第 1832 节要求窃密者明知滥用信息将损害机密信息所有者利益，而令其他人受益，第 1831 节仅要求窃密者意图令一个外国政府或其代理者受益。[④]

《经济间谍法》为美国政府阻止和打击窃取美国科技和经济机密信息的间谍活动提供了法律依据。但经济间谍的特殊性在于受害者往往不愿意声张，事实上即便司法部门愿意帮助企业保护商业机密和知识产权，但受害者却有很多顾虑，一些机密被窃的公司宁愿独自承担损失或寻求网络安全公司帮助，也不愿通过起诉在法庭上曝光，因为商业机密被窃的消息传出会损害企业形象，动摇市场信心。《经济间谍法》即是在这种两难处境下运作，《经济间谍法》1996 年通过，直到 2001 年 5 月才出现第一例以经济间谍罪提起的诉讼，第二起诉讼发生在 2002 年 12 月。尽管数量少，但总体上还是呈现逐年上升趋势，如 2010 年相关诉讼就达到七起。

在美国司法部诉中国军人案中，联邦大陪审团提出涉嫌违反美国联邦法律的 31 项指控，包括计算机欺诈、故意访问受保护的计算机并获取信息、故意损坏受保护的计算机、盗窃身份信息、经济间谍、窃取商业机密等六类罪名。[⑤] 起诉的法律依据集中在美国法典第 18 卷，包括第 1028 节“与身份证明文件、身份验证功能及信息有关的欺诈和相关活动”、1030 节“与电脑有关的欺诈和相关活动”、1031 节“针对美国的重大欺诈行为”、1032 节“利用存储设备、接收设备或清算代理隐瞒资产”等等。其中，四类指控涉及侵入计算机并获取信息，两类指控涉及经济间谍和窃取贸易机密。如第 31 项指控的具体依据是 1832 节“意图将与一个用于或可能用于各州之间或对外商业活动的产品或服务有关的商业机密转换为其所有者之外任何人的经济利益，

① U.S. Public Law 104-294, "Economic Espionage Act of 1996," October 11, 1996, available at: http://www.gpo.gov/fdsys/pkg/PLAW-104publ294/pdf/PLAW-104publ294.pdf.

② U.S. Public Law 112-269, "Foreign and Economic Espionage Penalty Enhancement Act of 2012," January 14, 2013.

③ U.S. Public Law 106-578, "Internet False Identification Prevention Act of 2000," December 28, 2000.

④ Charles Doyle, "Stealing Trade Secrets and Economic Espionage: An Overview of 18 U.S.C. 1831 and 1831," available at: *U.S. Congressional Research Service*, July 25, 2014, https://fas.org/sgp/crs/secrecy/R42681.pdf.

⑤ U.S. District Court for the Western District of Pennsylvania, "Indictment: Criminal No.14-118," May 1, 2014, http://s3.documentcloud.org/documents/1164069/indictment.pdf.

并有意或明知将损害商业机密的任何所有者的情况下”。①

表： 美国司法部诉中国军人案的指控及法律依据

指控项目	指控罪行	法典卷/节
1	2010~2014.04，阴谋实施计算机欺诈	法典 18 卷 1030 节 b 条
2~9	2010~2012.04.13，故意访问受保护计算机并从中获取信息	法典 18 卷 1030 节 a 条 2 款 C 项、c 条 2 款 B 项 i-iii 目
10~23	2010.02.08~2012.04.13，故意破坏受保护计算机	法典 18 卷 1030 节 a 条 5 款 A 项、c 条 4 款 B 项
24~29	2010.12.30~2012.04.13，恶意窃取身份信息	法典 18 卷 1028A 节 a 条 1 款、b 条、c 条 4 款
30	2010.05.06，经济间谍	法典 18 卷 1831 节 a 条 2、4 款
31	2010.05.06，窃取贸易信息	法典 18 卷 1832 节 a 条 2、4 款

资料来源：U.S. District Court for the Western District of Pennsylvania, “Indictment: Criminal No.14~118,” May 1, 2014。

从美国司法部援引的法律条款来看，经济网络间谍所涉计算机犯罪和经济犯罪的司法依据并不复杂，故针对经济网络间谍进行司法处置，难点并不在于窃密事实的认定，而在于如何找到网络窃密者，以及如何处理境外嫌疑人。依据中美两国法律，入侵计算机信息系统、窃取数据信息都是违法或犯罪行为，而一旦涉及政府行为或跨国行为，两国法律都存在着相应盲区。如中国《国家安全法》规定，“国家安全机关、公安机关、有关军事机关根据职责分工，依法搜集涉及国家安全的情报信息。”②《反恐怖主义法》规定，“公安机关、国家安全机关、军事机关在其职责范围内，因反恐怖主义情报信息工作的需要，根据国家有关规定，经过严格的批准手续，可以采取技术侦察措施。”③这些规定赋予相关政府部门进入网络系统和获取数据信息的权限，同时并未排除包含技术专利和商业秘密的系统和数据。《美国爱国者法案》也赋予美国国家安全局、联邦调查局等情报和安全机构获取网络数据和信息的权限。一般而言，政府行为经国内法律授权，同时基于维护国家安全的需要，其合法性并不存在疑义，而如果涉及其他国家或跨境行为，则应该遵守国际法、双边或多边的条约义务。但现实是，迄今并没有国际法和国际条约对利用网络获取反恐或国家安全情报的国家行为进行约束和规范，一旦面临其他国家的网络窃密活动，现有国际法规范、国际争端解决机制或多边协调机构都没有提供适当的法律依据和政策工具。

（二）技术问题：辨识经济网络间谍活动的难点

① U.S. Code § 1832, “Theft of trade secrets,” https://www.law.cornell.edu/uscode/text/18/1832.

② 《中华人民共和国国家安全法》（2015 年 7 月 1 日通过），法律出版社，2015 年 7 月第 1 版，第 13 页。

③ 《中华人民共和国反恐怖主义法》（2015 年 12 月 27 日通过），法律出版社，2016 年 1 月第 1 版，第 18~19 页。

促使中美经济网络间谍争端复杂化的一个重要原因是经济网络间谍活动在网络空间展开，其虚拟性、普遍性和全球性等特性都使得对中美关系中的经济网络间谍问题性质的判断更加困难，必须以相应的技术能力和恰当的评估方法为依据，而很长一段时间争端双方都把焦点放在意图和事实的辩驳上。

首先，经济网络间谍行为的虚拟性和隐秘性使得网络窃密活动很难防范。经济网络间谍攻守双方在技术、方法和能力等方面都是非对称的，即目标企业往往没有建立网络安全管理制度，窃密者则掌握各种突破系统防御屏障的技术和工具，并通过社会工程途径搜集目标企业和管理人员的信息，在暗处不断寻找目标系统的技术漏洞和管理缺口，即便企业加大网络安全投入，仍然有可能百密一疏，或者落入精心设置的鱼叉式攻击陷阱。① 如美国国家反情报行政办公室的一份报告指出了网络间谍活动盛行的原因，“外国在网络空间搜集敏感经济信息，而被窃密目标的私营部门检测到的风险很低。”②

经济网络间谍的受害者主要是私营企业和科研机构，它们防范网络窃密的能力参差不齐，一些企业甚至没有配备专业系统管理职位，不仅面临专业网络攻击时无能为力，甚至系统被入侵且长时间控制也毫无察觉。此外，网络窃密者针对入侵目标企业网络系统进行充分准备，分析系统缺陷、利用管理漏洞乃至收买内部管理人员，这种来自暗处的攻击更是将企业置于被动和脆弱的位置。由于经济网络间谍活动的广泛性，受害者也存在着不确定性和随机性，因为入侵网络系统技术复杂程度差异很大，入侵者往往同时扫描数以千计的主机和数据库，寻找漏洞，一些防护严密的系统也许永远无法得手，一些遭到入侵的系统却未必存有重要数据信息。

其次，经济网络间谍行为的跨国特性导致追踪和取证的合作障碍。在中美元首会晤达成合作打击网络犯罪的共识后不久，美国官员就开始表示担忧，认为中国政府可能会以各种理由阻挠协议实施，且无法有效阻止经济网络间谍活动。即便其他国家政府愿意与受害方政府合作，网络活动的跟踪调查需要投入的资金和人力也是一个障碍，2015 年 9 月中美元首会晤时，习近平主席告诉奥巴马说中国有 6 亿网民，意即很多网络攻击行为并非政府所为，要限制和阻止所有对外网络攻击行为非常困难，但中国愿意与美方合作，共同打击商业网络窃密行为。

---

① 鱼叉式攻击（phishing）是一种针对特定目标的网络攻击方法，最常见的做法是将木马程序作为邮件附件或网页链接，发送给目标用户，诱使用户打开附件，从而感染目标电脑，获取账号密码等信息。据统计，90%以上的高级持续性威胁（Advanced Persistent Threat，APT）采用鱼叉式攻击方法。

② U.S. Office of the National Counterintelligence Executive，“Foreign Spies Stealing US Economic Secrets in Cyberspace：Report to Congress on Foreign Economic Collection and Industrial Espionage，2009～2011，” available at：October 2011，http：//www.dni.gov/files/documents/Newsroom/Reports and Pubs/20111103_report_fecie.pdf.

正因追踪和取证对于管控经济网络间谍活动非常重要，因而合作能否展开就取决于具体网络窃密行为的性质和涉案国如何看待彼此间的外交关系。对于一般的网络犯罪行为，一般都会给予积极配合。但一旦涉及国家主权、核心国家利益或国家声誉，则往往不予配合，如 2014 年 5 月美国司法部公布针对中国军人的诉状，中国政府第一时间否认相关指控，并即刻进行外交反应。这意味着美方事先没有就调查取证向中国提出协助请求，尽管中美 2000 年 6 月就签署了《关于刑事司法协助的协定》，包括在刑事诉讼的文书送达、调查取证以及冻结、扣押、没收等程序中提供协助，显然美方特意绕过了这一机制。中方在获知起诉后也未表明要进行调查，包括核实有关人员是否存在、相关指控是否事实等。可见对于这类关乎司法管辖主权和国际关系基本准则的问题，无论是否应为网络窃密行为承担责任，都很难有协助调查的意愿和行动。为了落实中美两国元首关于解决经济网络间谍问题的共识，2015 年 12 月中美打击网络犯罪高级别对话的一项内容，就是商讨一方遭受来自另一方境内网络攻击的个案时，可向对方提出哪些协助查询请求，另一方必须及时提供哪些信息。

第三，经济网络间谍损失缺乏合理有效的评估方法。尽管中美经济网络间谍争端主要涉及窃密事实的责辩，窃密造成的实际损失并不经常被提及，然而正是不恰当地损失评估将威胁提升到了不适当的高度，也将经济网络间谍问题塑造为中美核心议题。2009 年奥巴马曾提到全球每年因网络窃密造成的经济损失达 10000 亿美元（美国是最大受害者），[①]这是一个非常巨大的数字，数字来源是网络安全公司迈克菲（McAfee）此前发布的一份报告，[②]而后奥巴马多次引用该数字以表明美国面临严峻的网络安全形势。然而 2013 年，战略与国际研究中心和迈克菲公司又发布一份报告，称该数字存在计算方法上的错误，经重新估算美国因经济网络间谍的损失为 1000 亿美元，[③]且不论先后两种计算方法孰优孰劣，单就两个数字间的巨大差异，也可见经济网络间谍造成的损失实际上是很难估算的。

评估网络经济间谍活动给企业带来的损失非常复杂但又至关重要，商业机密和技术专利被窃取的损失涉及金融资产或知识产权损失、对企业品牌和声誉的损害、弥补用户受骗以及服务中断的机会成本，还有相应增加系统维护人员和网络安全措施

---

① The White House Office of the Press Secretary, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, available at: https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

② U.S. White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," May 29, 2009, available at: https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

③ James Lewis and Stewart Baker, "The Economic Impact of Cybercrime and Cyber Espionage," July 23, 2013, available at: http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

的成本。知识产权的价值确实很难估计，一些遭到网络窃密的企业不愿透露实际损失，还有一些企业则不知道到底被窃取了哪些数据。数据不准确是引发争端的重要因素，对于美国政府而言，将经济网络间谍问题上升到国家安全层级，很大程度上是因为损失巨大，来自企业、公众和国会的压力相应就大，而如果实际损失并不大，则很可能在一般的法律层面寻求解决方法，而不一定要上升到国家安全高度。因此，在经济网络间谍问题上，美国政府无疑受到网络安全公司和智库的误导，不恰当地将中国视作其网络安全的最大威胁来源之一，进而误判了中美网络关系的性质。

（三）合法性之争：经济网络间谍与网络情报搜集

美国政府以经济网络间谍为由指责中国的同时，毫不讳言自己也从事网络窃密活动。中美两国政府都秉持不参与不支持经济网络间谍的立场，中美争端的焦点在于能否及如何区分经济网络间谍和其他网络窃密活动，由于网络窃密的虚拟性和跨国性，在主权管辖和相互协作的方式和途径上，并未建立起行之有效的合作机制。

一方面，美国政府将经济网络间谍与网络情报搜集区分开来。美国国家安全局长期系统地通过网络入侵各国互联网和通信系统获取数据，是众所周知的事实。面对国际社会的指责，美国政府以应对恐怖主义威胁为由辩解，而各国确实也没有可援引的国际法和国内法，来应对美国情报机构入侵网络和窃取数据的行为。时任美国司法部部长埃里克·霍尔德（Eric Holder）称，尽管所有国家都从事间谍活动，但美国政府从来不把本国情报机构收集的信息转交给美国企业，使其在商业上得益。针对司法部起诉中国军人案，“本案的不同之处在于，我们面对的是国家支持的实体在利用情报手段获取商业优势。”这一表述基本上体现了美国政府刻意区分经济网络间谍与网络情报搜集的基本逻辑。于是，当美国国家安全局被曝光对中国政府和华为等企业进行监控和窃密后，美国国家安全委员会发言人凯特琳·海登（Caitlin Hayden）即刻辩解道，“我们不会将搜集到的情报交给美国公司，帮助它们增强国际竞争力。”[①]国家安全局发言人瓦尼·瓦因斯（Vanee Vines）紧跟着阐明立场，“持续和有选择地公布国家安全局跟踪合法的外国情报目标时使用的特定技术和工具，不利于美国和盟友的安全。”[②]

另一方面，美国政府积极推动其网络情报合法化。在国内，通过立法和行政命令赋予情报机构在网络空间更大的活动权限，并以信息共享的方式促使企业与政府合作，这方面以《美国爱国者法案》的相关条款为主要依据。国际上，则将以安全和外

① Gregory Wallace, “Report: Leaked Snowden Documents Show NSA Hacked Chinese Telecom Company,” *CNN News*, March 24, 2014, available at: http://money.cnn.com/2014/03/23/technology/security/nsa-china-huawei.

② Gregory Wallace, “Report: Leaked Snowden Documents Show NSA Hacked Chinese Telecom Company.”

交为目的的网络情报活动等同于传统形式的情报和间谍活动，是合法和必要的维护国家安全的手段，以此与经济网络间谍区分开来，尽管两者都包含未经授权进入其他国家网络系统和未经许可读取数据的行为。美国情报机构拥有强大的网络情报和网络攻击能力，通过长期、大规模和系统性地监控和入侵各种网络系统，网络情报搜集和海量数据处理能力不断提高，这对于提升预防和应对恐怖主义袭击发挥了积极作用，也有助于加强国际反恐合作中的情报共享。美国政府重点强调各国共同关注的反恐合作，要求国际社会在美国情报机构入侵多国网络系统和数据中心问题上保持宽容，显然这是一种典型的双重标准。

窃密与情报的差异在于获取信息的目标。情报活动是国家处理对外关系的重要手段，现有国际法对情报和间谍行为没有明确的规范，对经济网络间谍行为也无相关规定。从事经济网络间谍的主体是政府、犯罪组织还是个人，对于问题性质判断和解决途径有着直接影响。就国家职能而言，制定有利的贸易、金融和市场管理政策，帮助本国企业获取竞争优势，是一项重要职责，因此，任何一国政府都会进行公开或秘密的经济情报活动，如驻外使领馆即承担搜集驻在国经贸政策信息的职责。为此，美国政府积极寻求其政策主张的国际支持，如 2016 年 3 月，美国和德国第四届网络双边会议发表声明，称双方讨论了利用各种外交工具来应对网络空间的恶意行为，包括通过网络窃取知识产权以获得商业收益的行为。[①] 这显示美国政府将推动国际社会接受对其有利的认知和理解作为其一项政策目标。

三　美国的考虑与中国的反应

经济网络间谍日益成为全球性公共问题，中美经济网络间谍争端无疑最受国际社会瞩目，其激烈程度和影响范围大大超过其他国家间的类似纠纷。美国积极挑起中美经济网络间谍争端有其深层考虑，既有维护美国企业利益的现实压力，也是为了把握中美关系主动权，还包含维持网络空间国际领导地位的战略意图。而作为一个具有重要影响力的网络大国，中国在应对相关指责时的坚定立场无疑也促使了冲突升级。鉴于迄今中美经济网络间谍争端的演变具有非常明显的单边特征，此处侧重探讨美国的动机，并对中国的反应略加评述。

（一）维护企业利益的现实考虑

私营企业是美国经济运行的基础，通过向国际市场输出高品质的产品和服务，美

① U.S. Department of State, "Joint Statement on U.S.-Germany Cyber Bilateral Meeting," March 24, 2016, available at: http://www.state.gov/r/pa/prs/ps/2016/03/255082.htm.

国企业获取了大量高额利润，成为提升本国国民福祉和国家综合实力源源不断的动力。美国的强大建立在其大量具有国际竞争力企业的基础上，技术专利和商业机密是美国企业的核心资产，也是维持国际竞争力的根本，保护企业的技术专利和商业秘密不被非法窃取和滥用，也成为美国政府的重要职责，甚至是国家安全的首要目标。而且，美国自认为站在世界科学技术的顶端，美国的技术专利和商业机密才是有价值的网络窃密目标，并在潜意识里认为其他国家包括中国的技术和商业秘密则是不值得窃取的，因而是经济网络间谍的唯一和单方面的受害者，美国国家情报总监办公室的一份报告就指出，"因为美国是一个领导者，是新技术发展和全球金融贸易网络的核心角色，其他国家收集美国技术和经济信息的意图和行动将继续维持在较高水平，从而对美国经济安全形成日益增长和持续的威胁，这种网络威胁将随着全球信息环境和技术进步的不断发展而加大。"①

经济网络间谍涉及窃取企业技术和商业机密、侵犯企业知识产权等问题，大规模的网络窃密确实从根本上侵害美国企业的切身利益和国际竞争力。战略与国际研究中心的一份报告认为，"外国针对企业的经济网络间谍活动则抵消了对教育、科技和研发进行投入带来的竞争力，使得被盗的发达国家难以生产那些需要用来支付进口账单的商品，因而间谍活动实际是为国外生产厂家进行了补贴。"②这就令美国政府高度关注经济网络间谍问题，并且意图通过外交、司法甚至军事手段加以应对。

美国政府认为，美国的经济运行对网络空间的依赖已经达到前所未有的程度，其先进技术、商业机密和知识产权面临着比传统条件下更复杂、更难以防范的风险，并认为获取他国先进技术和商业机密可能被一些国家作为实现跨越式发展的重要手段，外国政府不仅有通过公开渠道搜集、学术交流、商业合作等合法途径，也有包括商业间谍或网络窃密等灰色或非法的途径。美国企业在各自环境中比其国内和国外竞争者有更吸引力的价格和质量来进行设计、生产并销售货物，以及提供服务的能力和机会。美国政府毫不隐讳对维护美国企业利益的重视甚至毫不妥协的立场，并力图提供全方位、更有效的保障。自 1995 年以来，美国总统每年都会向国会提交一份报告，详细陈述针对美国私营企业和科研机构的外国间谍活动情况，并提出应对措施。奥巴马政府第一个网络安全政策讲话就强调，"21 世纪美国经济的繁荣有赖于网络

① U.S. Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009~2011," available at: October 2011. http://www.dni.gov/files/documents/Newsroom/Reports and Pubs/20111103_report_fecie.pdf.

② Center for International and Strategic Studies, "The Economic Impact of Cybercrime and Cyber Espionage," July 2013, available at: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

安全，保护企业识产权和商业秘密关乎经济安全和国家安全”。[①] 2015 年《国家安全战略报告》更是宣示将依据本国法律和国际法，通过司法行动提高攻击者的代价，并通过外交甚至军事手段打击和遏止外部网络攻击和网络窃密活动。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行为、对美国国家安全和外交政策、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，从事网络攻击和网络窃密的个人或组织的资产或被冻结，禁止进入美国、禁止与美国公民或公司进行商业往来。[②]

就维护美国企业现实利益而言，美国政府还有另一层不可明说的考虑，即为美国企业在国内国际市场提供更全面和周到的支持，包括打压竞争对手、促使其他国家的市场对美国企业开放等。因此挑起中美经济网络间谍争端，还有为美国企业加一把力的意图，以帮助美国企业同中国对手竞争。如美国司法部诉中国军人案中，涉及美国铝业、阿勒格尼技术、太阳能世界、美国钢铁公司、西屋电气等五家企业，还包括美国钢铁工人联合会一家工会组织。从这几家企业的业务内容和市场范围来看，它们都是在近年来越来越受到中国企业竞争压力的产业和行业。此外，已经成为全球最大的通信设备供应商的中国华为，不断受到来自美国政府包括网络窃密、网络攻击和与中国政府保持特殊关系等指责，其网络和通信设备至今无法进入美国政府采购市场，也无法参与美国国家关键信息基础设施项目投标。

（二）制约中国的平衡主义思维

美国对华挑起经济网络间谍问题，反映了美国政府对于中美关系发展方向不确定的焦虑，也是基于其对中国网络能力增长和网络安全战略选择的应对，特别是对于中国提出的网络强国战略可能对美形成全面挑战的防范。中国应对美国指责和施压时显示出较为强硬的立场，也助推美国近年来出现的一种对华政策新思维：即不能帮助中国在与美国交往中获取利益，使中国扩大威胁美国国家安全的能力。美国外交关系委员会 2015 年 3 月发布的一份报告认为，美国现有将中国纳入美国主导下的国际体系的思路，并不符合美国的长期战略利益，“美国应平衡崛起的中国的力量，而非继续协助其已形成的优势”，“应采取更加强硬的对抗中国在网络空间行为的措

① “Remarks by the President on Securing Our Nation's Cyber Infrastructure,” May 29, 2009, available at: https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

② U.S. White House, “Executive Order: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” April 1, 2015, available at: https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

施”。①

在上述思维的引导下，美国政府将经济网络间谍的矛头集中指向中国也就不难理解了。随着中国在网络空间的利益、能力和影响力持续增长，近年来中美在网络领域的矛盾和冲突也逐渐增多，美国的网络战略也就有较多针对中国的成分。同时，中国有着不同于美国的发展和安全理念，引起美国政府的警惕，因而限制中国网络能力的发展，也就成为美国网络战略的重要目标。美国政府毫无讳言其盟友伙伴、敌对国家都在觊觎美国的先进技术和商业秘密，面临来自对手和伙伴无孔不入的威胁，但针对具体案例，就会根据国内政治和外交关系的需要加以区别对待。当经济网络间谍涉及其盟友，不仅媒体采取淡而化之的姿态，公众也不太感兴趣，政府往往低调处理。而当经济网络间谍涉及中国时，则会一哄而上，大加渲染。2007 年 8 月 2 日，华裔美国人孟小冬被援引《经济间谍法》指控获取属于 Quantum3D 公司的商业机密，并计划交给中国一家科研单位海军研究中心。② 而在 2010 年，依据《经济间谍法》审判的七起案件中，六起与中国有关。近年来，关于华裔美国人或中国人卷入经济间谍的案例接二连三，也显示美国政府从各个方面限制或打压中国的意图。

2015 年美国《国家安全战略报告》提出应从实力立场出发管控中美竞争，“就网络安全而言，我们将采取必要措施，保护我们的商业企业，维护我们的网络，对付窃取贸易机密获取商业收益的网络窃贼，不论是个体行为者还是中国政府。”③2016 年 4 月，美国国防部向国会提交中国军力年度报告，再次宣称“中国将继续利用外资投资、商业合资、学术交流、留学研究，以及国家支持的工业和技术间谍活动，以增加可用于军事研究、开发和购买技术和专业知识水平。”④实际上，美国政府认为其企业的商业机密和技术专利可能成为多个国家网络窃密的目标，而单独将中国描述成最活跃和最持久的经济间谍则有政治考虑，“炒作中国黑客威胁、人为制造所谓‘网络窃密’议题的背后，除面对中国发展的焦虑，就是要为美国发动网络攻击正名。美国大力推进网络战能力建设，拓展网络军事同盟，主张网络威慑，试图推动国际社会就网

① Rober D. Blackwill and Ashley J. Tellis, “Revising U.S. Grand Strategy toward China,” Council on Foreign Relations, March 2015, available at: http://i.cfr.org/content/publications/attachments/China_CSR72.pdf.

② U.S. Department of Justice, “Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center,” August 2, 2007, available at: http://www.justice.gov/archive/opa/pr/2007/August/07_nsd_572.html.

③ U.S. White House, “U.S. National Security Strategy of 2015,” February 2015, available at: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

④ U.S. Department of Defense, “Annual Report to Congress: Military and Security Developments Involving the People's Republic of China,” April 26, 2016, available at: http://www.defense.gov/Portals/1/Documents/pubs/2016 China Military Power Report.pdf.

络战制定规则，为其先发制人的网络攻击战略披上合法外衣。”[①]因而，在经济网络间谍问题上挑起与中国的争端，契合美国国内正在讨论的所谓“第三波抵消战略”的思路，也是在网络空间制约中国的具体体现。

（三）谋取全球优势的网络战略

美国是互联网的创建者和推动者，对于互联网及网络空间的全球推广、信息社会的培育成长有着积极贡献，美国决策者据此认为可以享有特殊权利、维持优势地位，成为网络空间的领导者，对于那些可能挑战美国网络优势和网络事务主导权的想法和做法，美国则想方设法予以规制和打压。

美国政府强调领导网络空间国际规则的制定和主导网络安全治理，这是其谋求全球领导地位大战略的一部分。奥巴马政府将塑造国际秩序作为国家安全的战略支柱之一，在处理国际事务时往往以国际规则的诠释者和维护者自居。奥巴马虽曾表示美国不能要求他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国际标准，但总体上是意图以其制定或认可的规则来约束其他国家。

而网络空间是一个新型领域，网络空间的国际规则远未完善，国际秩序有待形成，越来越多国家寻求利用网络空间行使传统的国家力量，而同时对什么是网络空间可接受的国家行为，国际社会又缺乏各国一致认可的、清晰的规范。美国认为其职责就是要填补这个“鸿沟”，“通过制订规范来确保网络空间的稳定”。[②] 美国意图抓住先机，将对美国有利的政策选择塑造成为国际共同遵守的网络空间国际行为规范。2015 年《国家安全战略报告》强调，美国将致力于“塑造网络安全的全球标准”，[③]斯诺登揭秘美国国家安全局棱镜计划后，奥巴马政府极力为其全球网络监控和网络入侵行为辩护，并将基于反恐和国家安全的网络监控行为与基于商业获益的网络窃密行为进行区分，试图赋予其长期从事的网络监控活动以国际合法性。此外，美国政府还推出一系列构建网络空间规则的具体措施，包括规划各类网络安全国际合作议程、在现有各种网络治理平台推动机制化合作、为双边和多边网络安全合作提供专业支持等，力图通过这些措施扩展美国网络战略的国际影响力，寻求国际社会对美国的价值理念和政策主张的认同和支持。从效果看，美国将经济网络间谍和网络情报搜集活动确定为不同性质的网络行为，确实得到了一些西方国家的支持，美国政府反过来

---

① 钟声《别把网络当战场，切勿损人又害己》，载《人民日报》，2013 年 2 月 27 日，第 1 版。

② U.S. White House, “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” May 2011, available at: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

③ U.S. White House, “National Security Strategy of 2015,” February 2015, available at: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

以此为据来约束其他国家的网络行为，并保持其网络空间的领导地位。

对于中国而言，美国上述三个方面的考虑，一些是可以互洽的共同利益，如建立信息领域的技术和贸易规则、打击破坏市场秩序的网络犯罪等等。而一些则是结构性矛盾，中美经济网络间谍争端与其他领域的争端具有同质性，即美国意欲维持其领导下的国际秩序并制订符合其国家利益的规则，而中国则需要寻求与自身国力相匹配的国际话语权和与自身利益相一致的国际秩序。在网络空间亦是如此，中国政府面对美国的指责时采取针锋相对的姿态，是认为美国的作为侵犯了中国的网络空间主权和网络安全利益。这也反过来增强了美国政府的不满和担忧，即如果不能在网络安全国际规则的制订和阐释中占据主动，也不能指望在国际贸易和跨国投资等领域继续维持优势。总之，中美经济网络间谍争端反映了中美关系中的这种结构性矛盾，即使经济网络间谍问题可以得到管控，也会在其他领域形成新的争端。

四　塑造共识、建立规则和务实合作

中美围绕经济网络间谍而展开的博弈，既是两国网络发展道路和网络安全战略的一种碰撞，也可视作两个网络大国理念认知和利益诉求的互动调适过程。尽管中美围绕网络安全问题有过激烈的言辞交锋和微妙的明争暗斗，两国政府都认识到妥善处理分歧和发展务实合作的重要性，也都有意愿在网络领域探索大国相处的新路径。

（一）建立应对共同网络威胁的共识

应当建立的第一个共识是经济网络间谍是中美面临的共同威胁。迄今中美经济网络间谍争端的一个重要特点是对于威胁认知的共识不足，甚至双方都将对方视为网络安全威胁的最大来源。中美两个网络大国都在积极利用互联网促进经济、社会、军事等领域发展，都需要确保网络空间的开放、安全和互通，而经济网络间谍不仅对美国，也对中国的经济发展和网络安全构成威胁。在全球范围内，通过互联网和电信网络窃取企业技术专利和商业机密，其规模和造成的损失呈不断增长的趋势，但美国政府主要指向中国政府支持的网络窃密，形成一种仅仅是美国才是经济网络间谍主要受害者的印象，这不仅不符合事实，也是不公平的。

美国是当前世界上科技水平最先进的国家，其企业研发投入、科技成果的积累都居世界前列，因而往往“疑邻盗斧”心理作祟，认为其他国家都有动机从其企业获取商业机密和先进技术。对中国而言，随着科技水平不断上升，科研投入不断加大，也面临保护知识产权和企业研发投入的压力，中国政府多次表示中国也是经济间谍和网络窃密的受害者，这并不仅是应付美国的指责，而是正在发生的现实，且未来形势

更加严峻。根据斯诺登揭秘曝光的一份美国国家安全局文件，该机构自 2007 年起就侵入华为的内部网络和服务器，目的是为了获得包括源代码在内的华为系统技术资料，以便监控那些安装了华为网络设备的系统，同时寻找华为与中国军方的联系。由此可见，美国以前和现在对于经济网络间谍的担忧，也是中国现在和将来要面临的问题。

第二个应当形成的共识是经济网络间谍并不有利于经济社会可持续发展。在经济网络间谍问题上，确实存在一种思维，即通过获取更广泛的经济、技术和安全信息，有助于实现本国关键技术突破和提升经济增长潜力，这种思维在中美两国都存在，即为本国政府在网络空间的政策和行为辩护，不论是出于经济发展的经济网络间谍行为，还是为了维护国家安全和社会稳定的网络情报活动。

在美国，一种代表性的观点是认为中国政府的策略是通过间谍手段获取先进技术，从而实现跨越式发展，而中国在技术改进和产品研发即是受益于经济间谍活动，甚至将“863”计划、“973”计划等科技发展规划与经济间谍相联系。① 这种认知既有信息不充分的逻辑缺陷，也有结论先导下的主观臆断，忽视了中国对基础科学和应用研究的重视，没有看到中国政府在推动科技进步方面的积极作用。并且科学研究需要系统和长期的投入，包括资金保障、人才培养、项目支持等等，单就一些具体案例涉及的隐形材料、制药工艺等受美国集中指责的产品和技术而言，也绝非通过偶尔和片段的机密信息就能完成突破的。

第三个共识是中美负有促进网络空间稳定和善治的共同责任。中美都是互联网大国，网络空间全球治理和管控经济网络间谍需要包括中美在内的大国合作。“作为网络大国，不是要对信息资源更多地掠取，不是要对话语权更多地垄断，而是要承担更多义务，履行更多责任，贡献更多力量。”②网络空间的安全、战略、治理等是国际关系新领域，各国的理念认知和利益诉求在不断发展演变，中美的网络战略也有相互塑造的空间，中美网络战略存在分歧，但共同点也非常广泛，如都致力于构建一个和平、稳定、开放和互连的网络空间，都表示坚决反对网络空间的军事化，都认为网络犯罪和网络恐怖主义是中美共同威胁。光从政策表述看，两国的合作空间毫无疑问是非常广泛和丰富的，但现实又是两国间的纷争不断。正如分歧不会一开始就出现，共识的形成也需要一个过程，是通过不断争论、交流、互动逐渐形成的。

---

① “The Emergence of the Cyber Nation-State and Technology Espionage Red China Rising and Its Global Cyber Theft Strategy,” in Ulsch N. MacDonnell ed., *Cyber Threat: How to Manage the Growing Risk of Cyber Attacks* (John Wiley & Sons, Inc., 2014), p.36.

② 鲁炜《担当大国责任 共建网络空间命运共同体》，2016 年 4 月 27 日，参见网页：http://www.cac.gov.cn/2016-04/28/c_1118761681.htm.

(二)制定共同遵守的国家行为规则

中美经济网络间谍争端演变过程中,规则争议贯穿始终,双方都非常强调规则对于妥善处理分歧和争端、改进网络空间治理的重要意义。2011 年 5 月美国在《网络空间国际战略》中提出致力于制定公认的国际协定与新标准,加强网络安全的同时维护自由贸易和信息自由流动。[①] 11 月,中、俄等国向联合国大会提交《信息安全国际行为准则》,呼吁各国尽早就规范各国在信息和网络空间行为的国际准则和规则达成共识。但网络空间国际行为规则的建立并不顺利,其原因在于各国政府都有各自不同的国家利益和原则立场,希望建立于己有利的规则内容。美国意图以其单边认定的规则限制和约束他国行为,同时维持甚至扩展其自身行动自由,图谋有利的网络环境,不仅未能得到国际社会的普遍赞同,也使得美国卷入越来越多的争议与冲突。就经济网络间谍问题而言,建立共同遵守的网络空间国际行为规则,可从以下几点展开。

首先,确立主权原则对于管控网络空间国际争端的适用性。网络空间应当有相适应的主权管辖,这是重要的国际关系基本原则,管辖边界可以通过协商达成一致。中国一向强调国家主权适用于互联网,先后提出互联网主权、网络主权等概念,并将保护网络空间主权利益写入 2015 年 7 月通过的《国家安全法》,首次将政治宣示上升为国家法律,拟议中的《网络安全法》更明确地提出维护网络主权的目标。而美国政府也并非完全排斥网络空间的主权管辖,对于信息社会世界峰会、联合国专家工作组等提出各国政府有权制定互联网相关公共政策的意见,美国也不持异议,2015 年 5 月,美国国务院网络事务协调员克里斯托弗·佩因特(Christopher M. E. Painter)明确承认"网络主权一定程度上是适用的",[②]这是迄今美国政府对于网络主权基本立场的最直接表述。美国对网络主权提法保持警惕,主要是担心其他国家借此排他性地管辖境内互联网事务,影响美国在全球网络空间的行动自由。各国基于自身安全和发展需要,独立自主制定互联网管理政策和法律,这是一个事实,并不受到外部力量的干预。网络主权的形成需要得到国际法、国际公约的确认,这将是一个长期过程,而不论网络空间能否如领土、领海、领空一样,成为国际社会相互承认和共同遵守的主权管辖领域,在面对国际网络冲突时,一个基本前提是确定管辖边界。现阶段,针

---

① U.S. White House, "U.S. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, available at: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

② Christopher M. E. Painter, testimony before the Senate Foreign Relations Committee Subcommittee on East Asia, the pacific, and international cybersecurity policy, "Cybersecurity: Setting the Rules for Responsible Global Behavior," May 14, 2015, available at: http://www.foreign.senate.gov/hearings/cybersecurity-setting-the-rules-for-responsible-global-cyber-behavior.

对共同面临的网络犯罪、经济网络间谍、网络恐怖主义等问题，中美完全可以就主权原则在网络空间的适用性展开交流和磋商，达成一致意见，进而在联合国等平台将中美共识扩展为国际讨论的基础。

其次，明确网络空间国际行为的国家责任。网络空间国际行为难以规范的一个重要原因是规则的缺失，美国战略与国际研究中心的网络问题专家詹姆斯·刘易斯（James Lewis）就称“没有国家行为的国际协定，不可能确保网络安全”，[①]因此，不论是以主权原则为核心构建“多边主义”的网络空间国际秩序，还是以多利益攸关方为基础的“多方主义”治理模式，都必须首先确定网络空间国际行为的责任归属。可明确将一国政府作为网络空间国际行为最后责任人的角色，即以网络行为实施者及其网络接入点为依据判定管辖权和责任归属。在包括经济网络间谍在内的网络窃密问题上，之所以许多案例不了了之，受害者无从寻求追偿，一个重要原因是网络窃密实施者及其网络接入地所在国家未在网络行为溯源和追踪、网络取证和嫌疑人控制等方面予以充分配合，网络窃密事实认定及嫌疑人起诉审判都无法进行。故配合经济网络间谍受害国的调查请求，就成为一种国际责任，不应以技术能力或不承担责任为由推脱。另根据权责相适的原则，应赋予国家管理本国网络空间国际行为的合法性，同时在提升政府相应侦查和执法能力方面展开合作。

第三，遵循建立最低限度共识并逐步扩展的规则形成路径。中美管控经济网络间谍争端的一个有益启示是，从个别到一般的思路有助于网络空间国际行为规则的建立。若双方首先从反对任何形式的网络窃密展开谈判，则很难在是否允许基于国家安全和反恐目的的网络情报搜集和网络入侵等问题上达成一致，正是因为在经济网络间谍问题上设定的规则是“双方都不会在知情的情况下支持网络窃取知识产权、商业秘密、并且提供给企业获取商业利益的行为”，含义明确，且中国政府本来就持反对经济网络间谍的原则立场，接下来就是如何确保各自政府部门切实遵守相关承诺的问题，进而化解了中美网络关系的一个主要冲突点，并以此为契机将中美拉回到对话协商的轨道上来。因此，中美网络空间国际规则的协商应从指向明确、有助于双方明晰自身利益和权责、各方共同关切的行为入手并逐步扩展。

（三）发展管控网络分歧的务实合作

当前，各国政府管理网络事务的能力和制度建设普遍落后于网络技术和应用的发展，都面临能力建设和制度规划的压力。中美两个互联网大国促进网络发展、维护

① James A. Lewis, Statement before the House Committee on Foreign Affairs, “Cyber War: Definitions, Deterrence and Foreign Policy,” September 30, 2015, available at: http://docs.house.gov/meetings/FA/FA00/20150930/104003/HHRG-114-FA00-Wstate-LewisJ-20150930.pdf.

网络安全和打击网络犯罪等问题上的务实合作，不仅有助于促进政策意图的相互理解、妥善解决双方矛盾和分歧，对其他国家和国际社会也将产生示范效应，推动网络空间的全球治理水平。中国政府主张网络安全不能建立在个别或一些国家安全而其他国家不安全的基础之上，也愿意正视中美网络争端、寻求务实合作以促进共同安全，“中国愿同各国一道，加强对话交流，有效管控分歧，推动制定各方普遍接受的网络空间国际规则。”“健全打击网络犯罪司法协助机制，共同维护网络空间和平安全。”①美国政府也在各种场合表达了愿与中国对话交流和发展合作的意愿。

对话交流与合作可以从多个层面展开。在战略层面，通过两国最高决策层的直接对话，明确中美应对网络争端的基本立场，是通过对话而非对抗，加强交流而非互斥，从而促进相向而非背离，一旦两国发展网络空间合作的大方向确定下来，则涉及双方利益和关切的具体问题，就都是可以展开合作的领域。因而在中美经济网络间谍争端发展演变的不同阶段，中国政府都表达了推动网络空间成为“双边合作新亮点”的意愿和信心，②促使美国政府意识到并且相信网络安全合作是必要的、可行的，这也是中美网络安全对话能够进行并取得进展的重要前提。

务实合作有着广阔的空间，最有效的方式是两国政府对应职能部门之间的合作。一般而言，具体职能部门更多关注事务本身，受政治立场和外交氛围的影响相对较小，更易展开合作，也更可能获得实际成效，进而积累共识，增加互信。前文所述中美《刑事司法协助协定》即是部际合作的重要机制，双方司法部为协定指定负责机构，两国在双边协定和多边公约框架下开展刑事司法协助，在一些个案合作上取得很大成效。尽管由于中美刑事司法协助请求涉及的案件大多较为复杂，一些协助请求并没有得到预期回应，但这一途径还是为双方解决分歧提供了很好的缓冲。中美打击网络犯罪的合作也由两国司法部负责，这也是 2015 年中美达成网络安全共识后落实的第一个定期双边对话机制。

技术层面是务实合作的重点，由于通过网络间谍获取经济收益的动机很难根除，故应在切断获利和变现的途径，以及在惩治网络窃密活动调查取证的相互协助等方面扩展合作空间。这些都需要两国政府从立法和管理入手，将国家承担的网络空间国际责任转化为政府部门、私营机构和网络用户的法律依据和行为规范，对于跨国犯罪或侵权，受害一方可以通过双边或多边条约，要求相关国家给予司法协助，如司法文书传递、涉案证据搜集、嫌疑人引渡等。

---

① 习近平《在第二届世界互联网大会开幕式上的讲话》，载《人民日报》，2015 年 12 月 17 日，第 2 版。

② 参见《习近平同奥巴马总统举行中美元首会晤》，载《人民日报》2013 年 6 月 9 日，第 1 版《跨越太平洋，路在脚下——习近平主席对美国进行国事访问综述》，载《人民日报》2015 年 9 月 30 日，第 2 版。

结　语

网络空间是一个新型空间，与互联网快速发展和广泛应用相对应的，是国家的战略认知和政策应对、国际的行为规范远落后于技术变革所蕴含的创造力、想象力和破坏力，社会和政治关系发展相对滞后造成的制度不适应也自然会反映到中美网络关系中。

迄今，美国在网络空间仍保持总体优势，这使得中国在处理两国网络争端时必须考虑实力对比。2015 年 9 月中美元首会晤达成共识，要求各自约束基于商业目的的网络间谍活动，但没有为出于国家安全目的的网络入侵行为设限。中美两国对两类网络间谍活动有着不同的关切，显然美国政府的要求得到了优先满足。同时，中国也已是举足轻重的网络大国，在网民总数、市场规模和发展潜力等方面显示出巨大吸引力和重要影响力，美国政府也不得不慎重考虑中国对其政策可能的反应。

总之，经济网络间谍问题的根源是商业获益，网络空间蕴含的经济利益越大，经济网络间谍的威胁也就越大，中美确定从打击网络犯罪的司法合作出发解决双方关切，是管控分歧、避免冲突的一个可行选择。应认识到经济网络间谍问题确实对企业利益以及国家经济安全造成威胁，美国政府挑起经济网络间谍争端固然有抹黑中国或对中国施压的考虑，但另一重要驱动力源于对本国企业和经济竞争力的保护。随着中国信息化进程进一步发展，经济网络间谍也将成为需要面对的问题，所以应既要明确反对任何形式网络攻击和网络入侵，也要认识到经济网络间谍不仅是中美争端，更是全球性公共问题。中美在协助个案调查取证、制定国际行为规则、加强国际应对能力等方面展开务实合作，这是两个互联网大国的共同责任。

汪晓风：复旦大学美国研究中心副研究员

（本文责任编辑：魏红霞）

ARTICLES