中国矿业大学学报(社会科学版)
Journal of China University of Mining & Technology(Social Sciences)
ISSN 1009-105X,CN 32-1593/C

《中国矿业大学学报(社会科学版)》网络首发论文

题目：　拜登政府网络安全战略的调整与中国应对
作者：　邢瑞利
网络首发日期：　2021-09-15
引用格式：　邢瑞利．拜登政府网络安全战略的调整与中国应对．中国矿业大学学报(社会科学版)**.** https://kns.cnki.net/kcms/detail/32.1593.c.20210914.1743.002.html

网络首发时间：2021-09-15 11:07:55
网络首发地址：https://kns.cnki.net/kcms/detail/32.1593.c.20210914.1743.002.html

拜登政府网络安全战略的调整与中国应对

邢瑞利

[摘 要]拜登上台执政后高度重视网络安全问题，美国网络安全战略呈现出一系列的调整与最新动向。调整网络安全的人员和机构设置、加大对网络安全的资金投入和人才培养力度、重振与盟友及伙伴国的协同合作关系、强化与私营部门及公民社会的伙伴关系等构成了拜登政府网络安全战略的四个重要着力点。拜登政府调整网络安全战略可能加剧中美网络空间战略对峙，双方围绕数字技术、意识形态以及网络空间规则主导权的竞争将进一步升级，最终不利于中美网络空间关系的稳定。我国须及时评估拜登政府网络安全战略调整带来的消极影响，妥善应对美国对华网络安全施压及挑战，进而有效管控好中美网络空间关系。

[关键词]拜登政府；网络安全战略；网络空间；中美关系

[基金项目]国家社科基金青年项目“‘印太战略’背景下‘东盟中心地位’重构研究”（项目编号：20CGJ029）

[中图分类号]D815　　[文献标识码]A

随着互联网产业和数字技术的迅猛发展，网络空间已经被视为陆地、海洋、天空、太空之外的“第五疆域”[①]。作为互联网的发源地以及世界性网络超级大国，美国历届政府对网络安全问题非常重视并出台了一系列的网络安全战略，谋求美国在网络空间的优势地位。2020 年总统大选后，“太阳风”事件的发生暴露出美国在预防及应对网络安全风险方面存在的缺陷，特朗普政府也因在网络安全方面发表一系列不当言论及作出错误决定而受到广泛批评。在此背景下，约瑟夫·拜登（Joseph Biden）于 2021 年 1 月 20 日正式就任新一届美国总统后，究竟如何调整美国的网络安全战略也就成为国际社会备受关注的焦点问题。鉴于网络安全议题在中美关系中占据重要位置，而拜登政府网络安全战略的施政重点与政策动向也将在很大程度上影响中美网络空间关系的走向，因此，本文尝试探究拜登政府网络安全战略调整的背景及新动向，在此基础上分析其对中美网络空间关系产生的影响，为中国及时采取相关应对之策提供参考借鉴。

一、拜登政府网络安全战略调整的背景

拜登上台执政后高度重视网络安全问题并对美国网络安全战略逐步做出调

[①] A’ndre Gonawela and Ryan Rosenthal, “The long game: Why the US must rethink its cyber strategy”, The Hill, https://thehill.com/opinion/cybersecurity/534257-the-long-game-why-the-us-must-rethink-its-cyber-strategy, 2021 年 1 月 14 日。

整，这主要源于美国面临着复杂的国际和国内背景。从国际背景看，网络空间大国战略竞争加剧、加强网络防御能力以及维护美国网络霸权地位等构成了拜登政府网络安全战略调整的重要国际驱动因素。从国内背景看，拜登政府调整网络安全战略主要在于纾缓“太阳风”事件后来自美国国内社会各界的压力。

（一）国际背景

拜登政府网络安全战略的调整根本上源于全球网络空间大国日趋激烈的战略竞争与博弈。在人类社会迅速从信息化、数字化迈向智能化时代的过程中，网络空间在大国战略竞争与博弈中的地位明显得到提升，成为大国进行地缘政治博弈的新舞台。新冠肺炎疫情暴发后，美国操纵疫情问题政治化并将之与网络空间大国战略竞争挂钩，美国、中国、俄罗斯等国在网络空间的战略冲突与对抗态势更趋白热化。2020 年 5 月，美国网络空间日光浴委员会在发布的一份有关新冠疫情的白皮书中就指出，“新冠疫情与网络安全问题都是美国面临的全球性威胁，由于中国与俄罗斯等国正在利用新冠大流行而肆意攻击美国政府及私营部门的网络系统，美国亟需采取全政府手段进行应对”[①]。在网络空间日光浴委员会的建议下，2021 年 3 月，美国公布的《临时国家安全战略方针》将中国与俄罗斯定位成“头号战略竞争对手”与“次要挑战”[②]。根据这一定位，拜登政府将大国战略竞争与博弈引入到网络安全领域，把应对来自中俄的网络威胁作为美国网络安全战略的重要目标。2021 年 2 月 4 日，拜登在美国国务院发表上任后首次重要外交政策演说时明确宣称：“我以一种与前任总统截然不同的方式向普京总统表明，美国面对俄罗斯的挑衅、干涉选举、网络攻击和毒害公民等激进行径却毫无作为的日子已经结束。”[③]随后，2021 年 2 月 19 日，拜登还出席七国集团峰会和慕尼黑安全政策会议两场国际性会议，呼吁民主国家携手应对中国与俄罗斯等“独裁国家”的威胁，这向国际社会释放了重要信号[④]。显然，拜登政府网络安全战略的调整是在大国战略竞争这一语境下展开，已经打上了大国传统地缘政治博弈的烙印。

---

① Cyberspace Solarium Commission, “Cybersecurity Lessons from the Pandemic”, https://www.solarium.gov/public-communications/pandemic-white-paper, 2020 年 5 月 15 日。

② The White House, “Interim National Security Strategic Guidance”, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf, 2021 年 3 月 3 日。

③ James Andrew Lewis, “Toward a More Coercive Cyber Strategy”, Center for Strategic and International Studies, https://www.csis.org/analysis/toward-more-coercive-cyber-strategy, 2021 年 3 月 10 日。

④ “President Joe Biden signals US return to world stage”, Deutsche Welle, https://www.dw.com/en/president-joe-biden-signals-us-return-to-world-stage/a-56626997, 2021 年 2 月 19 日。

拜登政府网络安全战略的调整旨在加强网络防御能力从而维护美国在网络空间的霸权地位。随着中国、印度和俄罗斯等新兴网络空间大国的崛起，美国网络空间霸权优势在一定程度上被削弱，战略警惕和焦虑情绪随之产生。在此情形下，加强网络防御能力以维护美国在网络空间的霸权地位构成了拜登政府网络安全战略的重要目标。一方面，拜登政府认为提升美国网络防御能力的前提是要加大对外来网络攻击的制裁力度。2021 年 3 月 29 日，拜登政府宣布延长奥巴马政府于 2015 年签署的网络攻击制裁行政命令，规定在美国处于由境外人员“重大恶意网络活动”造成的紧急状态的情况下，政府有权对发起或参与重大网络攻击和网络犯罪的个人或组织机构实施制裁[①]。随后，拜登于 2021 年 4 月 15 日正式签署了对俄罗斯实行新制裁的行政命令，禁止美国金融机构参与以卢布或非卢布计价的俄罗斯主权债券一级市场。同时，还将制裁俄罗斯 32 家实体和个人，理由是其在俄罗斯政府指示下试图影响 2020 年美国总统选举，并且存在虚假信息和干预行为[②]。另一方面，拜登政府试图在网络进攻与防御之间寻求新的平衡从而更好地维护美国的网络空间霸权。例如，美国新任国防部长劳埃德·奥斯丁（Lloyd Austin）在参议院军事委员会提名听证会上透露，国防部将致力于以“前置防御”的网络安全理念挫败来自俄罗斯和中国的威胁。他认为国防部可以通过三种方式进行“前置防御”：深入了解竞争对手的网络行动和能力；推动部门间、行业和国际伙伴的合作以建立更好的网络防御体系；在必要时采取行动扰乱并阻止竞争对手的网络恶意行为[③]。当然，拜登政府并不会单纯采取防御行动来规避网络空间风险，正在考虑制定一套新的更具强制性且有效的网络空间战略。

（二）国内背景

“太阳风”（SolarWinds）事件的发生将美国网络安全问题提升到前所未有的高度，拜登政府迫于国内各界压力不得不及时作出调整与应对。“太阳风”事件属于一种高度复杂的“供应链攻击”，黑客利用“太阳风”软件的系统漏洞先后对美国微软公司、联邦政府机构、私营企业、非营利组织在内的约 1.8 万名客

① Eduard Kovacs, “Biden Extends Executive Order on Cyberattack Sanctions”, Security Week, https://www.securityweek.com/biden-extends-executive-order-cyberattack-sanctions, 2021 年 3 月 30 日。
② The White House, “FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government”, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/, 2021 年 4 月 15 日。
③ Lauren C. Williams, “Austin tackles cyber and social policy in nomination hearing”, Federal Computer Week, https://fcw.com/articles/2021/01/20/austin-dod-senate-hearing.aspx, 2021 年 1 月 20 日。

户进行攻击，对美国网络安全造成了大规模破坏[①]。2020 年 12 月 13 日，“太阳风”事件被披露后，美国国家安全委员会于次日立即启动第 41 号总统政策指令并召开网信安全事件应急响应小组会议，成立了由联邦调查局（FBI）、中央情报局（CIA）和国家情报总局办公室（ODNI）共同组成的网络统一协调小组（UCG）围绕该事件展开调查。尽管如此，“太阳风”事件依然暴露出美国在预防应对网络安全风险方面存在的缺陷，也对拜登政府尽快出台新的网络安全战略造成了不小的压力。

一是“太阳风”事件引发了美国学术界和战略界对网络安全问题的担忧。尽管美国拥有世界上最先进的情报搜集和进攻性网络能力，但鉴于其极度依赖数字通信，加之网络空间威胁具有牵一发而动全身的脆弱性，这也导致美国成为最容易遭受网络攻击的目标对象。“太阳风”事件的发生将美国在网络安全态势感知、情报预警及应急处置、政府与企业各部门间协同能力等方面存在的漏洞暴露无遗，也为美国重塑网络安全机制敲响了警钟。卡内基国际和平基金会核政策项目和网络政策倡议高级研究员阿里尔·莱维特（Ariel Levite）认为，“太阳风”事件给美国带来了 7 个深刻的教训：发动此次网络攻击的国家是俄罗斯；该事件对网络攻击的性质界定提出了挑战；网络空间的不法行为几乎不会受到惩罚；美国面临永久性的网络安全漏洞；美国“持续参与”网络空间战略的风险很大程度上被忽视；美国已经丧失在网络空间的主导地位；建立更具韧性的网络应对措施至关重要[②]。美国战略与国际问题研究中心高级副总裁詹姆斯·安德鲁·刘易斯（James Andrew Lewis）也强调，美国的网络安全战略存在不连贯性，对自身实力和军事优势的过度自信使美国对网络安全威胁缺乏及时且有效的应对。拜登政府亟需扭转在网络安全领域的守势地位，新的网络安全战略需聚焦管控风险、信号传递和联盟体系构建等三个方面，使美国能够在网络空间采取果断行动的同时尽量减少网络威慑升级的风险[③]。

二是“太阳风”事件致使特朗普政府时期推行的网络安全战略倍受质疑与批

[①] Caitlin Chin, “After the SolarWinds hack, the Biden administration must address Russian cybersecurity threats”, The Brookings Institution, https://www.brookings.edu/blog/techtank/2021/01/11/after-the-solarwinds-hack-the-biden-administration-must-address-russian-cybersecurity-threats/, 2021 年 1 月 11 日。

[②] Ariel Levite, “America must bolster cybersecurity”, The Hill, https://thehill.com/opinion/cybersecurity/533763-america-must-bolster-cybersecurity, 2021 年 1 月 12 日。

[③] James Andrew Lewis, “Can We Compete in Cyberspace?”, Center for Strategic and International Studies, https://www.csis.org/analysis/can-we-compete-cyberspace, 2020 年 11 月 2 日。

判。在特朗普政府时期，美国联邦通信委员会（FCC）在巨大的争议下废除了宽带隐私性与网络中立性等两项重要互联网原则。特朗普政府淡化联邦通信委员会对国家安全和公共安全责任的举动导致联邦通信委员会“太阳风”事件发生后并未能及时采取紧急应对措施。与此同时，尽管特朗普政府推动联邦通信委员会将华为和中兴列为美国“国家安全威胁”并切断华为芯片供应链，但对该问题的关注并不能掩盖其未能有效应对供应链网络安全威胁的事实[①]。正如美国布鲁金斯学会研究院金凯琳（Caitlin Chin）所言，“‘太阳风’事件是促使美国战略界及学界反思特朗普政府网络安全战略错误做法的催化剂，也迫使拜登政府在这一问题上作出新的改变”[②]。事实上，“太阳风”事件发生后，拜登及其执政团队也围绕网络安全问题对特朗普政府进行猛烈批判，并对该事件迅速作出强硬表态以回应美国国内社会各界关切。2020 年 12 月 22 日，拜登在特拉华州的一场活动上评论称，“特朗普在执政四年期间未能将网络安全议题摆在优先位置，网络安全事实上是美国面临的最严重威胁之一，应将这一问题与使用其他非常规武器发动的攻击同等对待”[③]。与此同时，针对特朗普政府网络安全战略存在的问题，拜登及其执政团队提出改进举措，“美国新政府会把网络安全议题作为重中之重，进一步加强与私营部门的伙伴关系，并扩大美国对防御恶意网络攻击所需的基础设施与人员投资。此外，将通过与盟友及伙伴国进行协调以阻止竞争对手发动重大网络攻击”[④]。

三是“太阳风”事件迫使拜登政府出台新的网络安全战略以回应国内呼声。关于“太阳风”事件的性质，美国国内社会各界存在定义为“网络战争行为”还是“网络间谍行为”的分歧，但目前持强硬观点的一派明显占上风。持强硬观点的一派认为，“太阳风”事件是网络战争行为，呼吁拜登政府采取强势应对举措。

---

① Tom Wheeler, “Protecting the cybersecurity of America’s networks”, The Brookings Institution, https://www.brookings.edu/blog/techtank/2021/02/11/protecting-the-cybersecurity-of-americas-networks/, 2021 年 1 月 11 日。

② Caitlin Chin, “After the SolarWinds hack, the Biden administration must address Russian cybersecurity threats”, The Brookings Institution, https://www.brookings.edu/blog/techtank/2021/01/11/after-the-solarwinds-hack-the-biden-administration-must-address-russian-cybersecurity-threats/, 2021 年 1 月 11 日。

③ Jordan Fabian and Jennifer Epstein, “Biden Says Hack of U.S. Shows Trump Failed at Cybersecurity”, Bloomberg, https://www.bloombergquint.com/politics/biden-says-hack-of-u-s-shows-trump-failed-at-cyber-security, 2020 年 12 月 23 日。

④ Sonam Sheth and Jake Lahut, “Biden says he will ‘not stand idly by’ on the massive US cyberattack that Trump hasn’t bothered to address yet”, Business Insider, https://www.businessinsider.com/biden-statement-solarwinds-cyberattack-trump-russia-2020-12, 2020 年 12 月 18 日。

美国联邦参议员理查德·德宾（Richard Durbin）就声称，俄罗斯发动的这场攻击实际上等于在网络空间向美国发出了正式“宣战”[①]。美国众议院国土安全委员会资深委员、众议员约翰·卡特科（John Katko）也强烈敦促拜登总统尽快提名网络安全和基础设施安全局局长人选。卡特科认为，“美国现在比以往任何时候都更需要由永久的政治领导来领导美国的主要联邦网络安全机构”[②]。在此情形下，2020 年 12 月 17 日，拜登在当选总统后发表的一份声明中回应称，“处理网络漏洞是执政后的首要任务，将进一步加强与私营部门的伙伴关系，并扩大抵御恶意网络攻击所需的基础设施和人员方面的投资。为了遏制恶意网络攻击行为，美国会加强与盟友及伙伴的协调并对那些要为此负责的个人征收巨额费用”[③]。随后，拜登政府在 2021 年 3 月 3 日发布的《临时国家安全战略方针》中明确指出，将网络安全议题视为新政府的当务之急，提升美国在网络空间的能力、准备和应变能力[④]。此外，拜登政府还于 2021 年 5 月 12 日签署了一项行政命令，提出采取多项行动加强美国网络安全能力，解决美国当前易受黑客攻击的问题。这些行动举措主要包括：消除政府与私营部门之间的信息共享障碍；推动联邦政府网络安全现代化；确保软件尤其是关键软件的供应链安全；成立网络安全审查委员会等[⑤]。

二、拜登政府网络安全战略调整的新动向及特点

拜登上台执政后将网络安全问题列为政府重要议程，美国网络安全战略的调整已经初步呈现出基本轮廓。通过分析拜登政府发布的一系列政策文件以及公开讲话可以发现，调整网络安全的人员和机构设置、加大对网络安全的资金投入和人才培养力度、重振与盟友及伙伴国的协同合作关系、强化与私营部门及公民社

[①] Claude Barfield, “The SolarWinds hack: America, the helpless Gulliver?”, American Enterprise Institute, https://www.aei.org/technology-and-innovation/the-solarwinds-hack-america-the-helpless-gulliver/, 2021 年 1 月 14 日。

[②] Maggie Miller, “Microsoft breach ramps up pressure on Biden to tackle cyber vulnerabilities”, The Hill, https://thehill.com/policy/cybersecurity/543535-microsoft-breach-ramps-up-pressure-on-biden-to-tackle-cyber, 2021 年 3 月 17 日。

[③] Sonam Sheth and Jake Lahut, “Biden says he will ‘not stand idly by’ on the massive US cyberattack that Trump hasn’t bothered to address yet”, Business Insider, https://www.businessinsider.com/biden-statement-solarwinds-cyberattack-trump-russia-2020-12, 2020 年 12 月 18 日。

[④] The White House, “Interim National Security Strategic Guidance”, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf, 2021 年 3 月 3 日。

[⑤] The White House, “Executive Order on Improving the Nation’s Cybersecurity”, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, 2021 年 5 月 12 日。

会的伙伴关系等是拜登政府调整美国网络安全战略的重要着力点。

（一）调整网络安全人员与机构设置

拜登政府着力调整网络安全的人员和机构设置，将网络安全事务提升至政府优先考虑事项。早在竞选过程中，拜登就高度重视网络安全问题，强调要防止任何外部势力干涉美国总统大选。在正式入主白宫以后，拜登着手恢复被特朗普执政时期忽视的网络安全职务，重新调整网络安全机构的人员配置，组建网络安全政策精英团队。从 2020 年 11 月拜登公布的首批内阁成员名单可以看出，其网络安全政策思路体现出鲜明的“精英治网”特征。无论是新任命的国务卿安东尼·布林肯（Anthony Blinken）、国家情报总监艾薇儿·海恩斯（Avril Haines），还是国家安全顾问杰克·苏利文（Jake Sullivan）、国土安全部长亚列山卓·马约卡斯（Alejandro Mayorkas）均具有丰富的网络安全经验。艾薇儿·海恩斯曾担任过中情局副局长以及奥巴马的首席副国家安全顾问，而亚列山卓·马约卡斯曾担任奥巴马政府时期的副国土安全部长并主导过公私部门网络威胁信息共享项目，由这些资深专业人士担任内阁关键职位将很大程度上影响拜登推行网络安全战略的思路举措。2021 年 4 月，拜登政府宣布计划任命克里斯·英格利斯（Chris Inglis）和简·伊斯特利（Jen Easterly）分别担任白宫国家网络总监（National Cyber Director）以及网络安全和基础设施安全局局长（CISA Director）[①]。值得一提的是，国家网络总监这一新职位根据美国 2021 财年《国防授权法案》设立，既是美国总统在网络安全及相关新兴技术领域的首席顾问，也是政府与私营企业的联络枢纽，旨在负责监督和协调联邦政府给出网络威胁应对方案从而达到提升美国整体网络实力的目标[②]。除了克里斯·英格利斯和简·伊斯特利，拜登政府网络安全政策精英团队成员还包括负责网络和新兴技术的副国家安全顾问安妮·纽伯格（Anne Neuberger）以及即将被提名为国土安全部政策副部长的罗布·西尔弗斯（Rob Silvers）。显然，通过人员更换与机构改革，拜登政府对一大批网络安全领域的资深专业人士予以重任，这为推进落实美国的网络安全战略提供了制

[①] Ellen Nakashima, “Biden administration plans to name former senior NSA officials to White House cyber position and head of CISA”, The Washington Post, https://www.washingtonpost.com/national-security/former-senior-nsa-officials-named-to-white-house-cyber-position-and-head-of-dhs-cyber-agency/2021/04/11/b9d408cc-9b2d-11eb-8005-bffc3a39f6d3_story.html, 2021 年 4 月 13 日。

[②] Mark Montgomery and Robert Morgus, “A Cyber Opportunity: Priorities for the First National Cyber Director”, War on the Rocks, https://warontherocks.com/2021/01/a-cyber-opportunity-priorities-for-the-first-national-cyber-director/, 2021 年 1 月 7 日。

度保障。

（二）加大网络安全资金投入与人才培养力度

拜登政府着力加大对网络安全的资金投入和人才培养力度，维护美国在网络空间的技术领先地位。在资金投入方面，拜登政府大幅提升在网络安全领域的资金投入比例，谋划设置网络安全专项资金，以此来提高网络防御能力。2021 年 1 月 14 日，拜登政府公布了一项价值 1.9 万亿美元的“美国救援计划”提案，特别呼吁国会批准联邦政府在信息技术现代化和网络安全方面的重大投资，称“除了新冠肺炎疫情，美国在网络安全方面也面临危机，这是迫在眉睫的国家安全问题，不能再等待”[①]。2021 年 3 月，该提案在美国参议院正式获得通过，这是拜登政府任内的首个重大立法项目，也是美国历史上规模最大的刺激性法案之一。“美国救援计划”法案为网络安全和基础设施安全局、美国总务管理局（GSA）拨款 90 亿美元，以推出新的网络安全和互联网技术共享服务；专门拨款 6.9 亿美元给网络安全和基础设施安全局改善联邦民用网络安全监测和事故应对，并支持新的共享安全和云计算服务试点；专门拨款 3 亿美元资助美国总务管理局的信息技术项目；为联邦首席信息安全官和美国数字服务局拨款 2 亿美元用于聘用技术专家等[②]。在人才培养方面，拜登政府重视吸引国际化人才，提升网络空间领域的科研创新能力来维护美国的全球科技领导地位。拜登认为，美国在过去的几十年之所以迅速发展成为世界领先的科技强国，一个至关重要的因素在于吸引了一大批在科学、技术、工程和数学（STEM）领域具有专业背景的国际化人才。因此，拜登上台执政之后反复重申，要加大对研发和 STEM 教育的投资以吸引国际化人才。卡内基国际和平基金会研究员埃文·伯克（Evan Burke）为拜登政府吸引网络安全人才提出了具体建议，强调在平衡经济和安全利益关系的基础上，指示美国国土安全部延长 F、I 和 J 类签证年限，重审导致 H-1B 签证拒签量大幅增加的审查程序，并与国会合作为 STEM 专业博士等高技能人才开发新的

[①] Maggie Miller, “Biden includes over $10 billion in cyber, IT funds as part of COVID-19 relief proposal”, The Hill, https://thehill.com/policy/cybersecurity/534323-biden-includes-over-10-billion-in-cyber-it-funds-as-part-of-covid-19, 2021 年 1 月 14 日。

[②] The White House, “President Biden Announces American Rescue Plan”, https://www.whitehouse.gov/briefing-room/legislation/2021/01/20/president-biden-announces-american-rescue-plan/, 2021 年 1 月 20 日。

合法永久居留途径等[①]。

（三）重振与盟友及伙伴国的网络协调合作关系

拜登政府着力重振与盟友及伙伴国的协同合作关系，确保美国对网络空间规范的制定和主导权。重新将盟友及伙伴国凝聚在一起，以修复美国在双边及多边体系的作用和领导力是拜登政府外交政策最显著的标志。为了实现这一目标，拜登政府以网络空间合作为重要抓手，与盟友及伙伴国联合改善网络安全水平并制定国际标准，以此构建起全球网络空间行为规范。2020 年 3 月，拜登在《外交事务》发表的《为何美国必须再次领导世界——拯救特朗普之后的美国外交政策》一文中就强调美国应该与盟友及伙伴国建立统一战线，塑造在知识产权、5G 网络以及人工智能等领域的规则，防止中国主导未来技术和产业的发展[②]。具体而言，一方面，拜登政府注重联合欧洲传统盟友的力量，强调在网络空间、人工智能、生物科技等领域共同制定国际规则以主导新兴技术的发展。美国大西洋理事会高级研究员富兰克林·克莱默（Franklin D. Kramer）和欧洲政策分析中心研究员劳伦·斯佩兰萨（Lauren Speranza）为拜登政府联合北约盟友实施主动且可持续的网络空间战略提出了具体建议。他们认为，拜登政府与北约盟友的网络空间合作应从三个方向展开：北约需加强网络关键基础设施建设，制定并实施一套弹性化网络安全架构；北约成员国之间应积极提升网络空间防御能力；协调推进美国国防部倡议的持续接触战略，以减少俄罗斯与中国开展削弱北约联盟团结的网络空间活动[③]。另一方面，拜登政府也重视印太地区盟友及伙伴的作用，呼吁共同应对网络威胁、供应链安全、关键技术等新兴挑战。2021 年 3 月 12 日，美国、日本、印度和澳大利亚四国领导人首次召开“四方安全对话”视频峰会，四国一致同意成立以网络安全、新冠疫苗、气候变化和关键新兴技术为重点的工作组以

[①] Evan Burke, “Trump-Era Policies Toward Chinese STEM Talent: A Need for Better Balance”, Carnegie Endowment for International Peace, https://carnegieendowment.org/2021/03/25/trump-era-policies-toward-chinese-stem-talent-need-for-better-balance-pub-84137, 2021 年 3 月 25 日。

[②] Joseph R. Biden, “Why America Must Lead Again? Rescuing U.S. Foreign Policy After Trump”, Foreign Affairs, Vol.22, No.2(March 2020), pp.71-76.

[③] Franklin D. Kramer Lauren Speranza, and Conor Rodihan, “NATO needs continuous responses in cyberspace”, Atlantic Council, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/, 2020 年 12 月 9 日。

应对共同挑战[①]。值得注意的是，尽管此次峰会会后的联合声明和会议简报均避开了直接使用“中国”的字眼，但普遍认为具有明显抗衡中国的意味。

（四）强化与私营部门及公民社会的公私伙伴关系

拜登政府着力强化与私营部门及公民社会的伙伴关系，全方位提升美国应对网络安全威胁的能力。鉴于美国大多数个人数据及关键基础设施都由私营部门把控，而私营部门又是推动互联网与移动通讯技术保持创新与活力的关键主体，因此，深化政府与私营部门在网络安全领域的合作就显得尤为重要。在实践中，美国历届政府基本都强调在网络空间治理中采用“多利益攸关方”模式，发挥非政府组织、私营部门、公民社会以及学术界等政府之外的行为体自下而上的作用，借助多方力量合力应对日益严峻的网络安全威胁，从而提升网络空间治理的创新活力、透明度和实效性[②]。拜登上台执政之后也延续了美国历届政府重视私营部门及公民社会等非政府力量的传统，民主党在 2020 年政策纲领中就特别凸显私营机构的重要性，强调美国政府应与私营部门积极开展合作，保护个人数据及关键基础设施安全[③]。2021 年 3 月 17 日，拜登政府宣布成立一个由政府和私营部门组成的“统一协调小组”，专门调查及应对最近曝光的涉及微软电子邮件应用程序的网络间谍事件[④]。美国网络和新兴技术副国家安全顾问安妮·纽伯格在一份声明中也明确表示，“拜登政府致力于与私营部门合作以更好地推动美国网络防御现代化的进程，并提高对重大网络安全事件做出快速反应的能力”[⑤]。与此同时，拜登政府于 2021 年 4 月 20 日宣布启动美国电力行业网络安全“百日计划”，这是美国网络安全和基础设施安全局、能源部等政府机构与私营部门加强公私伙伴关系合作的一次重要尝试，旨在保护美国电力行业关键基础设施的网络安全免

① John Ruwitch and Michele Kelemen, “Biden And ‘Quad’ Leaders Launch Vaccine Push, Deepen Coordination Against China”, National Public Radio, https://www.npr.org/2021/03/12/976305089/biden-and-quad-leaders-launch-vaccine-push-deepen-coordination-against-china, 2021 年 3 月 12 日。

② Roger Hurwitz, “Depleted Trust in the Cyber Commons”, Strategic Studies Quarterly, Vol.6, No.3(Fall 2012), pp.21-23.

③ The American Presidency Project, “2020 Democratic Party Platform”, https://www.presidency.ucsb.edu/documents/2020-democratic-party-platform, 2020 年 8 月 17 日。

④ Alex Marquardt and Zachary Cohen, “Biden administration expected to form task force to deal with Microsoft hack linked to China”, CNN, https://www.cnn.com/2021/03/06/politics/microsoft-hack-task-force/index.html, 2021 年 3 月 7 日。

⑤ Maggie Miller, “Biden administration convenes government, private sector groups to respond to Microsoft vulnerabilities”, The Hill, https://thehill.com/policy/cybersecurity/543605-biden-administration-convenes-government-private-sector-groups-to, 2021 年 3 月 17 日。

遭攻击[①]。美国一些与电力行业运营商合作的私营企业对拜登政府启动“百日计划”此举表示欢迎，称赞“拜登政府专注于保护美国关键基础设施的网络安全并寻求与私营部门开展对话，使各种规模的行业利益相关方都能成为政府解决方案的一部分，这令人欣慰”[②]。

三、拜登政府网络安全战略对中美关系产生的消极影响

作为世界上两个最大的互联网大国，网络空间是中美双边关系的晴雨表。中美网络空间关系稳定与否将很大程度上影响甚至决定中美双边关系的整体走向。当前，拜登政府网络安全战略的调整既是美国重塑与世界各国关系的重要步骤，也是美国对华网络安全战略的关键一环，必定对中美双边关系产生深远的影响。

首先，大国战略竞争依然是拜登政府网络安全战略的主线，这导致中美网络空间战略对峙将进一步加剧。多种迹象表明，美国政府、智库与战略界对中美网络空间关系的看法认知趋向负面，这基本框定了拜登政府对华网络安全战略的竞争基调。美国智库与战略界对中国在网络空间不断上升的影响力表现出明显的担忧，将网络安全战略的矛头直指中国。美国战略与国际研究中心繁荣与发展项目主任丹尼尔·隆德（Daniel F. Runde）和资深研究员罗米娜·班杜拉（Romina Bandura）强调，“随着全球数字技术的迅猛发展，中国正在利用‘数字威权’来扩展自身在全球地缘政治中的影响力，美国亟需对此作出回应”[③]。美国企业研究所研究员克劳德·巴菲尔德（Claude Barfield）和威廉·劳（William Rau）则认为，中国推行 5G“威权主义”对以美国为首的西方发达国家构成了严重的经济和安全威胁。在此情形下，拜登政府的首要任务是要确保美国在 5G 无线技术的推广和管理方面的领导地位[④]。鉴于这些智库多为美国民主党精英的大本营且与拜登执政团队核心成员关系密切，因此，在很大程度上推动并主导着拜登政府网络安全战略的走向。受美国智库与战略界的影响，拜登政府也致力于出台全

---

① Brian Fung, “Biden administration unveils effort to strengthen cybersecurity of power grid”, CNN, https://edition.cnn.com/2021/04/20/politics/biden-electricity-grid-cybersecurity/index.html, 2021 年 4 月 20 日。

② Maggie Miller, “Biden administration kicks off 100-day plan to shore up cybersecurity of electric grid”, The Hill, https://thehill.com/policy/cybersecurity/549188-biden-administration-kicks-off-100-day-plan-to-shore-up-cybersecurity-of, 2021 年 4 月 20 日。

③ Daniel F. Runde, Romina Bandura and Sundar R. Ramanujam, “The United States Has an Opportunity to Lead in Digital Development”, Center for Strategic and International Studies, https://www.csis.org/analysis/united-states-has-opportunity-lead-digital-development, 2021 年 3 月 30 日。

④ Claude Barfield and William Rau, “Biden’s 5G to-do list, part I”, American Enterprise Institute, https://www.aei.org/technology-and-innovation/bidens-5g-to-do-list-part-i/, 2021 年 3 月 17 日。

新的网络安全战略，强化中国等网络空间大国的战略竞争。拜登政府已经明确将中国视为挑战美国网络空间领导地位的“头号战略竞争对手”，并呼吁民主国家做好与之进行长期抗衡的准备。拜登政府认为，中国越来越多地利用经济实力从事网络间谍、知识产权盗窃以及网络商业机密窃取等活动，这对美国关键基础设施以及国家经济安全与繁荣造成了极大的威胁。针对来自中国的网络安全威胁，拜登政府试图改善网络空间防御策略，通过向竞争对手强加成本来阻止敌对网络行动，并辅助利用外交手段加强网络安全方面的合作与规范，以遏制中国在网络空间的影响力。显然，拜登政府这种消极的战略定位与行动举措将进一步加剧日趋激烈的中美网络空间竞争和冲突，也严重影响全球网络空间秩序的稳定。

其次，拜登政府基本明确了对华战略竞争的核心是数字时代话语权和主导权之争，数字技术正成为中美网络空间竞争的新焦点。鉴于网络化时代数字技术的迅猛发展，拜登上台执政以后更加强调在数字经济和科技领域展开竞争，以维护美国的全球数字霸权地位。2021 年 6 月 8 日，美国参议院表决通过的一项长达 1400 多页的对华大战略法案——《2021 美国创新与竞争法案》是拜登政府试图从技术研发体系、治理模式制度和国际联盟体系上实行“数字去中国化”战略的一个典型表现[①]。为了使美国在国际数字市场议程中占据主导地位，同时构建一个“去中国化”的全球数字市场，拜登政府频繁攻击中国的网络安全问题，试图联合盟友及伙伴的力量来达到限制中国数字产业发展的目的。具体而言：一方面，拜登政府大肆渲染中国的网络安全问题，固化国际社会对所谓“数字威权主义”的错误认知，给中国建设“数字丝绸之路”设置障碍。2021 年 7 月 19 日，美国与澳大利亚、英国、加拿大、欧盟、日本、新西兰和北约等联合发表声明，共同谴责中国存在所谓的“恶意网络活动”[②]。值得注意的是，这是拜登政府上任以来首次就中美网络安全问题发表国际声明，折射出美国在对华网络安全问题上的强硬态度。另一方面，拜登政府还试图与盟友及伙伴构筑小多边同盟，寻求遏制中国在数字产业领域的影响力。目前，拜登政府正在考虑拉拢澳大利亚、加拿大、日本、马来西亚、新加坡等国，在印太地区推出一项意图将中国排斥在外的“数

[①] Congress of the United States, “H.R.1304 - American Innovation and R&D Competitiveness Act of 2021”, https://www.congress.gov/bill/117th-congress/house-bill/1304/text, 2021 年 6 月 8 日。

[②] Zolan Kanno-Youngs and David E. Sanger, “U.S. Accuses China of Hacking Microsoft”, The New York Times, https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html, 2021 年 7 月 20 日。

字贸易协议”，以维护美国在该地区数字经济中的主导作用[①]。与此同时，2021年7月13日，美国还联合全球十多个民主国家和国际组织领导人举办全球数字峰会，与会各方承诺集结资源以协同一致方式确保在人工智能科技革命中让民主力量走在中国“威权主义”模式前面[②]。显然，拜登政府将数字时代话语权和主导权视为中美网络空间竞争的关键一环，这给中国发展数字经济带来的消极影响不容忽视。

再次，价值观及意识形态因素在拜登政府对华网络安全战略中的分量上升，中美在网络空间的意识形态竞争可能进一步升级。美国长期将网络空间视为灌输意识形态、推广西方价值观的重要工具，其实质是利用自身在网络空间的技术优势，打着“网络自由”的幌子干涉他国内政，从而牢牢掌握制网权。美国在网络空间大搞意识形态对抗充满了赤裸裸的霸权思维，即“谁掌握了信息，谁掌控了互联网，谁就拥有了整个世界”[③]。拜登上台执政以后将民主价值观和意识形态因素置于美国网络安全战略的重要位置，以所谓民主、自由、人权和开放为幌子大肆污名化中国的治网政策，在意识形态领域持续向中国施压进而使美国在网络空间主导权的争夺中占据有利地位。2021年3月，美国《临时国家安全战略方针》就渲染称，“威权主义正在全球大行其道，民主国家正在被围攻”[④]。美国国务卿安东尼·布林肯（Antony Blinken）则鼓吹网络空间竞争是“民主国家与威权主义国家之间的一场战争，威权主义国家正在对网络空间的民主造成侵蚀”[⑤]。拜登政府认为，中国作为“威权主义”国家对网络空间造成的威胁包括干涉选举、网络造谣、网络攻击和数字威权等，作为民主复兴项目的一部分，美国须

① Peter Martin, Eric Martin and Saleha Mohsin, “Biden Team Weighs Digital Trade Deal to Counter China in Asia”, Bloomberg, https://www.bloomberg.com/news/articles/2021-07-12/biden-team-weighs-digital-trade-deal-to-counter-china-in-asia, 2021年7月12日。

② Jacob Fromer and Jodi Xu Klein, “US and allies must set ‘democratic’ rules for artificial intelligence, Biden administration officials say”, South China Morning Post, https://www.scmp.com/news/china/diplomacy/article/3140997/us-and-allies-must-set-democratic-rules-artificial, 2021年7月14日。

③ 阿尔温·托夫勒、海蒂·托夫勒：《创造一个新的文明：第三次浪潮的政治》，陈峰译，上海：三联书店出版社，1996年，第31页。

④ The White House, “Interim National Security Strategic Guidance”, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf, 2021年3月3日。

⑤ Elise Labott, “Biden Wants to Compete With China. Here’s How”, Foreign Policy, https://foreignpolicy.com/2021/02/22/biden-can-compete-with-china-democratic-values/, 2021年2月22日。

重新思考民主与网络空间的关系[①]。为了增强对华网络空间意识形态竞争的有效性，拜登政府试图推动组建“西方民主国家联盟”，阻止来自中国的“网络安全威胁”。例如，美国规划建立美国为首的“技术 12 国”（T-12）集团，成员将包括法国、德国、日本、英国、澳大利亚、加拿大、韩国、芬兰、瑞典、印度、以色列，回击中国“网络主权”下的互联网治理模式，进而维护西方自由民主国家的技术领导地位[②]。总之，拜登政府将意识形态领域的冲突对抗嵌入到中美网络空间战略竞争中，对中国的治网政策发起密集攻势，这不仅加剧了中美在网络空间的意识形态对立，而且对两国关系的稳定与恢复产生了极其消极的影响。

最后，拜登政府有意重塑全球网络空间规则，这将引发中美两国愈发激烈的网络空间规则主导权之争。美国一直将建立全球网络空间的“行为规范”标榜为网络空间战略的主要目标之一[③]。与前任政府在全球范围内推行单边主义谋求以实力求和平的做法不同，拜登政府将多边主义外交和现有国际机制作为推进美国对华网络安全战略的重要工具。拜登上台执政后更加重视依托美国与现有国际制度及多边机制平台的联系，致力于推动美国与盟友及伙伴国在制定网络空间行为规范方面的主导性作用，进而达到削弱中国网络空间影响力的目的。2021 年 2 月 19 日，拜登在慕尼黑安全政策会议上就明确提出，“美国与世界其他民主国家应在网络安全和技术问题上制定‘道路规则’，形成网络空间、人工智能、生物技术等领域的行为规范，中国等国也必须遵守这些规则”[④]。具体而言，拜登政府试图与盟友及伙伴国从全球数字互联互通、保护网络隐私权、数据跨界自由流动、网络言论自由、网络开放性及互操作性等规则规定方面联合对华施压，以强化美国全球制网权优势。以全球数字互联互通为例，新美国安全中心发布一份名为《利用多边主义促进数字发展》的研究报告就建议拜登政府与联合国以及其他多边机构建立富有成效的数字伙伴关系，围绕促进全球数字互联互通加强多边

[①] David P. Fidler, “America’s Place in Cyberspace: The Biden Administration’s Cyber Strategy Takes Shape”, The Council on Foreign Relations, https://www.cfr.org/blog/americas-place-cyberspace-biden-administrations-cyber-strategy-takes-shape, 2021 年 3 月 11 日。

[②] 余南平、戢仕铭：《西方“技术联盟”组建的战略背景、目标与困境》，《现代国际关系》2021 年第 1 期。

[③] 鲁传颖：《奥巴马政府网络空间战略面临的挑战及其调整》，《现代国际关系》2014 年第 5 期。

[④] Maggie Miller, “Biden calls for creating ‘rules’ on cyber, tech to combat China and Russia threats”, The Hill, https://thehill.com/policy/cybersecurity/539598-biden-calls-for-creating-rules-on-cyber-tech-to-combat-china-and-russia, 2021 年 2 月 19 日。

协调，以共同价值观和规范为基础重塑全球数字互联互通秩序[①]。此外，拜登政府还试图推动制定网络空间国际法框架以实现美国战略目标与国家利益的最大化，如倡导将《塔林手册》制定的网络战规则作为国际法规范、支持将《网络犯罪公约》作为打击网络犯罪的国际法文本等等。显然，拜登政府此举意在增强现有网络空间国际法框架的普适性，通过反对创设新的国际公约来限制中国等国的网络安全立法。总之，拜登政府试图引导全球网络空间规则朝着对美国有利的方向发展，中美之间围绕网络空间规则制定权与主导权的斗争也将进一步复杂化。

四、中国的应对策略

从上文分析可以发现，拜登政府的网络安全战略呈现出典型的对华竞争趋势，这将导致中美网络空间战略对峙进一步加剧，网络空间规则主导权之争也会愈发激烈，不利于中美网络空间关系的稳定。中国在从网络空间大国向网络空间强国迈进的过程中，须高度重视中美关系中的网络安全问题并及时采取应对举措以规避拜登政府网络安全战略的消极影响。

第一，中国要保持足够的战略定力，需看到中美在网络安全问题上既面临失去信任和对抗的风险，但也存在合作的空间和潜力。一方面，在拜登政府继续推行对华战略竞争的背景下，中国须做好应对美国在网络安全领域发动对华攻势的各种准备，坚守中国国家安全底线，妥善化解各类风险挑战。可以发现，尽管拜登政府的网络安全战略与特朗普政府的总体目标基本一致，但实现网络安全战略目标的策略手段却呈现明显差异。拜登政府对华网络安全战略调整主要聚焦意识形态、地缘政治、多边外交和技术竞争等四根重要的支柱，这对中美网络空间关系造成的挑战显然更为严峻[②]。对此，中国须做好应对来自拜登政府对华网络安全问题施压的心理准备。另一方面，在拜登政府对华政策重新回归理性的趋势下，中国也应及时抓住机遇寻求中美两国在网络安全领域的利益契合点，引导塑造积极稳定的中美关系。由于中美两国在网络空间都存在各自特殊的利益，因而双方

[①] Kristen A. Cordell and Kristine Lee, “Harnessing Multilateralism for Digital Development”, Center for a New American Security, https://www.cnas.org/publications/commentary/harnessing-multilateralism-for-digital-development, 2021 年 1 月 12 日。

[②] David P. Fidler, “America’s Place in Cyberspace: The Biden Administration’s Cyber Strategy Takes Shape”, The Council on Foreign Relations, https://www.cfr.org/blog/americas-place-cyberspace-biden-administrations-cyber-strategy-takes-shape, 2021 年 3 月 11 日。

在网络空间战略目标、网络空间军事化、网络言论自由与审查、网民隐私、网络主权等方面必然存在根本性的认知差异和理念分歧，这些差异和分歧很大程度上阻碍了中美的网络空间合作。然而事实上，中美两国在数字经济兼容性、网络数据处理及使用、打击网络犯罪、维护网络空间安全等方面也存在诸多的共性和利益契合点，这些共性和利益契合点使得双方能够成为彼此天然的合作伙伴，以符合各自国家利益的方式达成谅解，进而塑造良好稳定的网络空间秩序[①]。基于这一判断，中国可以在求同存异的基础上从上述共性方面入手，推动中美双方在网络空间这些具体的事务性领域开展务实合作。

第二，中国可考虑推动中美双方在避免网络空间冲突与对抗问题上达成共识，恢复并建立多层次网络空间对话与合作机制。伴随着拜登政府对华网络安全战略的逐步定型，管控中美网络空间的冲突与对抗风险显然已经成为当务之急。从中美网络空间关系发展基础看，双方已经建立了诸多开展网络对话的正式和非正式平台，从中美执法及网络安全对话、中美执法合作联合联络小组等双边机制，到东盟地区论坛、国际刑警组织亚洲及南太平洋地区信息技术犯罪工作组等多边平台，推动中美网络空间合作的场所和平台事实上并不短缺。不过遗憾的是，受制于中美两国关系恶化的大背景，这些现有的双边及多边网络安全对话机制能否顺利运行存在较大的变数。基于此，中国可考虑在推动中美双边关系逐步缓和的基础上，就两国共同聚焦关注的网络安全议题进行沟通，适时恢复、建立并完善中美多层次网络空间对话与合作机制。具体而言：一方面，中国可考虑与拜登政府加强建立紧急网络事件、重大活动例行通报、双边信息共享、危机预防与应急处理等协调机制的渠道，防止因机制缺失而导致中美网络空间关系因沟通不顺畅而陷入冲突甚至对抗的困境。另一方面，中国可考虑与拜登政府推动恢复中美网络安全领域政府间一轨对话合作机制，并扩展中美政府层面与企业、智库等民间机构的一轨半对话合作机制与中美非官方渠道二轨对话合作机制。以中美政府间执法及网络安全一轨对话合作机制为例，该对话机制是习近平主席与时任美国总统特朗普于 2017 年确立的四个高级别对话机制之一，但在举行了首轮对话后因

[①] Ariel Levite and Lyu Jinghua, “Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?”, Carnegie Endowment for International Peace, https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213, 2019 年 1 月 24 日。

中美双边关系恶化而受到阻碍[①]。因此，中国可在合适契机下与拜登政府重启该对话合作机制，为中美在执法及网络安全领域的良性互动奠定基础。

第三，中国应积极加强国际合作与对话，与世界各国一道推动构建和谐稳定的网络空间新秩序。面对拜登政府在网络安全问题上的对华施压，中国应该积极与世界上其他国家充分开展对话协商，推动网络空间规则以及治理机制的建设，塑造和谐稳定的网络空间新秩序。以尊重网络主权原则为例，美国倡导所谓的“网络自由”且过分关注本国国家利益的做法显然与中国、印度、俄罗斯等世界上绝大多数国家支持的尊重网络主权原则及政府主导的网络空间治理模式相矛盾。事实上，中国与印度、俄罗斯等网络新兴大国存在共同的利益诉求，都强调尊重网络主权原则，捍卫国家网络主权的独立性以及政府主导的网络空间治理模式。基于这一共识，中国可考虑与印度、俄罗斯等网络新兴大国以及世界上广大发展中国家一道推动建立和谐稳定的网络空间新秩序。与此同时，中国也应注重提升自身在未来网络空间新秩序中的话语权，顺应网络化时代的发展潮流，倡导建立“网络空间命运共同体”，与世界各国共享安全可靠且平等尊重的网络空间秩序。早在 2015 年第二届世界互联网大会和 2016 年第三届世界互联网大会上，习近平主席先后创造性提出与世界各国共同构建网络空间命运共同体的“四项原则”、“五点主张”以及“平等尊重、创新发展、开放共享、安全有序”的十六字方针，这为推动全球网络空间治理提供了重要的理论依据与路径遵循[②]。在这一理论指导下，中国应进一步做好“网络空间命运共同体”理念的对外传播与普及工作，争取得到世界上更多国家的认可与赞同，从而促使网络空间秩序朝着更加公正合理的方向发展。

第四，中国须加强自身网络安全保障体系与能力建设，切实维护好本国网络空间安全以不变应万变。面对拜登政府在网络安全问题上的对华施压，中国归根结底还是要将自身的事情做好，全面提升中国网络空间作战与防御能力，随时应对各种危机事件或突发情况。目前，尽管中国的网络规模与网民数量居于世界首位，但事实上中国在网络空间仍处于劣势地位，从网络大国迈向网络强国依旧有很长的一段路要走。基于此，我们必须理性认识这一严峻现实，根据中国在网络空间发展的实际情况科学制定出一套具有全局性和前瞻性的网络空间大国发展

[①] 耿召：《特朗普政府〈国家网络战略〉：实效与理念并举》，《和平与发展》2019 年第 1 期。
[②] 蔡翠红：《推动构建网络空间命运共同体》，《中国社会科学报》2021 年 2 月 23 日，08 版。

战略，走出一条具有中国特色的网络强国之路。党的十九届五中全会公报明确将网络安全纳入国家安全体系和能力建设范畴，提出“要坚定维护国家政权安全、制度安全、意识形态安全，全面加强网络安全保障体系和能力建设”，这充分体现出党中央对维护中国网络空间安全问题的高度重视，对于我国实现网络空间治理体系和治理能力现代化、建设网络强国具有重要指导意义[①]。具体而言，我国加强自身网络安全保障体系与能力建设须注重以下几点：一是聚焦提升关键信息基础设施防护体系与能力建设，吸收借鉴美国、日本以及英国等国在该领域积累的经验教训，筑牢网络安全防护屏障。二是着力实现网络空间核心技术突破，在人工智能、区块链、量子计算等关键核心技术领域加大资金及人才投入，从而在网络空间掌握更大的发展自主权。三是专注提升网络空间作战能力建设，通过加强网络武器研发、改进网络作战系统以及强化网络作战模拟培训等方式，打造一支专业性强且训练有素的网络作战部队。总之，打铁还需自身硬，唯有发展壮大自身力量，中国才能随时随地妥善应对日趋复杂严峻的中美网络空间形势。

（作者：邢瑞利，南京航空航天大学马克思主义学院，
从事美国外交战略与中美关系研究）

（责任编辑：付继娟）

The Adjustments of Biden Administration’s Cybersecurity Strategy and China’s Policy Response

XING Ruili

[Abstract] When Joseph Biden became the president, he attached great importance to the issue of cybersecurity, and the US cybersecurity strategy showed a series of latest trends. The adjustments of Biden administration’s cybersecurity strategy include four aspects: adjusting the personnel and organization settings of cybersecurity, increasing the capital investment and personnel training, revitalizing the cooperative relationship with allies and partner countries, and strengthening the partnership with the private sector and civil society and so on. The adjustment of Biden administration’s cybersecurity strategy may exacerbate the confrontation between China and the United States in cyberspace strategy. The competition between the two sides around digital technology, ideology and the dominance of cyberspace

[①] 郭声琨：《建设更高水平的平安中国》，《人民日报》2020 年 12 月 2 日，06 版。

rules will further escalate, which is ultimately not conducive to the stability of Sino-US cyberspace relations. China should timely evaluate the negative impact of Biden administration's cybersecurity strategy, properly respond to the pressure and challenges from the US, and then effectively control the Sino-US cyberspace relations.

[Key words] Biden administration; cybersecurity strategy; cyberspace; Sino-US relations