特朗普政府《国家网络战略》：实效与理念并举[1]

耿 召

【内容提要】白宫2018年9月发布的《国家网络战略》标志着特朗普网络空间政策的成熟。特朗普政府对内注重网络新技术的研发，力推基础设施的信息化升级，确保美国数字经济的发展。在全球网络空间治理领域，特朗普政府力推既有的多利益攸关方模式成为主导治理形式，反对以国家为中心的治理方式，并在该领域继续拓展美国价值理念。此战略的出台充分表明特朗普政府的网络空间政策特点在于既重视实际效果，也强调美式价值观念的传播；在保证自身网络安全的同时，维持既有优势地位。其所带来的后果在于网络空间全球治理将会进入动荡与调整阶段。网络守成大国和新兴国家在治理理念与模式上的分野短时间内难以消弭。

【关 键 词】《国家网络战略》 特朗普政府 网络安全 网络空间治理

【作者简介】耿召，上海外国语大学国际关系与公共事务学院博士研究生，美国哥伦比亚大学政治学系联合培养博士生。

【中图分类号】D815
【文献标识码】A
【文章编号】1006-6241(2019) 01-0116-15

[1] 本文系上海外国语大学第二届导师学术引领计划“中美参与网络空间全球治理合作研究”（项目编号：2017037）阶段性研究成果，本文也得到国家留学基金委“2018年国家建设高水平大学公派研究生项目”（编号：201806900064）的资助，一并致谢。

特朗普就任美国总统以来，奉行“美国优先”的执政理念，对内推动美国经济的振兴，对外注重对美国利益的维护。特朗普政府的施政重点虽不是网络空间领域，但重视保持该领域美国既有的领导地位，强调网络空间对美国国家总体安全的重要意义，并通过出台一系列相关文件，展现其在该问题上的立场。2017 年 5 月，特朗普签署颁布《关于加强联邦政府网络与关键性基础设施网络安全》行政命令，12 月发布的《国家安全战略》，其中也涉及到了网络空间安全议题。

2018 年 5 月，美国国土安全部发布了新版《网络安全战略》，从国家总体安全的维度对此前《国家安全战略》中的网络安全部分进一步进行战略细化。而 9 月白宫发布的《国家网络战略》标志着特朗普政府的网络空间政策更为明确。它以《国家安全战略》和特朗普政府已执政 18 个月的既有进展为基础，概述了美国将如何确保美国人民继续从安全的网络空间中获益并从中反映出美国的准则，保护美国的安全并促进本国的繁荣。[1]《国家网络战略》的颁布使得特朗普政府的网络空间战略得以定型，标志着其相关政策进入到了一个新的阶段。

一、《国家网络战略》总体分析

《国家网络战略》聚焦网络基础设施建设、网络人才培养与创新、阻止网络空间恶意行为以及维护互联网自由理念，全面阐述了美国政府在网络空间的行动目标以及与私营部门和国际伙伴的协作计划，充分体现出特朗普政府在网络空间领域的行动准则。

（一）美国《国家网络战略》的主要内容

美国《国家网络战略》共分为四个部分，被称为四个支柱。第一支柱

[1] The White House, “National Cyber Strategy of United States of America,” September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, p.1.

为保护美国民众、国家以及美国人的生活方式；第二支柱是促进美国的繁荣；第三支柱即通过力量维护和平；第四支柱是提升美国的影响力。上述四个支柱是这一战略的重要目标，全面涵盖了特朗普政府对网络空间的利益关切。其中，第一和第三支柱侧重于网络空间防御，以及推动网络空间的合理秩序与安全；第二和第四支柱强调网络空间对美国国内各方面发展以及美国稳固全球领导地位的重要作用（见表1）。

表1 美国《国家网络战略》的主要内容[1]

四个支柱	细化内容
第一支柱：保护美国民众、国家和美国人的生活方式	安全的联邦网络和信息
	安全的关键基础设施
	打击网络犯罪并改善事件报告
第二支柱：促进美国的繁荣	培育充满活力且具有弹性的数字经济
	培养并保护美国的独创性
	培养优秀的网络安全员工队伍
第三支柱：通过力量维护和平	通过负责任国家行为的规范增强提升网络稳定性
	网络空间不可接受行为的属性与威慑
第四支柱：提升美国的影响力	促进开放、可相互操作、可靠且安全的互联网
	建立国际网络能力

第一支柱可以说是美国政府对网络空间发展的基本要求，即保护美国国家、民众以及生活方式，具体议题细化为包括维护联邦网络和信息安全、保障关键基础设施的安全以及打击网络犯罪改善相关事件报告三个方面，其中第一方面是这一支柱的优先目标。该战略提出除了现有的国家安全系统、国防部和情报部门以外，国土安全部也要参与到维护联邦网络与信息

[1] The White House, "National Cyber Strategy of United States of America," September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

安全的行动中来。同时，联邦政府各部门将会协调风险管理和信息技术活动，但赋予首席信息官（Chief Information Officers，CIOs）领导职责。此外，联邦行政部门会把供应链的风险管理纳入机构采购与风险管理流程中，这些要求符合行业最佳做法，以更好地确保联邦政府部署的技术安全可靠。这包括确保各部门和机构之间更好地分享信息，以提高对供应链威胁的认识；减少美国政府内部重复的供应链活动，包括建立供应链风险评估共享服务。[1] 由于美国政府的不少网络设施承包给企业等相关机构，维护这些承包商的网络安全也至关重要。未来，美国政府将在审查承包商风险管理能力、审核与承包商签订的合同、与承包商分享有关网络威胁信息等方面加强行动。[2] 战略中还提到，尤其在通信保护方面，美国必须尽快制定相关标准，保护公钥加密的安全。[3]

而在关键基础设施维护上，美国政府需要与私营部门合作，提升关键基础设施的网络安全水平。因此，行政部门需要明确自身定位，增强相关培训与演练，并根据风险等级确立优先行动，保证能源、电力、银行、通信等关键领域的网络安全。同时，通过与公私部门的合作，使其对适当的安全措施进行投资并获益。此外，在地方与联邦民主选举中，相关设施的网络安全保护也是维护美国民主价值理念的重要内容。最后，在交通运输行业，关键能源输送中的网络资源保护也十分必要。[4]

在打击网络犯罪方面，该战略也提出较为清晰的谋划。首先是改善事故报告和响应，做到及时处理网络犯罪问题。其次是电子监控和计算机犯罪法的现代化。美国政府将与国会共同修订现有的相关法规，提升针对网络犯罪的执法能力。第三，减少网络空间中的跨国犯罪组织的威胁，执法机构借助有效的法律工具对这些犯罪行为进行制裁。第四，提升对海外犯

[1] The White House, "National Cyber Strategy of United States of America," p.7.

[2] Ibid., pp.7–8.

[3] Ibid., p.8.

[4] Ibid., pp.9–10.

罪人员的认识。美国政府通过外交和其他方式，推动合法引渡行动，对犯罪分子进行制裁。最后，提升与伙伴国家合作打击刑事犯罪的执法能力，加强国际执法合作对打击网络犯罪及网络恐怖主义十分必要。[1]

支柱二即推动美国的繁荣，这是美国政府希望借助网络空间实现的新政策目标。美国作为网络空间的发源地，在全球网络空间治理中占据了十分重要的地位。特朗普就任美国总统以来，促进美国经济增长是其重要施政目标之一。因此，特朗普政府也一直希望能够利用已有的互联网优势促进美国经济的增长。在这其中，培育充满活力与弹性的数字经济便是一个关键突破口。特朗普政府着重在以下六个方面进行努力。一是激励一个具有适应能力且安全的技术市场。政府将与私营部门、民间社会在内的利益攸关方合作，促进最佳实践并制定相关战略以克服采取安全技术的市场阻碍。此外，在提高网络安全实践意识与透明度的同时，美国政府将视情况与其他国际伙伴合作，推动政府所支持的开放、且行业驱动的网络标准，以及适当采用基于风险的方式来处理网络安全挑战。[2] 二是优先创新。美国政府通过更新网络相关标准和最佳实践，防止网络生态系统的所有领域受到现有以及不断变化的威胁。[3] 三是投资下一代基础设施。基础设施建设一直是特朗普提振美国经济的重点领域，早在特朗普竞选总统时，就多次提到美国现有网络基础设施的陈旧。该战略明确提出政府会加速发展下一代电信和信息通信基础设施，借助政府的购买力刺激促进供应链的安全。美国政府会与私营部门及民间社会合作，推动 5G 技术的应用，同时与各部门合力促进人工智能与量子计算技术的研发与推广，并保证运用上述新技术初始阶段的安全。[4] 四是促进跨越边界的数据自由流动。美国一直主张数据跨边界的自由流动，这既符合美式价值观念，也有助于提升美国科技公司

[1] The White House, "National Cyber Strategy of United States of America," p.11.

[2] Ibid., p.14.

[3] Ibid., pp.14–15.

[4] Ibid., p.15.

的国际竞争力。五是维持美国在新兴技术领域的领导地位。美国政府推动网络尖端技术研发，促进网络安全相关科技创新。六是推动全周期的网络安全，这一目标在于需要强大的默认安全设置、适应性强且可升级的产品以及产品交付时内置的其他最佳实践。[1]

此外该战略指出，培养和保护美国的人才，将进一步提升美国在新兴技术中的主导地位，推动网络新技术的发展。[2] 因此，美国将在建立人才上升管道、提升美国工人受教育与培训的机会、扩大联邦网络安全人员队伍、借助行政权力奖励人才这四个方面行动。[3]

支柱三即通过力量维护和平，这再一次展现出美国网络战略的基本考量。一方面，美国将通过规范负责任国家的行为提高网络稳定性。特朗普政府提出，需要鼓励遵守网络规范的行为，并通过多边论坛形式进行协商讨论，从而建立起具有普遍共识的原则。另一方面，美国会对自身及伙伴国家受到危害且不可接受的网络行为进行遏制与威慑，与伙伴国家一道制定相应战略以阻止恶意网络活动，这囊括外交、信息、军事、金融、情报等多个方面，并在打击恶意网络活动中发挥领导作用。同时，美国将与其他伙伴建立国际网络威慑倡议，制定更加细致的政策使恶意网络行为的后果予以明确。[4]

提升美国的影响力成为这一战略的第四支柱，这再一次表明美国在希望保证互联网长期开放性、相互操作性，安全性和可靠性的同时，自身的利益需要得到绝对保证。该战略明确提出，要阻止所谓的专制国家把互联网开放当作威胁。所附的行动计划阐明需要做到以下 5 点，第一，保护并促进互联网自由；第二，与伙伴国家开展行业、学术与公民社会合作；第三，

[1] The White House, “National Cyber Strategy of United States of America,” p.15.

[2] Ibid.,p.16.

[3] Ibid.,p.17.

[4] Ibid.,p.21.

进一步推动网络空间治理多利益攸关方模式的建立；第四，推动可相互操作且可靠的通信基础设施和互联网连接；第五，在全世界促进和维护美国的创新市场。[1] 同时，特朗普把自身价值观念带入到其网络空间战略之中，不论是网络自由理念，还是多利益攸关方模式，这些均与美式价值观念有着紧密联系。对于建立国际网络能力方面，该战略提出，美国政府旨在提升自身网络能力建设，通过与盟国的合作，优化其现有的网络综合技术与资源，增强执法能力，共同消除网络威胁。[2]

（二）美国《国家网络战略》的特质

纵观《国家网络战略》，其涵盖了特朗普政府在该领域优先发展的各类事项。笔者选取一些相关关键词进行词频统计（见表 2）。

表 2《国家网络战略》重要关键词统计 [3]

关键词	出现次数
网络安全（Cybersecurity）	64 次
创新（Innovation）	20 次
关键基础设施（Critical Infrastructure）	14 次
网络犯罪（Cybercrime）	12 次
执法（Law Enforcement）	8 次
独创力（Ingenuity）	6 次
数字经济（Digital Economy）	4 次
网络威慑（Cyber Deterrence）	4 次
网络攻击（Cyber Attack）	3 次

通过各关键词出现的频次可以看出，首先“网络安全”出现频率最高，此报告基本可以看作是一份增强美国网络空间安全的重要文件。其次是“创

[1] The White House, “National Cyber Strategy of United States of America,” pp.25–26.

[2] Ibid., p.26.

[3] 笔者依据美国《国家网络战略》统计制作。

新”和“独创力”，共出现 26 次，可见特朗普政府欲推动美国继续在人工智能、量子技术等网络科技前沿领域继续保持国际领先地位。此外，“关键基础设施”出现了 10 次以上，“数字经济”也出现了 4 次，这再次凸显了特朗普在 2016 年总统竞选时就已强调的美国各类基础设施的更新不仅有利于拉动国内经济，也会进一步保障国家安全。特朗普上任后签署的第一个网络空间建设的行政命令，就是关于互联网关键基础设施建设的，相关基础设施的更新和维护可以说是特朗普政府保证国家总体安全、推动网络前沿科技研发以及增强自身全球网络空间领导力的重要基础。另外，“网络犯罪”和“执法”两个关键词各出现 12 次和 8 次，可见打击网络犯罪也得到特朗普的极大重视，现有层出不穷的网络犯罪行为乃至网络恐怖主义势力的抬头极大影响美国社会的稳定，损害民众个人信息安全与利益，也对联邦整体网络空间架构带来严重威胁。在该战略中，特朗普政府提出了不仅要更新相关法律规范，提升既有的执法能力，还要增强国际合作，促进多边执法力量的协同合作。上述行动目标与国土安全部更新的《网络安全战略》具有传承性与一致性。[1] 虽然，“网络威慑”与“网络攻击”出现的次数不多，但这体现出攻击与威慑在特朗普政府网络空间战略中逐步受到重视。

总体而言，美国各界对该战略的普遍共识在于其在很大程度上是现有政策的延续。前美国国务院网络协调员克里斯·施特尔（Chris Painter）认为，该战略表明美国政策的连续性。但也有评论认为，这一战略的主要缺点是缺乏细节。其作为政府将采取的长期行动清单，几乎没有说明哪个组织将在哪个优先领域、实现目标的时间点或任何其他指标上起带头作用，或者任何其他可以让政府负责任的指标。[2] 民主党人表示他们很高兴政府推出这

[1] 美国国土安全部发布的《网络安全战略》详见：“DHS Cybersecurity Strategy Fact Sheet,” Homeland Security, May 15, 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Fact-Sheet.pdf.

[2] Guest Blogger for Net Politics, “The White House National Cyber Strategy: Continuity with a Hint of Hyperbole,” Council on Foreign Relations, October 8, 2018, https://www.cfr.org/blog/white-house-national-cyber-strategy-continuity-hint-hyperbole.

一战略，但批评白宫没有提供关于如何实施该战略的具体细节。联邦情报委员会民主党资深参议员马克·华纳（Mark R. Warner）在一份声明中认为，《国家网络战略》列出了一些重要和已确立的网络优先事项，政府现在必须超越模糊的政策提案，并为实现这些目标采取具体行动。[1]

二、从《国家网络战略》看特朗普政府网络空间政策的走向

《国家网络战略》的颁布标志着特朗普的网络空间政策基本成熟，在其剩余任期内，美国将会按照该战略进一步增强本国网络空间防御建设，提升其在网络空间全球治理中的作用。不论是在网络实践，还是意识形态领域，特朗普均强调美国需要加强并巩固其主导地位。

（一）力图维护既有的多利益攸关方模式

在该战略中，特朗普明确表示，美国将继续积极参与全球网络空间治理，确保多利益攸关方模式，阻止试图建立以国家为中心的治理框架。这种框架会破坏开放和自由、阻碍创新，并危及互联网的功能。互联网治理多利益相关者模式的特点在于透明性与自下而上性，是一个共识驱动的过程。这会使政府、私营部门、民间社会、学术界和技术领域的人员平等参与。特朗普政府将通过积极参与互联网名称与数字地址分配机构（ICANN）、互联网治理论坛（IGF）、联合国和国际电信联盟（ITU）等关键组织，在多边和国际论坛上捍卫互联网开放及共同使用的属性[2]，通过与外国合作伙伴以及其他利益攸关方（包括民间社会和私营部门）合作，推动最佳实践和政策，以提升创新、开放和效率，从而使这一模式能够保护网络空间成为数字经

[1] Derek Hawkins, "The Cybersecurity 202: Trump Administration Seeks to Project Tougher Stance in Cyberspace with New Strategy".

[2] The White House, "National Cyber Strategy of United States of America," p.25.

济充满活力的引擎。[1] 既有的多利益攸关方模式很大程度上是在美国的主导下发展起来，但伴随网络新兴国家的群体性崛起，多利益攸关方模式正面临变革的威胁。新兴国家作为互联网世界中的后来者，其中不少国家基于自身不同于西方的政治制度，某种程度上受到西方世界的网络渗透与干预。因而，为了自身政权与国家的总体稳定和安全，政府在其国内网络治理中发挥主导作用，网络私有化属性被降低。伴随新兴国家总体实力的提升，在网络空间全球治理领域日益挑战西方传统国家的既有地位。双方力量上的竞争某种程度上源于各自对治理模式的不同理解。美国作为多利益攸关方模式的支持者，与私营和非营利机构均认为，如果要制定以国家为主导的多边治理模式，会阻碍互联网自由与创新。多边模式使得具有不同民主价值观的国家在互联网治理中拥有更大的发言权，从而更广泛地引入不民主的审查工具和国家网络主权。赋予这些国家全球互联网治理决策权可能会导致违反互联网建立时所确立的基本原则。[2] 但对支持政府主导网络空间治理的国家而言，其作为相对弱势一方，网络主权与网络审查的目的在于维护自身安全，但西方国家认为这是反对网络民主自由的托词。因而，双方的核心分歧还是源于对已有认知的差异。总之，这一战略再次表明了美国对既有网络空间治理模式的支持，同时这也反映出未来网络空间治理各方分歧的化解将是一个长期过程。

（二）坚持网络空间民主自由价值理念

维护网络民主自由是特朗普政府网络空间政策的重要指导思想。该战略明确表示，美国政府将网络自由概念化为在线行使人权和基本自由，譬如言

[1] U.S. Department of State, "Release of the 2018 National Cyber Strategy," September 20, 2018, https://www.state.gov/r/pa/prs/ps/2018/09/286093.htm.

[2]Ted Piccone, "Democracy and Cybersecurity Democracy and Security Dialogue Policy Brief Series," Brookings, September 2017, https://www.brookings.edu/wp-content/uploads/2017/08/fp_20170905_democracy_cyber_security.pdf, p.4.

论自由、结社自由、和平集会自由、宗教或信仰自由和在线隐私权等，且不受边界或媒介的约束。[1] 互联网自由是《国家网络战略》的核心原则，美国国务院通过一系列双边和多边参与以及通过对外援助计划实施这一原则。它包括通过自由在线联盟（Freedom Online Coalition）来参与，这是一个由 30 个国家政府组成的团体，致力于通过与民间社会、私营部门和其他利益攸关方的多边外交和多利益攸关方合作来推进互联网自由。国务院的工作重点还在于提升双向关注政府可能采取的限制互联网访问或抑制言论自由的行为，并敦促美国的互联网公司尊重人权，执行《联合国商业和健康指导原则》。美国为技术开发、数字安全、政策倡导和研究提供支持。自 2008 年以来，国务院提供了超过 1.65 亿美元的外国援助，以支持互联网自由计划。[2]

从上述行动能够看出，既有共识的达成决定规范与准则的制定。重利益、讲求实效是特朗普施政的重要特质，但这并不意味着其对网络自由、网络民主这些美国最早赋予互联网相关价值理念的轻视。特朗普作为美国国内保守势力的代表，美式传统价值观念在其心中是根深蒂固的。在美国看来，网络空间是美国人创造出来的虚拟空间，民主自由的普世价值自然而然成为指导其发展的核心理念。根植于不同的国内环境，网络新兴国家普遍需要政府在国内网络治理领域发挥主导作用。政府在推进本国互联网建设的同时，提升其在全球网络空间治理中的参与度。基于国内政治社会环境的现实情况，政府希望通过对网络空间进行管理以求得国内秩序的安定。可以说这只是一种国内治理的方式手段，并不需要进行孰优孰劣的价值判断。当前，中国、俄罗斯、印度等网络新兴大国呈现群体性崛起态势。不同于西方国家，新兴网络大国的深度参与使得既有网络空间治理理念与运作模式产生一定的变化。但这一战略表明，美国认为上述行为违背了网络自由原则。在美国看来，正是西方民主自由理念才能够孕育出互联网技术，民

[1] The White House, “National Cyber Strategy of United States of America,” p.24.

[2] U.S. Department of State, “Release of the 2018 National Cyber Strategy”.

主自由的价值理念与网络空间紧密相关。因此，在该战略中特朗普政府明确表示，反对以国家安全为借口的数据本地化与数据保护主义。另外美国强调，对人权的保护同样适用于网络空间，民主国家共同体应该保护和促进现有的人权法律和机制，并坚持不懈地维护在线的个人权利。[1] 因而，这种理念与认知之争未来将会继续影响网络空间全球治理的走向。

此外，该战略也提到中国、俄罗斯和朝鲜对美国所谓的网络干预，这也是特朗普政府继续强调网络自由民主理念的重要原因之一。虽然就特朗普本人而言，人权与民主价值观念并非其关注的焦点，但他也深知这些价值理念对于美国在网络空间领域塑造领导地位至关重要。因而在促进互联网自由层面，特朗普政府延续了小布什和奥巴马政府的政策。网络自由现已成为该战略在网络空间推进“美国影响力”目标的一部分。[2]

（三）增加对网络新技术与基础设施的投入

5G 通信技术、人工智能以及量子技术在该战略中得到了具体呈现，这也是特朗普政府今后在网络新技术领域的重要着力点。目前，中美两国持续在 5G 通讯标准的制订上展开竞争：美国电信业巨头 AT&T 和 Verizon 均宣布，在 2018 年底之前在美主要城市推出 5G 通讯服务；而中国移动、中国联通和中国电信大致在 2019 年把 5G 通讯投入商业运营。面对中国在移动通信领域标准制订与核心技术的快速发展，特朗普政府希望确保美国能够继续主导未来电信产业。同时，前沿技术的掌握也对国家安全具有举足轻重的作用。另外，基于互联网技术的特质，网络安全与海上运输安全与外太空安全紧密联系，战略报告中着重强调了这一点。该战略提及包括海上运输在内运输业网络安全的原因在于，由于 2017 年勒索软件 NotPetya 的

[1] Ted Piccone, “Democracy and Cybersecurity Democracy and Security Dialogue Policy Brief Series,” p.5.

[2] Guest Blogger for Net Politics, “The White House National Cyber Strategy: Continuity with a Hint of Hyperbole”.

攻击，严重影响了马士基（Maersk）和联邦快递（Federal Express）等运输公司的运营。[1] 同时，特朗普政府重视投入网络新技术研发的另外一个重要原因在于，其希望能在研发及相关标准的制订初期就能避免相关安全威胁，保证新技术投入应用的安全性。[2]

此外，新技术的研发与网络基础设施的更新相辅相成，均受到特朗普政府的极大重视。该战略明确指出，网络通讯技术的研发会促进全球通信基础设施与互联网连接的开放性、互相可操作性与可靠安全性，这也会提升美国在全球数字经济中的竞争地位，从而维护国家安全与商业利益。[3] 虽然关键基础设施保护的相关政策早在克林顿政府时期就已出现，小布什和奥巴马政府发布的有关报告也涉及到了这一问题，但特朗普在该战略中把关键基础设施建设保护与数字经济以及网络前沿技术结合起来，这展现出其不同的目标侧重。[4]

因此，网络新技术、基础设施的更新、数字经济三个领域密切联系，构成今后特朗普政府网络空间政策实践层面的核心要素。同时，这也事关美国所推崇的治理模式与意识形态能否继续主导全球网络空间。

（四）借助网络威慑加强防御

网络威慑此次出现在这一战略中，其内涵较为广泛。从微观层面看，它既包括关键基础设施，也包含一系列经济与法律措施。[5] 具体而言，打击

[1] Eduard Kovacs, "Industry Reactions to New National Cyber Strategy," Security Week, September 24, 2018, https://www.securityweek.com/industry-reactions-new-national-cyber-strategy.

[2] The White House, "National Cyber Strategy of United States of America," p.15.

[3]]Ibid., p.25.

[4] 有关克林顿至奥巴马政府时期关键基础设施保护的政策信息详见：Markus Hesse and Marcus Hornung, "Space as a Critical Infrastructure," in Kai-Uwe Schrogl, Peter L. Hays, Jana Robinson, Denis Moura and Christina Giannopapa ed., *Handbook of Space Security Policies, Applications and Programs,* New York: Springer, 2015, pp.189-195.

[5] The White House, "National Cyber Strategy of United States of America," p.8.

网络犯罪、网络恐怖主义、经济间谍、侵害知识产权等恶意行为是采取网络威慑的具体行动。它包括通过一系列技术手段识别上述恶意行为，并通过公私部门的联合行动以及相关法律规范的修订从而更好地施行。而在宏观层面，该战略明确提出美国将发起国际网络威慑倡议，通过建立相应的联盟，制定有关战略，从而使网络恶意行为发起者知晓其行为所造成的后果。美国将与志同道合的国家合作，协调和支持彼此对网络重大恶意事件的反应，包括通过情报分享、支持归属主张、公开声明支持采取回应行动，以及对恶意行为者共同施加压力。[1] 通过与盟友的全方位合作，对美国所认定的对手形成威慑。但从战略的总体框架可以看出，网络威慑的最终目标还是在于维护自身网络空间安全与和平。

为了保障美国国家安全，特朗普在该战略中没有提及攻击性网络行动，但强调政府将使用“所有国家权力工具”来对恶意网络行为者“施加后果”。迄今为止，它包括实施制裁、发布起诉书以及“点名羞辱”那些与俄罗斯和朝鲜的网络攻击有关的人。国家安全顾问博尔顿也表示，白宫已经授权允许对对手实施进攻性的网络行动，这不是因为美国想要在网络空间进行更多的进攻性行动，而是为了创造威慑结构，向对手表明，与美国作战的成本比他们所设想的要高。但这一战略并未详细说明进攻行动的性质及重要程度，或者打算采取何种具体的恶意行为。[2]

三、结 语

《国家网络战略》的颁布充分体现出特朗普政府重视网络空间在国家整体安全中的作用，力促借助基础设施升级与新技术的研发，以保证国家网

[1] The White House, “National Cyber Strategy of United States of America,” p.21.

[2] Derek Hawkins, “The Cybersecurity 202: Trump Administration Seeks to Project Tougher Stance in Cyberspace with New Strategy”.

络空间安全和数字经济的发展。但同时，特朗普并没有抛弃前任在网络治理中的意识形态色彩。该战略进一步明确未来美国依然会保卫所谓的“网络自由”，反对政府在既有的多利益攸关方治理模式中占据更重要的地位。基于这一点，未来全球网络空间治理将会进入动荡与调整过程。此外，该战略宣称俄罗斯和朝鲜对美国进行了网络攻击，宣称中国对其开展网络经济间谍行为，并侵害了美国的知识产权。因而未来美国与中俄等网络新兴大国的博弈竞争愈发激烈。中美两国在2017年确立的4个高级别对话机制中，“执法及网络安全对话”作为其中之一在新时期中美网络安全关系中扮演了重要角色。但遗憾的是，受到2018年中美贸易争端的波及，两国关系面临较大阻碍。第二轮执法及网络安全对话至今未能举行。因而，中美现有的网络安全对话机制能否顺利运行下去尚未可知。基于两国目前对网络空间治理认知与理念的分歧，未来中美网络安全关系必将面临新的挑战，这也势必会影响到全球网络空间治理总体态势的发展。

总之，这份战略清晰阐明了特朗普政府的网络空间政策走向，其网络战略政策并不有利于未来美国与网络新兴国家的协商与合作。网络守成大国与新兴国家之间的博弈也将会影响各类非国家行为体与主权国家关系的发展。网络空间全球治理将会进入一个改革与保守、演进与徘徊交织的时期。

【收稿日期：2018-12-05】