网络安全视角下中美贸易冲突的分析

汪晓风*

【内容提要】 基于网络安全目标的政策和法规往往包含贸易限制措施，可能改变贸易均衡和贸易结构，推动贸易报复的产生和升级，这是中美贸易冲突演变的重要动因之一。而在网络技术和应用与贸易过程不断融合的趋势下，网络安全关切难以通过贸易冲突的方式得到解决。本文以网络安全与贸易过程的逻辑结构为起点，分析触动贸易规则的各种网络安全议题，梳理网络安全与中美贸易关系的互动演变，探讨网络安全影响中美贸易关系的主要原因。本文认为，妥善解决中美间网络安全关切，有助于缓解贸易数量失衡和贸易结构扭曲、响应自由贸易和公平贸易诉求，促使经贸关系回归稳定中美关系的作用。

【关键词】 中美关系 贸易冲突 网络安全

* 汪晓风，复旦大学美国研究中心副研究员。复旦大学国际关系与公共事务学院本科生谭桂雯对本文写作亦有较大贡献。本文是教育部人文社会科学重点研究基地重大项目“中美战略新边疆的互动与博弈”（17JJDGJW003）的阶段性成果。

2018年3月22日，美国贸易代表办公室公布《对华“301调查”报告》，报告确认此前美国总统特朗普一份备忘录中关于中国长期执行“不公平”贸易政策的要点，其中包含诸多对中国互联网管理政策、法规和行动的指责，认为中国政府通过支持商业网络窃密、执行网络安全审查、限制跨境数据传输、实施数据等级保护等做法，歧视性地对待美国企业，削弱了它们的市场竞争力，继而伤害了美国的经济和就业。①特朗普随即指示行政当局采取贸易报复措施，包括向世界贸易组织起诉中国，对航空航天、信息通信技术、机械等中国输美产品清单加征关税，限制中国企业通过投资获得美国关键技术等。这份报告是中美贸易冲突的重要节点，鉴于报告对网络安全的特殊关注，以及网络安全议题在中美贸易中不断扩大的影响，本文尝试对网络安全在中美贸易冲突中的角色定位、作用路径和影响方式进行分析。

一、网络安全与贸易过程的逻辑结构

随着网络技术和应用的发展，经济社会运行与网络空间密切融合，网络安全日益成为国家战略规划和政策制定的核心议题，并全面向经济、政治、军事、社会等领域渗透，包括融入贸易过程的各个环节。

（一）内涵与目标

一般而言，网络安全是网络和安全的逻辑组合，是安全在网络空间的延展或投射。在国际关系研究中，网络安全已逐渐成为安全研究谱系一个新的重要分支，反映了网络空间发展对国际体系运行的深远影响。安全（security）则是国际关系的基本概念和重要目标，是免于危险与恐惧的客观现实或主观感知，是不存在或未觉察到风险或威胁的状态，传统现实主义代表性学者、耶鲁大学和约翰·霍普金斯大学教授阿诺德·沃尔弗斯（Arnold Wolfers）在其著作《纷

① Office of the United States Trade Representative, “Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974,” March 22, 2018, https://ustr.gov/sites/default/files/Section 301 FINAL.PDF.

争与协作——国际政治论集》中，从主体价值的角度将安全描述为“客观上对所获得的价值不构成威胁，主观上不存在这样的价值会受到攻击的恐惧”①。

参照沃尔弗斯的定义，可以将网络安全视为网络空间对于活动主体的一种价值，是网络环境不存在风险或风险可控、网络活动不产生威胁或威胁已被消除的一种状态。国际电信联盟曾提出一个工作定义，“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、最佳实践、保证和技术的总和”②。中国《网络安全法》则对网络安全作出了清晰的法律界定，“通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力”③。上述定义所指向的状态、总和及能力等反映了不同的观察角度和目标诉求，也说明对网络安全有着较为宽泛的理解。

网络安全目标是主体对于网络环境和网络活动能够达到理想状态的一种期待，也是国家战略规划和政策实施的核心目标，实践中往往形成一系列可量化的指标，并以技术标准和行为规范的形式固定下来。如英国标准协会制定的《信息安全控制操作规范》和中国国家质量监督检验检疫总局与标准化管理委员会发布的《信息安全控制实践指南》，均是将网络安全目标标准化和规范化的指导性文件。在上述两份规范性文件中，网络安全目标均被描述为“保护信息的保密性、完整性、可用性及其他属性，如不可否认性、可控性等”④。这就体现了国际上对于网络安全目标一种共识，而在国际贸易中，一国政策法规的条文和外国经营者的需求之间仍然存在诸多无法兼容之处，不同主体在网络安全目

① Arnold Wolfers, *Discord and Collaboration: Essays on International Politics*, Maryland: The Johns Hopkins Press, 1962, p.150.

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

③ 参见《中华人民共和国网络安全法》，第七十六条。

④ British Standards Institution: *BS EN ISO/IEC 27002:2013*, BSI Standard Limited 2013, November 2013, p.28；国家质量监督检验检疫总局、国家标准化管理委员会：《信息控制安全实用规则（GB/T 22081-2016）》，2016 年，第 22 页。

标上的分歧往往会形成数字贸易壁垒，这也是导致迄今全球统一的数字贸易规则难以达成的重要原因之一。

如保密性（Confidentiality）是指网络信息不被泄露给未经授权的用户、实体或过程，强调只有被授权对象有权使用信息的特征。可控性（Controllability）则是指对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统。[①]在国际贸易中，商品和服务的定价和议价过程、交易合同和报关文件等数据传输都涉及商业秘密，一般做法是贸易各方通过租用专线或虚拟专用网络（VPN）进行传输以保证重要数据不会外泄，确保跨境信息流动的保密性。而一些国家出于维护国家安全或公众利益的目的，对于租用专线和虚拟专用网络进行跨境传输有着较为严格的限制，如要求提供访问接口或将加密密钥提供给监管者。这样，国家基于跨境数据传输的可控性目标而制定的政策和国际贸易经营者基于商业利益而进行加密传输的需求之间就产生了矛盾。

又如可用性（Availability）是指保证合法用户对信息和资源的使用不会被不正当地拒绝。网络资源和网络数据的可用性对于国际贸易参与者的重要性不言而喻，这种可用性不仅指贸易参与方对于网络交易平台稳定运行和网络数据有效获取的需求，而且包括通过互联网提供的数字产品和服务可以合法地进入目标市场。如此看来，一国为维护网络信息安全而采取的过滤信息、屏蔽网站和应用服务、禁止访问社交媒体等技术和措施，也会被美国视为一种市场准入的限制，或是不利于美国企业的歧视性做法。美国政府就常常抱怨其互联网运营企业无法进入中国市场、获取利润，致使受牵连美国企业的潜在损失高达十亿美元。[②]

再如不可否认性（Non-repudiation）是指在网络环境、在线交易过程中，信息交换双方不能否认其交换过程中发送信息或接收信息的行为。这一特性可为交易双方建立信任保障，促使贸易过程顺利进行，也是化解国际贸易纠纷和提起法律诉讼的重要依据。如《美墨加贸易协定》规定，“为促进数字贸易，缔约

---

① 王可：《信息安全“自主可控”》，载《人民日报海外版》，2014 年 4 月 5 日，第 8 版。

② The Office of the United States Trade Representative，“2018 National Trade Estimate Report，” March 2018，https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2018/2018-national-trade-estimate.

方应确保产品和服务供应商在应用数字化认证或电子签名时不受限制”①，如此就建立了不可否认性的安全目标与确保数字贸易有序进行之间的关键联系。一般而言，这种数字化认证和电子签名需要由商业银行等金融机构或第三方认证机构提供技术、平台和法律保障，并最终从主权国家的政府那里获得背书。完全实现了非中心化的数字货币也可以实现信息传输及交易过程的不可否认性，如基于区块链技术的比特币转账时会生成数字签名，私有密钥持有人是唯一可生成数字签名者，②并且每一转账行为都能得到全部节点的背书，这种去中心化的不可否认性机制虽然具备技术可行性，但迄今未能发展成为通行的国际贸易支付手段，正体现了网络安全目标和国家政策目标之间的差异。

（二）外延与过程

就网络安全的外延而言，可以从多个角度进行划分，观察角度的不同和目标应用的差异，就会衍生出不同的网络安全类别，如系统安全、应用安全、数据安全、传输安全等。从战略规划和政策制定角度，可以把网络安全划分为网络运行安全和网络信息安全两个大类。

网络运行安全涉及关键信息基础设施、网络、系统、平台、应用和服务，国家维护网络运行安全而制定的政策、法规和措施，会对采购产品和服务的贸易过程产生直接影响。如中国《网络安全法》规定，“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”③，由于关键信息基础设施涉及国家安全和国家利益，国家安全审查即是为了确保进入关键信息基础设施的网络产品和服务安全可控，这种审查并没有明确区分本国企业和外国企业的产品和服务，而涉及外国企业提供的网络产品和服务，外交关系也会成为国家安全审查的重要考虑因素，从而使得贸易过程会因为运行安全原因而被阻止和中断的可能。

---

① “The United States-Mexico-Canada Agreement（USMCA），” September 2018，https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/united-states-mexico.

② Bitfury：*White Paper on Blockchain Auditability*，November 14，2016，https://bitfury.com/content/downloads/bitfury_white_paper_on_blockchain_auditability.pdf.

③ 参见《中华人民共和国网络安全法》，第三十五条。

网络信息安全涉及个人隐私、知识产权、商业数据、社会和政治信息、国家机密等网络信息的搜集、存储、加工、传输、应用等。对此中国《网络安全法》也有规定，“国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录”，这对贸易数据跨境传输形成了约束条件，运营企业为使数据信息发布、传输和存储符合规定，必须增加技术、设备和人力投入，确保网络信息安全，一定程度上会导致贸易成本增加。同时，“对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播”①，该项规定将境外信息纳入管控范围，即便相关信息不包含法规禁止内容，也会由于增加了审查环节而对跨国贸易产生影响。

网络安全也是一个过程，即制定网络安全政策时，需要全面衡量网络系统的预防保障、应急处置和功能恢复等环节，确保为每个环节建立权责一致的制度安排、人员配备和资金支持。美国国家标准与技术局制定的网络安全框架将网络安全过程划分为防护、监测、响应、恢复四个阶段，②保护（Protection）即保障关键基础设施服务的提供，是对潜在网络安全事故的事先预防，包括设置防火墙、控制访问等。监测（Detection）是通过连续监控来识别网络安全事故的发生，是对网络安全事故的事中监测，要求信息来源稳定、建立实时监控系统。响应（Response）是对监测到的网络安全事故采取行动，是网络安全事故发生后的短期应急处理，对国家及时动员和资源调度能力提出要求。恢复（Recovery）则是恢复因网络安全事故而受损的任何功能或服务。③

网络安全过程不仅需要网络运营企业建立完善的保障制度，还需要技术、执法和安全等政府职能部门承担监管、处置和协调职能，以及需要与相关私营部门、技术社群、非政府组织和网络用户建立网络安全伙伴关系。就跨国贸易而言，网络安全过程的核心是运营企业创建、运行和维护的网络交易平台，政

---

① 参见《中华人民共和国网络安全法》，第五十条。

② The Cybersecurity and Infrastructure Security Agency（CISA），“Update on the Development of the Cybersecurity Framework，” June 18，2013，https://www.nist.gov/sites/default/files/documents/itl/nist_cybersecurity_framework_update_061813.pdf.

③ National Institute of Standards and Technology，“Framework for Improving Critical Infrastructure Cybersecurity，” February 12，2014，https://www.nist.gov/cyberframework/framework-version-10.

府部门通过开放接口提供报关和税收等服务，国际金融机构提供支付和结算等服务，全天候运转的国际贸易活动伴随着庞大的跨国数据流动和国际资金转移，需要执行高标准的网络安全过程，以及维持一致性的网络安全和贸易规则。一些跨国企业既是维护网络安全过程的活跃主体，也是推动贸易规则一致性的积极力量，如华为公司通过加入开放及可信技术论坛、参与东西方研究所网络空间项目，与欧洲各国政府协商 5G 网络建设事宜，以消除有关方面的网络安全顾虑，增强华为产品与服务的全球可用性，有利于延续、加强全球贸易合作。①

二、贸易过程的网络安全议题

随着互联网技术的发展和应用的普及，越来越多贸易活动通过网络空间展开，其交易平台、终端应用、电子支付、数据传输等需要应对各种网络风险和威胁，保障贸易过程的网络安全。与此同时，各国政府越来越重视网络安全，出台了各种维护网络安全的政策和法规，其中往往包含一些针对网络产品和服务的贸易限制措施，又可能推高贸易壁垒和引发贸易冲突。

（一）网络风险、威胁及保障

从电子商务到数字贸易，从线上运营到线上线下融合，日益网络化和数字化的贸易过程推动了贸易总量的提升和交易成本的降低。外贸企业因此也面临新的挑战，既需要为安全可信的网络环境支付成本，又需要为适应不断提升的网络安全规范而增加投入。

首先，网络运行环境蕴含的风险。网络运行环境涉及关键信息基础设施、硬件设备和软件平台，是应用和服务安全、可靠与正常运行所必需的基本设施与设备条件及其功能的总和。贸易过程的网络运行环境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，这些风险首先来自网

① 安迪·珀迪：《全球网络安全挑战：解决供应链风险正当其时》，2019 年 6 月 23 日，https://www.huawei.com/cn/about-huawei/cyber-security/whitepaper/huawei-cyber-security-white-paper-2016。

络运行环境的脆弱本质，分布广泛的关键信息基础设施很难抵挡恶意破坏，也会面临地震、海啸等自然灾害而造成损毁，这些风险也来自应用终端、传输介质及网络连接等类别广泛的通信和网络设备及其全球连接的复杂产业链，其稳定性、兼容性、可控性等诸多因素都会导致运行中断，这些风险还来自软件平台可能存在的漏洞，包括程序功能上的不足、应用结构的缺失以及整个系统逻辑框架的弱点，漏洞与网络技术和应用的发展相伴相随，是网络运行环境最主要的风险来源。

其次，恶意网络活动形成的威胁。恶意网络活动以制造和传播网络病毒、通过网络攻击和入侵应用系统等手段，以达到窃取商业机密、获取经济利益、破坏竞争者网络等目标。2018 年广泛蔓延的 Ryuk 勒索软件通过定制化和定向攻击，侵入上市公司等贸易主体的财务系统，加密重要数据和文件，要求支付购买网络保障和数据恢复的高昂费用，阻碍贸易活动正常进行。①通过网络窃取技术专利、贸易秘密及其他机密商业信息，使自身或本国企业在市场竞争中居于优势地位的做法，损害知识产权持有者的利益，危害市场开放和贸易公平，商业网络窃密也已成为科技创新和企业发展的重要威胁。据 2018 年美国战略与国际研究中心和网络安全公司迈克菲的一份报告测算，网络攻击和网络入侵等网络犯罪活动每年造成近 6 000 亿美元损失，大约占全球国内生产总值（GDP）的 0.8%。②不论报告测算方式是否合理、损失评估是否恰当，因恶意网络活动造成的商业和贸易损失确实呈不断上升的趋势。

最后，网络安全保障造成的壁垒。国家为维护网络空间稳定、打击网络犯罪而制定的政策、法规和措施，会不同程度限制信息技术产品、网络应用和服务、跨境数据转移等贸易或贸易相关活动的范围，即是因网络安全保障形成的贸易壁垒。如网络安全审查是市场准入的重要步骤，美国不仅对华为公司进入其市场实行严格的网络安全审查，而且将这种限制措施国际化，阻止华为在其

---

① Alexander Hanel, "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware," January 10, 2019, https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/.

② James Andrew Lewis, "The Economic Impact of Cybercrime-No Slowing Down," *CSIS & McAfee*, February 21, 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf.

盟友伙伴开展贸易活动。2019 年 9 月，美国副总统和波兰总理在华沙签署 5G 网络合作协议，并发表联合声明，称将确保只有可信和可靠的供应商参与两国基础网络建设，两国将加大对 5G 设备供应商进行审查的力度，确认外国政府对供应商的控制情况。①网络安全审查以潜在国家安全风险为重点评估内容，阻止或限制他国产品进入本国市场，提高了企业跨境贸易成本，也损害了自由贸易环境。

数据本地存储和分级保护政策对贸易企业运营成本和业务整合也有较大影响。美国贸易代表办公室经过评估后认为，要求数据存储本地化和等级保护制度对美国企业运营产生重要的不利影响，如中国要求执行等级保护标准，要求保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未经授权的修改，俄罗斯法律规定外国企业必须在俄罗斯境内处理以及存储通过电子渠道搜集的俄罗斯公民的特定信息，越南、土耳其等国也都有各种数据本地化和限制数据跨境传输要求，这将加重外国公司在这些国家中从事贸易活动的成本，影响其数据服务整合能力，是潜在的数字贸易壁垒。②

此外，保护个人隐私、商业数据和国家机密的政策法规也会降低国际贸易的便利性和提高合规成本。基于维护社会秩序和政治稳定目的而加强网络信息传播的监控和阻断操作，会干扰贸易过程的有序性。一些国家强调关键核心技术可控性，也会对相关产品的供应链完整产生不利影响。

（二）贸易规则、贸易保护及网络安全

世界贸易组织框架下的货物贸易多边协定、服务贸易总协定、与贸易有关的知识产权协定等一系列多边贸易协定，构成现行世界贸易体系的基本架构，确认了互惠、关税减让、市场准入、公平竞争等基本贸易规则，也赋予各缔约方在一定范围内基于产业保护和国家安全考虑实行贸易保护措施的权利。

货物贸易框架下，信息技术产品因其高技术含量和安全敏感性，往往会被

① U.S. White House, "Remarks by Vice President Pence and President Duda of Poland in Joint Press Conference," September 5, 2019, https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-president-duda-poland-joint-press-conference-warsaw-poland.

② The Office of the United States Trade Representative, "2018 National Trade Estimate Report."

施加高额关税和市场准入限制。《信息技术协定》是专门针对信息技术产品的多边货物贸易协定，涉及计算机、电信产品、半导体、半导体制造设备、软件和科学仪器6大类共200多项产品，成员应完全取消协议涵盖的信息技术产品的关税和其他税费，提高信息技术产品市场准入机会。①截至2018年底，协定成员已由最初29个增加至82个，贸易量约占世界总量的97%，年交易总值逾1.3万亿美元。近年来，一些国家出于维护网络安全目的，通过加征关税、限发牌照、专许经营等方式，限制特定国别或特定企业的信息技术产品进入本国市场。如2019年5月，美国总统特朗普签署名为“确保信息和通信技术及服务供应链安全”的行政命令，宣布进入国家紧急状态，限制信息和通信领域可能威胁国家安全的交易。②美国随后宣布对2 000亿美元中国输美产品加征25%关税。中国对此表示强烈反对，认为这是与世界贸易组织规则逆向而行的贸易壁垒。③

《服务贸易总协定》协调缔约方开展服务贸易，将国际服务贸易划分为跨境交付、境外消费、商业存在和自然人流动四种方式。④与货物服务相比，服务贸易更为复杂、涉及面更广、垄断性更强，尤其是与网络与信息安全密切相关的电信服务，服务贸易壁垒也比以关税为代表的货物贸易壁垒更为隐蔽。一些国家出台专门法律规章，限制面向本国市场和用户的在线服务与结算方式，这种国内救济方式不符合世界贸易组织达成的国际协定。⑤2010年9月，美国要求就“对支付卡交易的电子支付服务以及这些服务的供应商的某些限制和要求”与中国方面进行协商，称中国境内只允许中国银联公司提供以人民币计价的电子支

① World Trade Organization, “Information Technology Agreement,” November 22, 2018, https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm.

② U.S. White House, “Executive Order on Securing the Information and Communications Technology and Services Supply Chain,” May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

③ 2019年5月14日外交部发言人耿爽主持例行记者会就中美贸易战的表态，https://www.fmprc.gov.cn/web/fyrbt_673021/jzhsl_673025/t1663262.shtml。

④ World Trade Organization, “Agreement on Trade in Services (GATS),” https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.

⑤ 中华人民共和国商务部：《对外贸易壁垒调查暂行规则》释义及说明，2006年8月18日，http://www.mofcom.gov.cn/article/zhengcejd/bl/200608/20060802913146.shtml。

付服务，所有支付卡处理设备必须与银联兼容，且卡面必须印有银联标志。美方认为中国没有向其他成员的电子支付系统供应商提供国民待遇，构成服务贸易壁垒。①

《政府采购协定》致力于减少各缔约方公共行政部门运用财政支出购买产品和服务的贸易限制措施。政府采购是为了政府运行目的而非商业销售、转售，或供商业销售或转售的商品或服务的生产目的，以任何合同手段，包括购买、租赁和无论是否享有购买选择权的租购等方式进行的采购。非歧视性是政府采购协定的一般原则，缔约方对于来自其他缔约方的货物和服务及其供应商，应当立即和无条件地给予相同待遇。而在涉及国家安全或国防目的所需的政府采购方面，在其认为为了保护国家安全利益，一方可以阻止任何缔约方参与采购活动，或者不公开披露任何信息，也可以为保护公共道德、秩序或安全，以及为保护知识产权采取必要措施。②例外条款的存在，以及网络安全问题的高度敏感性，使得缔约方常常以国家安全为由，优先采购本国企业和本地产品，对特定企业的特定产品实行市场准入限制或采购限制。

可见，世界贸易组织框架下，针对信息技术产品、服务贸易和政府采购的规则设置，缔约方可以援引贸易规则例外，制定各种贸易限制措施，无论是否确实出于为网络安全的目的。例外规则的竞相运用就会降低已有信任，引发国家间贸易冲突。

三、网络安全与中美贸易冲突的互动

伴随着中美贸易的发展，其中涉及的网络安全议题轮廓逐渐清晰，影响日益彰显，并成为引发贸易冲突的关键要素，这其中既有两国经济产业发展引发的贸易结构改变、市场竞争加剧的原因，也与各自对于网络安全的理念认知、

① World Trade Organization, "Dispute Settlement, DS413: China-Certain Measures Affecting Electronic Payment Services," July 16, 2012, https://www.wto.org/english/tratop_e/dispu_e/413r_a_e.doc.

② World Trade Organization, "Agreement on Government Procurement (GPA)," April 3, 2017, https://www.wto.org/english/tratop_e/gproc_e/gp_revised_gpa_e.htm.

利益诉求和政策主张的差异有关。

（一）市场竞争与贸易稳定阶段

20 世纪 90 年代中期，随着克林顿政府将互联网向商业开放，以及中国全功能接入国际互联网，美国众多高科技企业和网络运营企业开始在中国市场进行投资、开展业务，获得丰厚的市场回报。一直到 2010 年前后，中美间与互联网相关的研发、贸易、投资等领域的合作总体是积极的。随着信息技术产品全球产业链逐步形成，中美网络产品和服务的贸易量和贸易品类不断增长，网络安全逐渐成为中美贸易不可忽视的影响因素。中国高科技和网络运营企业也快速成长起来，能够提供更加物美价廉的产品和服务，市场竞争力不断增强，中美网络运营企业逐渐从合作为主到合作竞争并存的状态。

在上述过程中，美国企业在华业务受同行业竞争的趋势越来越明显。中国互联网络信息中心的一份报告显示，2009 年 7 月，中国搜索引擎市场以百度和谷歌为主导，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%。[①] 数字对比清楚表明了谷歌在中国搜索引擎市场上的失利，谷歌公司将搜索引擎业务退出中国大陆，一定程度上是市场竞争的结果。但美国政府却将其归咎于中国实行过于严格的网络安全政策，是一种不公平的市场壁垒和贸易保护。中国政府则表示依法管理互联网是世界各国通行的做法，要防止对国家安全和社会公众利益有害的信息的传播，任何在中国境内经营的外国企业都要遵守中国的法律和规定。

2010 年 3 月 23 日，谷歌宣布即日正式关闭中国大陆网站，不再按照中国法规要求过滤搜索关键词，并将搜索服务器移至中国香港地区。对于退出中国内地市场的原因，谷歌称一是有黑客非法入侵其系统、窃取用户电子邮件、对其应用平台进行网络攻击，二是对用户搜索内容进行审查持不同意见。[②]该

---

① 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 页、第 30—31 页。

② 国务院新闻办公室：《谷歌退出中国内地》，2010 年 12 月 15 日，http://www.scio.gov.cn/zhzc/9/5/1/2010/12/Document/1008669/1008669.htm。

事件引起巨大反响，2010 年 10 月，美国美中经济安全与审查委员会称“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”①。2011 年 12 月，美国国务卿希拉里借此事指责中国“扩大政府权力，由政府为互联网制定条例规范，不仅损害人权和信息自由流通，还破坏了网络空间的互联互通，实质损害了美国在网络空间自由行动的权利和美国企业参与自由贸易的机会”②。

在这一时期，中美因网络安全关切引发争端初见端倪，但在中美贸易总体稳定的背景下，双方的反应和措施围绕事件本身展开，贸易分歧处于可控范围。中方将谷歌事件为代表的、涉及网络安全的贸易冲突归为个案，“谷歌事件只是一个商业公司的个别行为”③，谷歌公司仍在中国市场经营其他业务，说明主要是市场竞争及公共政策促成了这一事件，中方并不认同美方关于市场壁垒的观点。

（二）网络窃密与危机管控阶段

谷歌事件后，中美限制对方企业进入本国市场的政策措施开始增多。2012 年 10 月，美国众议院情报委员会认为中兴和华为与中国政府关系过于密切，可能帮助政府从事间谍活动和窃取商业机密，对美国国家安全产生威胁，建议政府禁止两家企业获得接入美国敏感网络的权限，并禁止收购美国资产。④2013 年 3 月，美国国会通过的一项拨款法案规定“未经联邦调查局或相应机构许可，国家航空航天局、司法部、商务部、国家科学基金会等部门不得购买与中国相关

① The United States Chamber of Commerce, “2019 Report to Congress of the U. S.-China Economic and Security Review Commission,” October 29, 2010, http://origin.www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf.

② Hillary Clinton, “Speech on Shades of hypocrisy on internet freedom,” *Guardian*, February 15, 2011, https://www.theguardian.com/world/2011/feb/15/hillary-clinton-internet-freedom.

③ 2010 年 3 月 23 日外交部发言人秦刚记者会就谷歌事件的表态，参见 http://news.cntv.cn/china/20100323/103931.shtml。

④ 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,” October 8, 2012, http://intelligence. house. gov/press-release/investigative-report-us-national-security-issues-posed-chinese-telecommunications.

的企业生产、制造、或组装的信息技术设备”①。而中国工业和信息化部也表示担忧关键信息基础设施过于依赖国外产品，需要重视发展自主知识产权及本土信息技术产品，并提出未来信息基础设施建设要以本土企业和产品为主导。②

2013 年 2 月，美国网络安全公司曼迪昂特发布报告，称一个来自中国的黑客机构多年来持续针对美国一百多家企业发起网络入侵和窃密行动，并推断中国军方参与了这些行动。③随即，美国国家安全事务助理汤姆·多尼隆在亚洲协会发表演讲，指出“网络安全问题增加了中美经贸领域发生摩擦的几率，已经成为两国经济关系日益严重的挑战”④。2014 年 5 月 19 日，美国司法部以网络窃密为由起诉 5 名中国军官，中方认为美国此举“严重违反国际关系基本准则，损害中美合作与互信”，敦促美方立撤销起诉。⑤逐步升级的网络安全争端开始全面冲击包括经贸关系在内的中美关系。

2013 年 6 月，前美国中央情报雇员爱德华·斯诺登揭露美国情报机构长期、系统性地监控和入侵全球互联网和电信系统，其中就包括了美国国家安全局对中国互联网主干网络、重要结构和企业进行入侵的内容。美国政府力图将基于国家安全的网络入侵和基于商业获利的网络窃密进行区分，认为前者等同于国际关系中的情报活动，绝大多数国家都从事类似活动，具有国际合法性，而后者破坏了国际贸易的公平原则，应当被禁止。⑥美国以意图区别对待网络攻击行为，显然不能令国际社会信服，其动机则是要尽量降低该事件对美国企业在国际市场上的负面影响。

---

① U.S. Congressional Budget Office, “H.R. 933, the Consolidated and Continuing Appropriations Act of 2013,” March 20, 2013, https://www.cbo.gov/publication/44015.

② 苗圩：《我国互联网行业的发展与管理》，2012 年 11 月 22 日，http://www.miit.gov.cn/n11293472/n11294464/n14835886/15025545.html。

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

④ Tom Donilon, “The United States and the Asia-Pacific in 2013,” March 11, 2013, https://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

⑤ 2014 年 5 月 19 日外交部发言人秦刚就美国司法部宣布起诉 5 名中国军官的表态，参见 http://ipc.fmprc.gov.cn/chn/fyrth/t1157508.htm。

⑥ 温宪等：《美国棱镜门愈演愈烈》，载《人民日报》2013 年 6 月 14 日，第 10 版。

2015 年 9 月，中美元首达成共识，承诺两国政府均不支持、不参与以商业获益为目的的网络窃密活动，“各自国家政府均不得从事或者在知情情况下支持网络窃取知识产权，包括贸易秘密，以及其他机密商业信息，以使其企业或商业行业在竞争中处于有利地位”①。这是中美迄今关于网络安全议题重要的双边共识，为化解因网络安全而紧张的双边关系奠定了基础。值得注意的是，涉及网络安全的内容主要是关于知识产权、贸易活动和市场竞争，但在成果清单中被归为全球性挑战大类，这意味着双方都认识到商业网络窃密及更广泛的网络安全议题是全球性公共问题，需要国际社会、各国政府和中美双方协调立场，采取一致行动，共同应对全球性挑战。

在这一时期，中美两国经贸竞争态势进一步明显，网络安全争端也呈多发趋势，两国都将网络安全上升到国家安全高度，理念认知和原则立场的分歧逐渐转为政策矛盾，中美在双边关系和国际场合围绕网络安全的博弈日渐增多。但两国对于稳定中美关系仍有基本共识，通过元首会晤和建立双边对话机制，还是有效地实现了危机管控，避免网络安全争端波及更多双边关系领域。

（三）网络安全与贸易冲突阶段

至特朗普政府时期，中美全面竞争态势愈益清晰，高科技产品和服务竞争不仅在中国市场，也在美国和全球其他市场展开，美国将中美贸易逆差视为其就业、贸易和经济问题的主要根源。特朗普政府第一份国家安全战略报告明确将中国视为竞争对手，要阻止中美间实力对比继续向不利于美国方向发展，并将经济视为维系国家安全的重要因素。②在中美竞争和经济优先背景下，贸易冲突、网络安全都被纳入新国家安全战略框架下，即重振美国经济和就业、重新取得经济和军事领域绝对领先优势。

2017 年 8 月，特朗普向美国贸易代表发出备忘录，称中国通过制定法律、

---

① 外交部声明：《习近平主席对美国进行国事访问中方成果清单》，2015 年 9 月 26 日，https://www.fmprc.gov.cn/web/ziliao_674904/1179_674909/t1300767.shtml。

② U.S. White House, “A New National Security Strategy for a New Era,” December 18, 2017, https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/.

政策，采取与知识产权、创新和技术相关的行动，鼓励或要求将美国企业的技术和知识产权转让给中国企业，这些做法对美国的经济利益产生了负面影响，包括抑制美国的出口、剥夺美国公民通过创新而获得公平报酬的条件、将美国的就业机会转移给中国工人、扩大美国对中国的贸易逆差，以及破坏美国的制造业、服务业和创新。①2018 年 3 月，美国贸易代表办公室公布《对华“301 调查”报告》，认为“中国政府实施和支持对美国公司计算机网络的非法入侵和窃取，获得了知识产权、商业秘密或技术数据、谈判立场、敏感和保密的内部商业通信等机密信息，也支持了中国的科技进步、军事现代化和经济发展等战略发展目标”；“中国对其关注领域的美国公司进行网络入侵是对自由贸易的破坏”；“窃取商业机密、损害知识产权，执行网络安全审查、限制跨境数据传输、要求数据本地化、实施数据分级保护，设置成本和范围都大大超过国际标准的国家网络安全标准”。②

相较于此前中美网络安全分歧和争端，调查报告矛头指向中国多项维护网络安全的政策、法规和措施，认为这些做法不仅严重损害美国的经济和就业，还是中国整体战略的一部分，因而必须从战略层面进行应对。除了加征关税，自 2018 年 9 月起，美国先后对华为及其关联公司、海康威视、大疆等众多中国科技企业执行市场准入、政府采购、产品供货等限制或司法起诉等措施。③中国企业对美投资并购受到更加严格的限制，2018 年中国蓝色光标公司收购美国一家大数据营销公司的申请被外国投资审查委员会否决，其审查程序不透明、否决原因披露不详，以危害国家安全为由阻碍正常交易的情况更为严重。④2019 年 8 月，特朗普政府发布过渡性规定，禁止联邦机构直接购买来自华为等五家中国

① U.S. White House, “Presidential Memorandum for the United States Trade Representative,” August 14, 2017, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-united-states-trade-representative/.

② Office of the United States Trade Representative, “Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974.”

③ 2019 年 5 月 23 日外交部发言人陆慷主持例行记者会就美国政府采取对华为公司断供措施表态，https://www.fmprc.gov.cn/web/wjdt_674879/fyrbt_674889/t1665967.shtml。

④ 国务院新闻办公室：《关于中美贸易摩擦的事实与中方立场》，北京：人民出版社 2018 年版，第 48 页。

企业的通信、视频监控设备或服务。[①]特朗普执政以来，两国政府间网络安全和执法对话先后暂停或中断，双边学术交流和人员往来也大幅减少。

特朗普政府对中美关系、经济安全、网络安全等一系列重大问题上的认知产生了重大变化，却又将实现经济繁荣和就业增长的复杂过程简单化，试图运用多种极限施压手段达到令谈判对手屈服而减少贸易逆差的结果。这些方式在《美墨加协定》《美韩自由贸易协定》的谈判中一定程度上实现了预期目标。而在处理更为复杂且双方实力相对均衡的中美贸易关系和网络安全议题上，运用极限施压的手段反而促使分歧更加扩大，矛盾更加突出。

四、原因分析及其启示

中美关系中的网络安全问题很早就受到关注，两国展开各个层级对话磋商，也曾形成将网络安全合作打造成中美关系新亮点的共识。[②]而中美贸易冲突自始就蕴含着网络安全要素，这是随着网络技术和应用的发展，网络安全问题与中美关系诸多领域、多种因素相互作用的结果。

（一）原因分析

第一，网络空间发展与经济社会运行高度融合，信息技术产品、数字应用服务在国际贸易中的比重不断上升。网络技术快速发展和网络应用广泛普及，将越来越多政府部门、私营企业、社会组织和个人的活动从线下拉到线上，贸易活动也几乎是同步完成了主导空间的转移，从 20 世纪 90 年代电子商务开始兴起，到近年来数字贸易全面展开，以互联网为交易平台或以网络产品和服务为交易标的的贸易不断增长，在整个国际贸易中所占比重越来越大，促使关键信息基础设施的互联互通、网络交易平台的可互操作、贸易数据的跨境传输、

① The U.S. Securities and Exchange Commission, "Amendments to Rules for Nationally Recognized Statistical Rating Organizations," August 7, 2019, https://www.sec.gov/rules/final/2019/34-86590.pdf.

② 国平：《将网络合作打造成中美关系新亮点——习近平主席访美并出席联合国系列活动成果评述四》，光明网理论频道，2015 年 10 月 4 日。

应用系统的稳定运行等都成为构建自由、开放和公平国际贸易体系的重要目标。

2019年，世界贸易组织发布的《世界贸易数据评估》显示，由信息通信技术驱动、通过电子传输实现的服务贸易，包括保险服务、金融服务、知识产权相关交易、电信服务、计算机和信息服务等，总价值从2008年的18.55亿美元增加到2018年的29.64亿美元。其中，计算机服务在信息通信技术贸易中所占份额从65%增长至78%。数据库开发、数据处理和软件设计也受益于技术变革，如企业将其信息技术运营业务转移至云计算。①

对于中美两个首要经济大国、贸易大国和网络大国，上述变化的影响是多方面的，两国在数字贸易和网络安全领域的共同利益不断扩大，需要不断寻求利益汇合点，扩展合作空间，但受国内政治、就业形势、经济增长和竞争优势消长等因素制约，中美贸易摩擦也不可避免地逐渐增多。

第二，网络安全因素全面介入中美商品和服务、与贸易有关的知识产权、政府采购等贸易环节。作为世界贸易组织成员，中美两国都应遵循多边贸易规则和市场开放承诺，避免对对方企业在本国市场上的经营活动施加直接行政干预，也应当保护外国企业的知识产权和商业机密，与知识产权有关的贸易是美国经济运行和对外贸易的关键产业，也是美国企业竞争优势集中的领域，2018年知识产权相关贸易分别占美国出口总额的16.1%和进口总额的10.0%，因而美国非常强调知识产权的保护，甚至过于敏感并试图干预他国公共政策。在政府采购中，也需要公平对待竞标企业和产品，尽管中国没有加入《政府采购协定》，美国企业的产品和服务也并未被排除在中国政府采购市场之外。而对于涉及网络安全的产品和服务，两国都可能利用贸易规则和条款中的例外和缺失，对于规则本身的不同理解和对于利用例外条款的态度，就可能成为引发中美贸易冲突的原因。

第三，中美两国信息技术产品、数字贸易领域互补性降低，竞争面扩大。过去十余年间，中国从全球产业链的下游加速向上游移动，附加值较高的信息技术产品进出口占外贸总量的比重越来越大，在更加依赖信息技术的商业服务

① World Trade Organization, "World Trade Statistical Review 2019," https://www.wto.org/english/res_e/statis_e/wts2019_e/wts19_toc_e.htm.

方面，中国也快速成长为全球第二大商业服务贸易国。一国在国际贸易中任何一个领域所占市场份额的提升，都意味着其他国家所占份额的相应降低。中国企业在信息技术产品和数字贸易领域竞争实力的增强，不可避免会侵蚀美国企业的市场份额，从而增加贸易摩擦的可能性。

面对中国企业在高科技领域的全面追赶态势，特朗普政府指责中国长期通过以市场换技术实施强制技术转让，知识产权保护政策避实就虚，并将中美贸易存在大量逆差归咎于中国对美国企业实行歧视性政策和市场准入限制。中国政府公布《关于中美经贸摩擦的事实与中方立场》白皮书，针对美方指责逐一反驳，认为贸易不平衡是美国经济结构和现有比较优势格局下市场自主选择的自然结果，美国企业通过订立商业合同与中国企业建立伙伴关系、转让或许可其技术、共享中国市场商业回报的行为，是自愿合作行为而非强制技术转让，中国政府支持企业走出去，也绝非一种推动企业通过并购获取别国先进技术的政府行为，中国在立法、执法和司法层面不断强化知识产权保护，美方的指责有悖事实。①

第四，两国均将对外贸易限制措施作为维护网络安全的手段。面对中美贸易冲突，美国加快建设审查制度和相关法律法规，扩大监管对象和审查范围，严格对外国投资实施安全审查。近年来美国动辄以维护国家安全和网络安全为由，否决和阻止多起中国企业的海外投资和并购项目，在拨款法案中禁止联邦政府采购由中国企业提供的通信设备和服务，美国联邦政府和州政府还出台政策，对包括信息技术产品在内的多个行业提供补贴、救助和优惠贷款。

中国也出台一系列维护网络安全的政策、法规和措施，2015 年至 2017 年，中国相继通过《国家安全法》《网络安全法》和《国家情报法》，2019 年 5—6 月，中国国家互联网信息办公室发布《个人信息出境安全评估办法》《网络安全审查办法》《数据安全管理办法》征求意见稿，②这些政策和法规将保障网络安全

① 国务院新闻办公室：《关于中美贸易摩擦的事实与中方立场》，第 15—38 页。

② 国家互联网信息办公室：《关于〈个人信息出境安全评估办法（征求意见稿）〉公开征求意见的通知》，http://www.cac.gov.cn/2019-06/13/c_1124613618.htm；《关于〈数据安全管理办法（征求意见稿）〉公开征求意见的通知》，http://www.cac.gov.cn/2019-05/27/c_1124544770.htm；《关于〈网络安全审查办法（征求意见稿）〉公开征求意见的通知》，http://www.cac.gov.cn/2019-05/24/c_1124532846.htm。

确立为国家主权、安全和发展利益的核心内容，并将网络主权作为维护网络安全的基本原则，提升网络技术和应用的安全需求，建立通信网络防护、网络安全审查、等级数据保护、数据跨境转移、个人信息保护等制度规范，完善中国维护网络安全的总体布局，对于部分在华开展业务的网络运营企业和面向中国境内用户的电子商务企业而言，则是提出新的挑战，一些企业需要通过增加资金和人力投入完成合规程序，另一些企业则因无法达标或者达标成本过高而放弃相应业务。

（二）几点启示

首先，网络安全问题日益成为国际贸易中的活跃变量，与中美贸易其他冲突因素交织互动，具有很强破坏性和全局影响力。网络空间为人类活动提供场所，既是促进经济发展和社会进步、增加整体福祉的新途径，也为运用隐蔽手段干涉经济社会运行和公共政策制定提供了新机会。研究表明，无论是出口国还是进口国受到的网络攻击都对贸易具有阻碍作用，特别是对消费品贸易有显著的阻碍作用。①在世界经济论坛《2018 年全球风险报告》中，在十大最可能发生的风险中，网络攻击、数据欺诈或盗窃排第三和第四位，仅次于极端天气和自然灾害，而在影响最大的十大风险中，网络攻击排在第六位，网络安全风险在两项排名中的位置都显著上升。报告还显示，高商业价值目标面临的网络安全风险显著提高，一些受到网络攻击的企业每季度亏损高达 3 亿美元。②随着贸易活动对网络技术和应用依赖程度的不断提升，关键信息基础设施、网络交易平台、商业和用户数据以及技术专利等，都有可能成为网络攻击和网络窃密的目标。频发的跨国网络攻击除了可能造成巨大经济损失，还会加深国家之间的不信任，进而对现行国际贸易体系应对新局势的能力提出挑战。

其次，维护网络安全的贸易限制措施对中美贸易冲突产生了直接影响。在《对华“301 调查”报告》中，网络安全审查、限制跨境数据传输、要求数据本

---

① 胡冠华、李兵：《网络攻击对贸易的影响——基于网络安全公司数据的研究》，载《产业经济评论》2018 年第 5 期，第 50 页。

② World Economic Forum，“The Global Risks Report 2018，13th Edition，” January 17，2018，https://www.weforum.org/reports/the-global-risks-report-2018.

地化、实施数据分级保护、国家网络安全标准等，都涉及国家基于维护网络安全指定的政策、法规和措施，从维护保密性、完整性、可控性等网络安全目标来看，这些政策、法规和措施都存在必要性和合理性，而从贸易自由和贸易公平的角度看，又都会增加贸易成本，提高市场准入限制。事实上，主要大国都已出台上述维护网络安全的政策、法规和措施，美国的网络安全审查制度、贸易实体清单制度、国防拨款法案中的采购条款，也都是以网络安全或国家安全为由采取的贸易限制措施。2014 年 9 月，在第二届中国互联网安全大会上，小布什政府首任国土安全部长汤姆·里奇（Tom Ridge）认为，由于“还没有一个国际准则，而网络攻击则是真实存在并在不断增加，因此每个国家都在采取措施来保障和促进他们的信息安全”①。里奇道出了美国政府惯常通过单边政策工具维护网络安全的思维逻辑，正由于美国政府以网络安全为由打压和限制中国的高科技企业，促使中美贸易冲突不断复杂化。

最后，中美可就管控贸易冲突与维护网络安全的贸易政策进行协商，达成一致性的网络安全规则和贸易规则。从中美贸易冲突的演变可以看出，网络安全相关的贸易保护政策、贸易壁垒措施、贸易报复手段，一定程度上侵蚀了经贸关系作为中美关系压舱石和稳定器的作用。2018 年 2 月以后，中美高级别贸易谈判团进行了多轮贸易磋商，美方提出的要求包含停止商业网络窃密、更改网络安全立法、放弃数据本地化要求和放松跨境数据转移限制等条件。中方亦多次明确贸易谈判立场，在《关于中美经贸磋商的中方立场》白皮书中，中国重申平等、互利、诚信的磋商立场，在不作原则性让步的同时，希望与美方共同努力，相向而行，认真、切实履行承诺。②应当认识到网络安全议题的复杂性、跨国性和虚拟性，由于绝大多数网络攻击和网络入侵是黑客组织或个人所为，按中美两国国内法律都是犯罪行为，因而美方的关切也是中国面临的问题，两国职能部门应坚持对话与合作，加强技术和执法合作，应对跨国网络犯罪活动，以缓解决策部门因维护网络安全而增加贸易限制措施的压力。

---

① 汤姆·里奇：《网络攻击已成全球性的威胁与挑战》，中国日报网 2014 年 9 月 24 日，http://xf.chinadaily.com.cn/2014/0924/4622.shtml。

② 国务院新闻办公室：《关于中美经贸磋商的中方立场》，第 28 页。

五、结　　语

经贸关系长期被视为中美关系的压舱石和稳定器，随着两国经济实力和贸易结构的变化，中美贸易领域的矛盾和分歧逐渐增多，直至引发贸易冲突，由于网络安全要素渗透性强、敏感度高，与中美贸易冲突其他要素相互交织叠加，进一步推升了贸易冲突的紧张程度。网络安全并非引发中美贸易冲突的首要原因，但可能成为化解中美贸易冲突的关键钥匙，如果对网络安全问题关注不够，双方网络安全关切没有妥善解决，那么中美贸易冲突发生和延宕的几率也会大大提高。故而应从网络安全与贸易冲突的结构联系入手，首先回应各自网络安全关切，进而逐步解决引发中美贸易冲突的其他问题，“本着相互尊重、平等互利的精神，管控经贸分歧，加强经贸合作，共同推进以协调、合作、稳定为基调的中美关系，增进两国和世界人民福祉”①。

① 国务院新闻办公室：《关于中美经贸磋商的中方立场》，第 31 页。