保守主义思想回归与特朗普政府的网络安全战略调整*

鲁传颖

【内容提要】 特朗普执政后，保守主义思想的回归引领了美国网络安全战略的转向。“美国优先”和传统共和党保守主义两种思想自上而下的调整与“黑客干预大选”事件自下而上的驱动共同推动形成了保守主义网络安全战略。联邦政府各部门并以此为指导制定了“全政府”的网络安全政策。主要表现为网络军事力量发展更加激进，并且试图突破“主权”限制，通过“持续交手”“前置防御”将行动空间拓展到他国主权范围；网络外交地位明显弱化，美国与主要大国之间网络外交陷入低谷，并消极对待网络空间国际治理进程；国土安全防御一改过去“虚大于实”的状况，定位得到了明显提升；信息与通信技术政策成为网络安全战略的新领域，引发了大国之间围绕供应链安全的激烈博弈。保守主义网络安全战略调整能否获得预期的战略收益还很难说，但一系列负面效应已经开始显现，单边主义让美国陷入了双重网络安全困境，进攻性网络行动增加了大国冲突风险。对外交和网络空间国际治理地位的弱化则加剧了国际秩序失范。作者旨在从特朗普政府保守主义网络安全战略调整入手，通过分析其背后的保守主义战略思想源流，并结合网络军事、外交、国土安全、信息与通信技术政策等领域的实际政策调整进行论证，对特朗普政府网络安全战略调整的影响进行评估。

【关键词】 保守主义思想；持续交手；前置防御；网络安全战略

【作者简介】 鲁传颖，上海国际问题研究院网络空间国际治理研究中心秘书长，副研究员（上海 邮编：200233）。

【中图分类号】 D815 【文献标识码】 A 【文章编号】 1006-9550（2020）01-0060-20

* 本文系国家社会科学基金一般项目“网络空间大国关系与战略稳定”（项目编号：19BGJ083）的阶段性成果。感谢《世界经济与政治》匿名审稿人的意见和建议，文中疏漏由笔者负责。

一 引言

特朗普政府执政以来，在外交方面先后退出跨太平洋伙伴关系协定（TPP）与应对全球气候变化的《巴黎协定》，签署修订版美墨加协定（USMCA）取代《北美自由贸易协定》（NAFTA），挑起与中国的经贸摩擦；在内政方面大力修建边境墙、实施严厉的移民政策，其核心执政团队频繁变动。特朗普政府一系列反传统、反建制、非常规的行为引发了一场关于美国战略思想的大讨论。特朗普本人打出了“美国优先”口号，并将之作为执政的战略思想。① 美国战略界对究竟什么是特朗普政府的执政思想有不同理解：瑞贝卡·李斯纳（Rebecca Lissner）认为，特朗普并没有学术界所谓的“大战略（grand strategy）”和政策界的“主义（doctrine）”，更多的是一种“战术性交易主义（tactical transactionalism）”。② 约瑟夫·奈（Joseph S. Nye）认为特朗普上台意味着“自由国际秩序”终结，美国开始回归孤立主义。③ 有学者认为美国政府军事干涉叙利亚、援助乌克兰、迁址美驻以色列使馆等一系列实际政策举措表明，特朗普政府并没有完全退出国际事务，也没有狭隘地界定美国的国家利益，更没有拒绝对外军事干涉，因此很难将其对外战略定性为孤立主义或民族主义。④

乔治·华盛顿大学国际关系学教授亨利·诺（Henry Nau）认为，特朗普政府的战略思想并没有突破国际主义的框架，而是反映了保守国际主义思想（conservative internationalism），其核心要素包括信奉国家主权而非国际机制、强调国家安全的高度意识形态化、保持强大的军事和国家安全实力、推行武力化的外交（armed diplomacy）、注重传统地缘政治威胁和恐怖主义威胁等。⑤ 2017 年 12 月，《美国国家安全战略》报告出台后，学术界对特朗普政府的战略思想进行了新一轮讨论。有学者认为美国的战略思想逐渐清晰地表现为孤立主义、经济民族主义与共和党现实主义的结合。⑥ 也有学

① Eric Rauchway, “How ‘America First’ Got Its Nationalistic Edge,” *The Atlantic*, May 6, 2016, https://www.theatlantic.com/politics/archive/2016/05/william-randolph-hearst-gave-america-first-its-nationalist-edge/481497/，访问时间：2019 年 11 月 26 日。

② Rebecca Lissner and Micah Zenko, “There Is No Trump Doctrine, and There Will Never Be One,” https://foreignpolicy.com/2017/07/21/there-is-no-trump-doctrine-and-there-will-never-be-one-grand-strategy/，访问时间：2019 年 11 月 26 日。

③ Joseph S. Nye, “Will the Liberal Order Survive?: The History of an Idea,” *Foreign Affairs*, Vol.96, No.1, 2017, pp.10-13.

④ 焦兵《特朗普保守国际主义战略分析》，载《现代国际关系》，2018 年第 8 期，第 32 页。

⑤ Henry Nau, “Why Conservative, Not Liberal, Internationalism?” *Orbis*, Vol.62, No.1, 2018, pp.24-29.

⑥ 倪峰《变轨、脱轨、延续——从美国对外战略的轨迹看特朗普新版〈美国国家安全战略〉报告的三个特点》，载《国际关系研究》，2018 年第 1 期，第 21—25 页。

者分析《美国国家安全战略》报告后认为其是特朗普“美国优先”与共和党建制派思想框架的结合。① 作为一个商人出身的“非传统”总统,特朗普善变的风格和充满不确定性的举动使各界围绕其战略思想的争论持续不休。

美国政府的战略思想对于安全战略而言具有设定战略目标、排列战略优先次序、引导政策制定方向的重要作用。因此,在对美国网络安全战略进行分析时,分析其背后的战略思想对于理解网络战略演变过程、判别未来发展方向、识别战略重点具有重要价值。相对于奥巴马政府战略思想与网络安全战略之间清晰的逻辑关系认定,学术界对于特朗普政府的网络安全战略思想存有不同观点。有学者认为“美国优先”是特朗普政府网络安全战略的指导思想,②也有学者提出“以实力促和平”“重视军事力量”等传统保守主义思想具有重要影响。③ 总体而言,特朗普政府网络安全战略是对奥巴马政府自由国际主义战略的替代,在大方向上实现了保守主义思想的回归。

二 保守主义网络安全战略思想的演进

在美国两党政治中,共和党政府一旦上台,会通过执政团队的调整将其保守主义思想贯彻到内政外交大政方针当中,取代民主党的自由主义执政理念。特朗普政府的特殊性表现在总统本人及其周围的“核心成员”与共和党建制派之间处于一种矛盾与合作共存的状态。这种状态也影响着保守主义网络安全战略的演进。一方面,特朗普本人所提出的“美国优先”思想中民族主义、孤立主义和民粹主义成分对战略演进的影响巨大;另一方面,共和党建制派网络安全团队秉持保守主义思想传统对战略进行调整。两者共同构成了保守主义网络安全战略的思想来源。

(一)“美国优先”对网络安全战略思想的影响

“美国优先”思想对网络安全战略的影响主要体现在该思想中民族主义、孤立主义和民粹主义成分与网络安全领域安全风险泛在、规则体系缺失、影响范围广阔等特点的内在关联性,主要表现为:对网络安全领域面临的风险高度重视,打破了安全与发展的平衡;将维护美国在网络安全领域的“霸权(supremacy)”视为优先目标,对潜在的挑战者予以全政府式的打击。

“美国优先”思想打破了安全与发展的平衡,过度强调网络安全风险及应对,对价

① 任晓《〈美国国家安全战略〉报告探析》,载《国际关系研究》,2018 年第 1 期,第 14—17 页。

② 汪晓风《“美国优先”与特朗普政府网络战略的重构》,载《复旦学报(社会科学版)》,2019 年第 4 期,第 179—188 页;张腾军《特朗普政府网络安全政策调整特点分析》,载《国际观察》,2018 年第 4 期,第 64—79 页。

③ 李恒阳《特朗普政府网络安全政策的调整及未来挑战》,载《美国研究》,2019 年第 5 期,第 41—59 页。

值观、经济等方面关注不足。奥巴马政府国家安全委员会网络政策主任在总结“奥巴马网络主义(Obama's cyber dotrine)”的时候提道“奥巴马政府的网络安全政策将互联网视为提升效率、拓展经济贸易和思想交流的平台。尽管网络安全带来了真正的风险,但是有效的应对方法必然是增加互联网的开放性和创新性。过度通过发展军事来应对网络安全会将会产生网络边界,伤害数字经济发展。”①特朗普政府的网络安全战略以国家安全为导向,突出安全的重要性,忽视了美国的软实力、价值观以及给数字经济发展带来的负面效应。《美国国家安全战略》报告中将网络安全视为与国土安全、反恐与打击跨国犯罪、提高抗灾能力同等地位的保卫美国国土安全与生活方式的四个要点之一。其用“网络时代的安全”来取代奥巴马政府时期提出的网络安全概念,用更加宏观和全方位的视角来看待网络安全对美国国家安全的深刻影响,指出联邦政府网络、社会赖以运行的关键基础设施和个人的日常生活都面临着网络安全威胁。② 通过网络空间,对手不用跨越国界,就可以发起一场破坏美国政治、经济和安全利益的行动。③

“美国优先”思想推动了从构建网络空间的“领导权”到维护网络“霸权”的转变。奥巴马政府更多强调美国在网络安全领域的领导权,把基本自由(fundamental freedom)、保护隐私和信息自由流动视为核心原则,注重通过承担责任和义务来获取美国的领导权,并强调网络空间的全球属性,重视其他国家、组织、私营部门的共同参与。④相比之下,特朗普政府则将美国网络霸权视为理所当然,不容挑战。《美国网络安全国家战略》中指出,“网络空间的崛起与美国成为唯一的超级大国有密切关联,互联网的开放、互操作、可靠与安全离不开美国的霸权”。⑤ 对于任何可能对网络霸权发起挑战的潜在国家,美国将予以高度防范和打击。特朗普政府将俄罗斯和中国视为“修正主义国家”以及网络安全领域的对手和威胁,称俄罗斯在全球开展的信息行动对美国

① Rob Knake, “Obama's Cyber-Doctrine,” *Foreign Affairs*, May 2016, https://www.foreignaffairs.com/articles/united-states/2016-05-06/obamas-cyberdoctrine,访问时间:2019 年 12 月 1 日。

② The White House, “National Security Strategy of the United States of America,” December 17, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf,访问时间:2019 年 12 月 1 日。

③ The White House, “National Security Strategy of the United States of America,” December 17, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf,访问时间:2019 年 12 月 1 日。

④ The White House, “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” May 2011, pp.3-16, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf,访问时间:2019 年 12 月 1 日。

⑤ The White House, “National Cyber Strategy of the United States of America,” September 2018, pp.1-2, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf,访问时间:2019 年 12 月 1 日。

网络安全构成严重威胁,[①]中国在大数据、人工智能等前沿信息通信技术(ICT)领域实力的增强也是对美国在网络空间中霸权的伤害。[②] "美国优先"还高度重视ICT技术和产业在维护网络空间安全上的作用,认为对手国家通过贸易、投资和合作研究大量获取美国的技术,并将其作为危害美国国家安全的工具。前白宫顾问史蒂芬·班农(Stephen Bannon)称美国与中国的关系是一场经济和信息"战争"。谷歌创始人之一的埃里克·施密特(Eric Schmidt)表示,尽管美国的利益与中国纠缠在一起,但中国是美国在全球技术霸权竞争中的头号对手。[③]

(二)共和党建制派决策团队对网络安全战略的调整

来自共和党建制派的网络安全决策团队一方面对民主党自由主义网络安全战略展开全面调整,另一方面也对特朗普"美国优先"中一些过于极端、民粹的理念进行了一定程度的调和。新团队制定的很多网络安全政策背后都有共和党传统安全政策的色彩。

特朗普政府对网络安全团队的人事和机构进行了调整。美国网络安全决策体系中具有重要影响的机构分别是白宫、国防部、国务院、国土安全部、情报界(IC)、商务部和财政部,主要人员包括国土安全与反恐助理(也负责网络安全事务)、白宫网络安全事务协调员、网络安全司令部/国家安全局负责人以及国务院、国土安全部、中央情报局、联邦调查局、商务部和财政部等机构负责网络事务的高级官员。特朗普政府对网络安全决策团队的调整分为两步:第一步是人员调整,按照常规从共和党内部选拔了一批官员重新担任上述重要岗位的负责人,取代了奥巴马政府的官员。如负责网络安全事务的白宫国土安全顾问托马斯·博塞特(Thomas Bossert)是小布什政府时期国土安全顾问,白宫网络安全协调员罗伯特·乔伊斯(Robert Joyce)是从国家安全局定制行动小组(TAO)负责人的岗位上内部提拔。第二步是机构改革,对奥巴马时期的网络安全架构进行了调整,先是于2017年7月撤并了国务院网络事务协调员办公室,然后在约翰·博尔顿(John Bolton)担任国家安全事务顾问后降级了博塞特曾担任的

① The White House, "National Security Strategy of the United States of America," December 17, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf,访问时间:2019年12月1日。

② The White House, "National Security Strategy of the United States of America," December 17, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf,访问时间:2019年12月1日。

③ Liz Moyer, "Engage China, or Confront It? What's the Right Approach Now?" *The New York Times*, November 11, 2019, https://www.nytimes.com/2019/11/11/business/dealbook/us-china-relationship-future.html?_ga=2.30331063.903463097.1577127949-1816048929.1577127949,访问时间:2019年11月26日。

国土安全与反恐助理的职位，并取消白宫网络安全事务协调员这一岗位。

建制派网络安全团队深受保守主义传统安全政策的影响，逐渐将其“移植”到网络安全领域，以替代自由主义网络安全战略思想。奥巴马政府的网络安全战略主要反映了民主党自由主义的思想，认为美国要发挥在网络空间国际规则方面的引领作用，追求增强软实力，注重国际法在网络空间中的适用，强调网络规范在约束国家行为方面的作用，积极推动与其他网络大国建立信任；对网络军事行动采取比较谨慎的态度，更愿意通过综合使用外交、政治、经济、执法手段，采取如“点名批评”“外交施压”“经济制裁”“司法起诉”等“跨域威慑（cross-domain deterrence）”的方式来解决网络安全问题。

保守主义通常“强调硬实力、重视主权、认为国际机构和组织是实现目标的手段而不是目标本身、主张自由贸易、对外部的安全环境抱较为悲观的观点”。[①] 特朗普政府的网络安全团队认为，美国面临的网络安全环境十分严峻，网络安全已经成为国家安全面临的最主要的风险来源与最复杂棘手的难题，网络安全一旦失守，国家安全将面临整体陷落的风险。[②] 网络安全威胁领域也极为广泛，作为国家安全的核心组成部分，网络安全与政治安全、经济安全、文化安全、社会安全、军事安全等领域相互交融、相互影响，在识别各个领域所面临的安全风险时，网络安全都是关键因素。此外，网络威胁来源也不断扩大，既包括国家，也包括恐怖主义、犯罪分子等。[③] 美国要维护自身的利益就必须采取更加主动、积极的网络安全政策。

“以实力促和平”“单边主义”“理念一致国家（like minded states）”同盟等传统共和党执政理念在网络战略中开始得到更多重视。“以实力促和平”政策在网络安全战略中表现为高度重视发展网络军事力量和建设网络国土安全防御能力。2017 年 8 月网络政策团队组建后不久，特朗普政府就宣布将网络司令部升级为美军的第十个一级作战司令部，迅速完成了奥巴马政府时期存有争议的网络军事政策转变。国土安全防御也得到了前所未有的重视，这反映在重新改组网络与基础设施局，增加国土安全部在维护联邦政府网络安全、关键基础设施安全等方面的职能。“单边主义”的网络战

① James Traub, “The Bush's Year: W.'s World,” *New York Times Magazine*, January 14, 2001, https://www.nytimes.com/2001/01/14/magazine/the-bush-years-w-s-world.html，访问时间：2019 年 11 月 26 日。

② The White House, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/，访问时间：2019 年 12 月 26 日。

③ The White House, “National Security Strategy of the United States of America,” December 17, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf，访问时间：2019 年 12 月 1 日。

政策也越来越多地开始影响美国在中东等地区开展的网络反恐行动。美军多次采取网络行动追踪“伊斯兰国(ISIS)”的成员,打击其指挥网络。① 在网络安全国际治理中,美国则主张降低联合国的地位,加强“理念一致国家”之间的协作。

三 保守主义思想催生进攻性网络安全政策

“美国优先”和共和党网络安全决策团队的保守主义思想通过自上而下的方式对网络安全政策进行调整,与此同时,“黑客干预大选”则以一种被动应对、自下而上的方式配合着保守主义思想的加速回归。“黑客干预大选”是美国网络安全领域中一次具有里程碑意义的事件,揭示出黑客组织通过综合利用网络攻击、虚假信息和社交媒体操纵活动操纵美国选民,②其被认为是一次超越传统间谍界限的、试图颠覆美国民主的尝试。③ 保守主义思想的官员和学者纷纷将其视为美苏冷战时期意识形态斗争的翻版。④

这一事件暴露出美国在网络安全预防措施和应对手段上存在的不足。在防御层面,国土安全部投入大量资源建设的“爱因斯坦”入侵检测系统、国家安全局数量众多的“网络监听”项目以及国防部、情报界所拥有的先进“态势感知”技术,都未能起到预防作用。⑤ 在事后应对中,网络外交、军事手段都未能发挥有效的作用。奥巴马政府试图通过复制中美在“网络商业窃密”领域的经验,通过“跨域制裁”施压来推动建立“规范”遭遇失败。美国花费巨资大力建设的“网军”在应对类似“武装冲突门槛之下(below the threshold of LOAC)”的冲突时,几乎无法发挥应有的作用。“黑客干预大选”所揭示出的对安全风险的应对举措不足成为保守主义网络安全战略演进过程中,

① Dina Temple-Raston, “How the U.S. Hacked ISIS,” *NPR*, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis,访问时间:2019 年 12 月 1 日。

② 关于“黑客干预大选”在多大程度上影响了选举结果,美国社会有一定分歧,但从《穆勒报告》中对这一事件用了近 30 页进行了详细描述,其中细节表明,这一事件对选举的影响不容低估。参见 Rosalind Helderman and Matt Zapotosky, *The Mueller Report*, New York: Scribner, 2019, pp.94-123。

③ Brianna Ehley, “Clapper Calls Russia Hacking a New Aggressive Spin on the Political Cycle,” Politico, October 20, 2016, http://www.politico.com/story/2016/10/russia-hacking-james-clapper-230085,访问时间:2019 年 12 月 1 日。

④ Seth Jones, “Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare,” CSIS Briefs, October 1, 2018, https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare,访问时间:2019 年 12 月 1 日。

⑤ Jonathan Reiber and Ikram Singh, “Where's the 9/11 Commission for Russia's Election Attack?” November 13, 2017, https://foreignpolicy.com/2017/11/13/russia-election-attack-usg-response-911-commission,访问时间:2019 年 11 月 26 日。

决策部门对网络军事、外交、国土安全、信息通信技术政策调整的主要参照对象。

(一)网络军事力量发展方向更加激进

民主党和共和党在发展网络军事力量方面具有高度共识。自 2007 年以来,美国国防部获得的网络军事预算一直呈大幅增长趋势。据民间机构"纳税人(taxpayer)"网站统计,仅 2007—2016 年国防部的网络安全支出就翻了 6 倍,从 30 亿美元上升至 185 亿美元,这一数字在特朗普政府时期继续保持高速增长。① 两党之间的差别在于如何使用网络军事力量。奥巴马政府时期,美国网军在开展军事行动上较为谨慎,面临着外交、国际法等多方面的约束。外交方面,网络军事行动后果难测,容易引起国家间冲突升级和附带伤害,美国也一直面临各国对其推动网络空间军事化的指责。国际法方面,"武装冲突法""国际人道法"在网络空间的适用上还存在较大争议,开展网络军事行动很难得到国际法"背书"。特朗普政府则更加注重发挥军事力量在国家战略中的作用,在网络军事力量建设和发展上越来越激进。

一是加速网络力量的体系化建设,完成了网络司令部的架构升级,构建完善了跨军种的联合作战指挥体系,网军战斗力初步形成。2017 年 8 月国防部正式启动网络司令部升级的工作,网络司令部成为美军第十个一级作战司令部,各军种的网络作战力量与网络司令部之间形成了自下而上的统分结构,网络军事力量基本完成了与空军、陆军一样的全军种覆盖。② 2018 年 5 月,133 支网络任务部队提前实现全面作战能力。此外,网络力量建设突破了"军民有别"的藩篱而向民用领域发展,突破了以往与私营部门合作的边界,将网络军事防御进一步扩大到民用领域,包括民用关键基础设施。③ 国防部明确指出,鉴于一些民用资产对美军确保在网络空间中绝对优势的重要意义,必须保护好国防关键基础设施(DCI)和国防工业基地(DIB)的网络系统与设备。④ 此外,国防部还改变了与私营部门合作的模式,从过去仅提供网络技术支持和技术的商业化指导升级为与私营部门建立"可信赖的合作伙伴关系",从而将私营部门纳入其网络行动部署的考虑范围,使国防部得以通过私营部门来获取更多的网络资

① 参见 http://cyberspending.taxpayer.net,"纳税人"是一家建立于 1995 年的独立民间机构,旨在对政府财政预算进行公开监督,其统计方法和资料来源主要依据国会和行政部门的公开资料,有较强的可信度。

② 陈婷《跨域融合:美国"网军"建设发展新动向》,载《信息安全与通信保密》,2018 年第 6 期,第 36—40 页。

③ Department of Defence, "Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge," January 19, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf,访问时间:2019 年 11 月 26 日。

④ Department of Defence, "Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge," January 19, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf,访问时间:2019 年 11 月 26 日。

源和更为广泛的态势情报。① 这一举动极有可能打破传统的“军民平衡”体系，改变美军不涉足美国国内事务的传统，并突破美国法律体系的规定。

二是重新认识网军面临的作战环境，认为现有的网络安全思维已经不适应网络空间战略环境的变化，无法应对网络安全的发展趋势。“黑客干预大选”揭示出网络是一个“灰色地带”，对手针对美国采取“武装冲突门槛之下”的行动并以此获取利益，挑战美国在网络空间中的主导权。现有的网络战略思想对此应对不足，“以实力促和平思想”并不能完全适用于网络空间，“网络威慑”也难以发挥应有的效用。因此，美国要突破原有网络安全战略思想的藩篱，积极适应新的网络战略环境。美国网络司令部/国家安全局新任负责人保罗·中曾根(Paul Nakasone)公开表示“美国的军舰不是在军港中保卫领海，飞机也不是在机场中保卫领空……按照这一逻辑，网军必须要在敌人的虚拟空间开展行动来保卫我们的军队和国家关键利益。”②“我们需要走出自己的网络，在边境之外开展行动，确保我们掌握对手的情况。如果仅仅在自己的网络中开展防御，将会丢掉主动权。”③此外，网络空间是一个新的战略环境，空间中的国家利益和对手的行为已经发生了巨大变化，因此美国需要适应环境变化，针对对手开展持续性的网络行动，降低对手的战略收益。④

三是扩大网军的行动空间，将网军的行动空间从传统的武装冲突法之上(above the threshold of LOAC)顺势拓展到武装冲突法之下，“持续交手(persistent engagement)”“前置防御(defend forward)”成为指导美军对外开展网络行动的指导思想。美国网络司令部将“持续交手”定义为“在不爆发‘武装攻击(armed attack)’的前提下，打击对手并获取战略收益”。⑤ 这一概念最初由美国国防研究所(IDA)的两名学者提出，后被保罗·中曾根认可，并写入美国网络司令部的战略文件中。⑥ “持续交手”本

① Department of Defence, “Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge,” January 19, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf,访问时间: 2019 年 11 月 26 日。

② Paul Nakasone, “A Cyber Force for Persistent Operations,” *Joint Forces Quarterly*, Issue 92, No.1, 2009, p.12.

③ “An Interview with Paul M. Nakasone,” *Joint Forces Quarterly*, Issue 92, No.1, 2009, p.7.

④ Michael P. Fischerkeller and Richard J. Harknett, “Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace,” *Lawfare*, November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace,访问时间: 2019 年 12 月 1 日。

⑤ US Cyber Command, “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,” April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010,访问时间: 2019 年 12 月 1 日。

⑥ “持续交手”概念的主要发明人迈克尔·菲斯凯勒 2019 年 9 月在上海参加学术研讨会时曾就“持续交手”专门做了发言，阐述了这个概念从学术概念上升为政策概念的过程。菲斯凯勒告知笔者之所以用 engagement 主要是要强调这是一个防御概念。基于持续交手的实际内涵，本文认为 engagement 更具有交手而非接触的含义。

质上就是采取进攻性网络行动来削弱对手的实力，是一种适应网络战略环境，有效应对对手行为的网络防御政策。① 这一政策导致了“第 20 号总统行政令”的废除，放开了美军在采取进攻性网络行动方面的限制，使网军能够更自由地对其他的国家和恐怖分子等对手开展网络行动，而不受限于复杂的跨部门法律和政策流程。② 从外界看来，“持续交手”存在着将进攻定义为防御、侵犯他国网络主权和违反国际法等后果。

为进一步完善“持续交手”的政策内涵，国防部提出了“前置防御”的战术概念。前置防御指在网络危害发生前，提前收集对手的信息，使对手放弃攻击行动。③ “从源头上破坏或阻止恶意网络活动，包括低烈度武装冲突。”④前置防御与主动防御存在两点主要区别：一是防御阶段前移。主动防御侧重及时识别与发现正在进行的网络攻击行为，前置防御则强调在恶意网络活动发生之前就采取行动，从源头上加以遏制，以进攻性的网络行动阻断和打击潜在敌人的网络攻击行为。二是防御范围扩大。在主动防御方针下，美军只需保护国防部的网络和系统安全，前置防御则要求美军在各种威胁发生之前就采取行动排除安全隐患，即美军可以在世界上任何地方展开网络行动，对各种“存在威胁美国国家安全利益”的目标发起攻击。通过以上转变，特朗普政府将对网络军事力量发展的限制降到有史以来的最低水平，以新的网络力量建设思路和行动方针为网军的实战化发展建立制度基础并争取最大的物资支持。应注意到，无论是“持续交手”还是“前置防御”都是在对手的主权网络空间当中开展，势必损害对手国家主权，带来冲突升级的风险。

（二）外交在网络战略中的地位明显弱化

特朗普政府总体上不重视外交在网络安全战略中的作用，这一点与“美国优先”中的孤立主义、民族主义思想相呼应，同时也与网络外交在应对“黑客干预大选”上的失败有关。奥巴马政府通过“跨域制裁”施加压力，建立“不干预选举”的网络规范来

① Michael P. Fischerkeller and Richard J. Harknett, “Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation,” Institute for Defense Analysis Pulication, May 2018, https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx，访问时间：2019 年 12 月 1 日。

② Department of Defence, “Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge,” January 19, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf，访问时间：2019 年 11 月 26 日。

③ Jeff Kosseff, “The Contours of ‘Defend Forward’ Under International Law,” published on 11th International Conference on Cyber Conflict, https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf，访问时间：2019 年 11 月 26 日。

④ Department of Defence, “Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge,” January 19, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf，访问时间：2019 年 11 月 26 日。

解决美俄之间冲突未能取得成功。俄罗斯不承认美国对自己的指控,也反对在国际上建立相应的网络规范。网络外交在奥巴马政府时期是美国网络空间国际战略的基石,也是美国网络空间安全战略的核心支柱之一。① 特朗普政府更加注重网络安全领域的"硬实力"而非"软实力",认为与其耗费数十年去谈判国际规则,不如建立强大的网络安全实力来维护自身安全。② 外交在网络战略中地位弱化有两个代表性的事件:一是特朗普政府撤并了负责网络外交和国际合作的国务院网络事务协调员办公室,并在首任美国网络安全事务协调员克里斯托弗·佩恩特(Christopher Painter)退休后取消了这一职位;二是在各个部门的网络安全战略纷纷出台之后,国务院主导的《网络空间国际战略》却迟迟难以出台。特朗普政府弱化网络外交导致美国消极对待网络空间的国际治理进程,美国与主要大国之间的网络外交也陷入低谷。此后,美国与其他国家的对话交流明显减少。中美网络空间国际规则高级别专家组和执法与网络安全对话仅开展一次就陷入暂停状态。美俄网络安全工作组因斯诺登事件被终止,至今未能恢复。不仅如此,美国与盟友国家之间的网络对话也基本没有继续。总体而言,特朗普政府的网络外交对话基本陷入静默状态。

在网络空间的国际治理层面,特朗普政府一改前任政府的积极姿态,消极对待国际社会在这一领域的努力。美国不仅对联合国等多边进程缺乏兴趣,还反对其他国家和组织提出的倡议。特朗普政府反对成立联合国信息安全开放式专家组(OEWG),拒绝签署法国政府在2018年首届巴黎和平论坛(Paris Peace Forum)期间提出的《网络空间信任和安全巴黎倡议》。奥巴马政府时期,在美国和英国政府支持建立的"伦敦进程"一度被认为是网络空间治理领域最有影响力的机制之一。特朗普政府不仅没有投入资金支持类似的国际治理机制,也不愿意在政治上积极参与,导致这些原本得到美国支持的国际机制的影响力江河日下。

特朗普政府从根本上质疑国际治理的作用,认为构建网络空间国际治理机制的谈判可能需要数十年才能产生成果,耗时费力。即使达成了共识,网络安全的"可抵赖性"也为美国的竞争对手不遵守这些国际机制提供了灵活操作空间。③ 美国反而会因为遵守国际机制而自缚手脚,赋予对手竞争优势。特朗普政府将网络空间国际治理机

① The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," June 2009, https://fas.org/irp/eprint/cyber-review.pdf,访问时间:2019年12月1日。

② Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis*, Vol.61, No.3, 2017, pp.381-393.

③ Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol.41, No.3, 2017, pp.44-47.

制视为落实美国网络战略的工具，一旦无法达到目标就坚决抛弃。如在第五届联合国信息安全政府专家组谈判中，尽管各方对于报告中 90%以上的内容都达成了共识，但由于在美国主张的赋予国家在网络空间的自卫权上存在争议而未能发布报告。美国的态度非常坚决，如果不能满足这一条，宁愿专家组机制失败。① 这与第四届专家组中美国表现出的协商与合作态度形成了鲜明对比。

（三）国土网络安全防御作用加重

特朗普政府极为重视国土安全领域面临的风险挑战，大幅提升了国土安全部在网络安全战略中的地位，赋予其统管美国网络安全风险识别、保护联邦网络和关键基础设施安全等重要任务。该调整一方面与保守主义重视国土安全的传统有关，另一方面与“黑客干预大选”暴露出美国在网络安全防御方面的体制弊端也有很大关联。“黑客干预大选”是美国网络安全防御面临的一次重大挫折，有人将其称为网络领域的“9·11”事件，②暴露出国土安全部履行网络安全职能时存在严重的能力不足。奥巴马政府时期，国土安全部不仅缺乏相应的技术能力和人才资源，还受到国家安全局、联邦调查局等情报机构的挤压。③ 此外，网络安全涉及内部隐私和敏感信息，无论是联邦政府部门还是掌握关键基础设施的私营部门都不愿意向国土安全部分享相关信息，这使得国土安全部前期投入大量资源建设的“爱因斯坦”入侵检测系统和“态势感知”技术由于受到多方制约而未能在防范“黑客干预大选”中发挥应有作用。

特朗普政府提出了国土网络安全积极防御的理念，旨在通过提升网络安全的态势感知、威胁分析能力以及提升网络的韧性（resilience）来增加攻击者的成本。随后，投入大量的政策和资源予以支持，先是发布《国土安全部网络安全战略》，明确国土安全部在网络安全方面的职责和职能扩张，并且在预算上大幅倾斜，2020 年国土安全部的网络安全预算在原本高速增长的基础上进一步增加到 19 亿美元。此外，国土安全部还被赋予更大的权力和行动空间，有权要求掌握大量关键基础设施的私营部门更加主动地配合该部门的领导。奥巴马政府时期更强调通过私营部门和社会在网络安全领域中的重要作用，通过公私合作（PPP）的方式维护美国网络安全，但存在私营部门缺乏配合动力的问题。特朗普政府则赋予国土安全部在态势感知、威胁情报共享等方面

① François Delerue, “The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?” *Euroupean Soceity of International Law*, Vol.7, No.4, 2018, pp.2-4.

② Jonathan Reiber and Ikram Singh, “Where's the 9/11 Commission for Russia's Election Attack?” November 13, 2017, https://foreignpolicy.com/2017/11/13/russia-election-attack-usg-response-911-commission，访问时间：2019 年 12 月 16 日。

③ 参见左晓栋主编《美国网络安全战略与政策二十年》，北京：电子工业出版社 2018 年版，第 248—250 页。

的领导权，运营关键基础设施的企业只有加强与国土安全部的合作才能获得政府提供的有害网络安全信息以及相应的业务指导。通过这种垄断并有选择地提供公共服务的方式来迫使企业就范，将国土安全部的权力延伸到私营部门领域。

约翰·博尔顿(John Bolton)就任国家安全助理后，着力解决国土网络安全防御多头管理的问题，对部分岗位进行了调整，实现国家安全委员会对网络安全的直接领导，以更加强硬的姿态来推动国家安全、网络安全和国土安全的融合。① 此外，国土安全部为了能够更好地完成《国土安全部网络安全战略》中所提出的任务要求行动，提升了网络安全事务在国土安全部内部的地位，新成立了网络安全与基础设施局(CISA)统筹负责新增的网络安全职能。

(四)网络安全因素推动ICT政策调整

“美国优先”在网络安全战略中的影响还表现为民族主义和孤立主义思想导致的ICT政策调整。② 随着大国在网络安全领域的博弈加剧，网络安全的影响范围也在向外拓展，ICT产品与服务作为网络安全的载体也成为网络安全战略的一部分。特朗普本人对经济和科技安全高度重视，促使ICT政策成为保守主义网络安全战略的重要组成部分。网络安全本质上是指确保ICT产品与服务的机密性、完整性、可用性(合称C.I.A)。美国政府在“第20号总统行政令”中做了关于进攻性网络行动和防御性网络行动所产生的网络效应的阐述，即“对计算机、信息或通信系统，网络，由计算机或信息系统控制的物理或虚拟基础结构或其中存储的信息的操纵、干扰、拒止、降级或破坏”，更加清楚地解释了网络安全的内涵。③ 奥巴马政府将网络安全的重心放在防止对ICT产品和服务的C.I.A实行操纵、干扰、拒绝、降级或破坏上。特朗普政府则将关注点进一步拓展到信息通信产品和服务本身，认为对手国家无法获得最新的信息产品与服务，也会导致其安全威胁等级的降低。例如美国威胁禁止中兴采购美国企业生产的芯片，一度导致中兴公司停产，逼迫其不得不认罚。从国际安全或国家安全出发，这就将网络安全从ICT产品与服务的安全进一步向外拓展到ICT科技创新生态和供应链安全领域。大国之间通过政治、外交、经济、科技等手段加强了在这一领域的战略竞争，目的是为了加强对自身供应链安全的控制并对对手予以打击。

① Brain Barrett, “The White House Loses Its Cybersecurity Brain Trust,” Wired, April 16, 2018, https://www.wired.com/story/rob-joyce-tom-bossert-white-house-cybersecurity-policy/amp, 访问时间: 2019年11月26日。

② 参见张业亮《另类右翼的崛起及其对特朗普主义的影响》，载《美国研究》，2017年第4期，第11—17页。

③ The White House, “Presidential Policy Directive 20,” http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf, 访问时间: 2019年11月26日。

特朗普政府通过多种政策手段来加强对自身供应链安全的建设: 一是以“国家安全”为由,禁止采购有安全“隐患”的外国企业的产品和服务。特朗普政府在“黑客干预大选”之后禁止联邦政府使用俄罗斯网络安全公司卡巴斯基的产品和服务,《2019 国防授权法案》禁止采购中国华为、中兴、大疆和海康威视的产品与服务。二是直接加大对 ICT 供应链中重点领域的投资力度。特朗普政府设立了一支由联邦通信委员会(FCC) 负责的 200 亿美元的基金,用于加强美国政府在 5G 领域的投资建设,加大对 ICT 行业的控制力量。① 三是通过公私合作,将更多的民用网络技术应用到国家安全领域,提升 ICT 的保障能力。传统军民两用技术往往是先应用在军事领域,随后再扩展到民用领域。在网络领域,这一趋势恰恰相反,很多核心技术初始是由互联网企业所掌握,后来用于进一步提升政府、军队的 ICT 保障水平。例如美国国防部与微软和谷歌开展人工智能合作研究,采购亚马逊物流系统服务于军事后勤等。②

特朗普政府通过实体清单、投资审查、长臂管辖、市场准入、国家安全审查等多种手段,打击对手的 ICT 行业,增加其供应链的脆弱性。2018 年 10 月,美国商务部工业安全署(BIS) 根据《出口管制改革法》授权出台了出口管制清单,③将来自中国的华为、四川大学、电子科技大学、中国电子科技集团等一系列 ICT 相关的企业、高校和研究机构列入实体清单,禁止美国相关机构与被列入清单的机构开展合作。美国还对外国投资审查制度(CFIUS) 进行了改革,将与网络安全相关的敏感行业、技术作为重点审查对象。在国际层面,特朗普政府更是动员了外交、情报、军事、法律等多种手段来打击对手。以对华为和卡巴斯基的打击为例,特朗普政府不仅通过外交途径向盟友施加压力,并且以信号情报分享和网络军事合作为筹码,胁迫“五眼联盟”和北约成员以及日本等国家共同封杀华为和卡巴斯基。

四 特朗普网络安全战略调整带来的影响

特朗普政府从国家安全战略角度高度出发重视网络安全问题,加大对网络安全领

① Edward Baig, “U.S. Establishes MYM20.4 Billion Fund to Bring 5G to Rural America: What 5G Means for You,” USA Today, April 14, 2019, https://www.usatoday.com/story/tech/2019/04/12/what-5-g-trump-makes-push-answers-your-questions/3445554002/,访问时间: 2019 年 12 月 26 日。

② David E. Sanger, “Microsoft Says It Will Sell Pentagon Artificial Intelligence and Other Advanced Technology,” *New York Times*, October 26, 2018, https://www.nytimes.com/2018/10/26/us/politics/ai-microsoft-pentagon.html,访问时间: 2019 年 12 月 16 日。

③ 参见钟燕慧、王一栋《美国“长臂管辖”制度下中国企业面临的新型法律风险与应对措施》,载《国际贸易》,2019 年第 1 期,第 93—97 页。

域的政策和资源支持，在一定程度上会提升美国网络安全能力，但保守主义战略思维对美国国内网络安全和国际网络安全形势的负面影响正在逐步显现。

（一）美国陷入新的网络安全困境

保守主义让美国网络安全战略陷入了新的网络安全困境。奥巴马时期，美国网络安全战略的内在逻辑矛盾表现为所谓“网络主权”与“全球公域”的矛盾。① 美国政府在网络空间的公域属性和主权属性之间采取了模糊立场，在具体政策上则奉行实用主义。当美国需要扩大在网络空间的行动范围时，其倾向于将网络空间定义为“全球公域”，强调其特殊性，比如网络自由政策、大规模网络监听政策都是基于否定网络空间的国家主权而开展。当美国需要应对自身的网络安全挑战时，则倾向于将其定义为主权领域，强调网络空间与物理空间的共同性，对美国网络的攻击等同于对国土的攻击，将会受到包括核武器在内的一切武力手段的反击。② 换言之，美国虽然没明确提出网络主权，但实际做法就是将网络空间视为主权范畴。美国的网络安全政策的核心是在精心维护自身行动空间的同时限制对手的行动空间。因此，在网络空间国际规则制定上，美国既缺乏道德制高点，也难以发挥主导权。斯诺登事件后，各国对美国网络战略的内在矛盾有了更加深刻的认识，这导致美国所谓网络自由战略的偃旗息鼓，网络主权的概念被更多国家所接受。

特朗普政府从构建全球秩序退回到主权国家之间的大国博弈，否定网络空间国际治理的作用，试图通过“持续交手”和“前置防御”等政策来维护美国的网络安全。“持续交手”思想在本质上就是将网络行动拓展到其他国家的网络主权范围之内。国际社会固然在网络主权的内涵上存在一定分歧，但是对于“国家在网络空间拥有主权”方面的认识则已取得基本共识，美国政策已经违反了第五届联合国信息安全政府专家组报告中“各国对其领土内的通信技术基础设施拥有管辖权，各国在使用通信技术时，除其他国际法原则外，还必须遵守国家主权、主权平等、以和平手段解决争端和不干涉其他国家内政的原则”，③必然会遭到国际社会的反对。此外，单边主义、孤立主义网络安全思想脱离了网络安全具有全球性议题属性的特征，带来了追求绝对安全与全球网络安全恶化之间的逻辑矛盾。

在保守主义政策的推动下，美国陷入了双重网络安全困境。第一重困境是罗伯特·杰维斯（Robert Jervis）所定义的经典的国家安全困境。美国不断加大对网络军

① 参见杨剑《数字边疆的权利与财富》，上海：上海人民出版社 2012 年版，第 207—215 页。

② 参见杨剑《美国“网络空间全球公域说”的语境矛盾及其本质》，载《国际观察》，2013 年第 1 期，第 46—49 页。

③ “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security，” UN General Assembly Document A/70/174，July 22，2015.

事的投入和采取进攻性的网络战略，引起了其他国家的不安全感，引发了网络空间的军备竞赛，从而抵消了美国网络军事投入的效果。[①] 美国网络军事力量的建设以及开展进攻性网络行动所带来的示范效应已经显现。据统计，全球已有 100 多个国家开始了网络军事力量建设，其中约 40 多个国家具有开展进攻性网络行动的能力。[②] 第二重困境是全球整体网络安全环境恶化对美国单方面努力的抵消作用。国家之间如果不能加强合作，将会给网络恐怖主义和网络有组织犯罪带来可乘之机。美国在网络空间国际机制建设上的倒退不仅使得信息安全政府专家组机制陷入分裂，更让国际社会在打击网络恐怖主义和网络犯罪等问题上的合作陷入困境。[③] 全球网络安全整体形势的恶化使得美国通过加强安全能力建设应对网络安全挑战的努力大打折扣。

（二）加剧大国网络军事冲突风险

“持续交手”和“前置防御”政策使得美军的网络行动目标、范围和手段都在不断扩大，实现了能力、法律和道德等层面的一系列突破，将行动空间拓展到他国主权范围内。这是对现存国际体系和安全架构的重大挑战，必然会引发其他国家的强力反击，引发大国之间的网络军事冲突。

首先，美国网络军事行动不断突破现存国际规则底线带来了新的冲突风险。美国一方面强调网络空间的共同性，认为现有的国际法适用于网络空间，另一方面涉及自身网络安全时又强调网络空间的差异性，认为现有的国际法无法应对风险挑战。因此，要赋予美国更大的自主权，包括单方面对攻击来源的溯源（attribution），对恶意网络行动采取反措施（counter measures），甚至按照所谓“持续交手”理念，在对手攻击尚未发起之前就采取措施攻击对手的网络措施，这将破坏现有国际法体系和挑战他国的网络主权。2018 年美国中期选举时，网络战司令部就主动对涉嫌干预美国大选的俄罗斯互联网研究局（IRA）进行了攻击，迫使其断网一天。[④] 2019 年 6 月，《纽约时报》

① 罗伯特·杰维斯著，秦亚青译《国际政治中的知觉与错误知觉》，北京：世界知识出版社 2003 年版，第 112—205 页。

② 参见北约卓越网络防御中心（CCDCOE）在线图书馆的相关统计，https://ccdcoe.org/library/strategy-and-governance/，访问时间：2019 年 12 月 1 日。

③ Andrey Krutskikh, “Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS’ Question Concerning the State of International Dialogue in This Sphere,” June 29, 2017, http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288，访问时间：2019 年 12 月 1 日。

④ Ellen Nakashima, “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms,” *The Washington Post*, February 26, 2019.

报道，为了反击俄罗斯对美国的网络攻击，美国在俄罗斯电网中植入了病毒。① 美国对他国采取网络行动是否侵犯对方主权，美国采取行动是否有确凿的证据支撑，这样的行为会引发被攻击方什么样的反应，这一系列问题都是引发大国之间网络攻击升级的重大隐患。

从当前国际网络安全治理的角度来看，美国的做法难以得到国际社会的认可，并有可能引发新的危机：第一，美国通过网络行动对他国网络实体进行攻击的行为明显缺乏国际法依据，显然侵犯了他国主权。② 类似的现象如果普遍发生，建立在主权之上的国际安全秩序将会被颠覆，导致国际安全秩序陷入混乱。第二，鉴于网络空间的虚拟性，溯源问题面临很大的技术挑战，尽管美国声称拥有比较先进的溯源技术手段，但通过对美国司法部公布的网络起诉案件进行分析会发现大量的漏洞和主观认定，存在很大的误判风险。③ 第三，被攻击方如何进行反击取决于其对美方发出信号的判断。以对俄罗斯互联网研究局的攻击为例，美方认为这是在向俄罗斯发出威慑信号，告诫其不要干涉美国选举。这种信号并不一定会被俄方接受并做出对等反应。接收方有可能会认为这种攻击是战争行为并采取更加激进的反击手段，从而引发网络冲突危机。

其次，大国在网络空间军事化问题上存在不同认知，这增加了网络行动后果的不确定性。国际法中使用武力上所秉持的“必要性原则、相称原则和区分原则”如何适用于网络空间也是很大的挑战。④ 例如，在受到网络攻击时国家应当如何反击？美国声称会使用包括核武器在内的一切手段进行反击。⑤ 但低烈度的网络冲突时时刻刻都在发生，任何一次网络攻击都有可能成为国家发起军事反击的原因。⑥ 实际上，网络攻击根据危害的程度有多种不同层次，美国进攻性网络行动所采取的网络攻击方式包括对计算机、系统和网络的控制、阻止、拒止、降级和破坏。⑦ 不同层次的攻击会造

① David E. Sanger and Nicole Perlroth, “U.S. Escalates Online Attacks on Russia’s Power Grid?” *The New York Times*, June 15, 2019.

② Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, 2017.

③ Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, Oxford: Oxford University Press, 2015, pp.20-23.

④ “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” UN General Assembly Document A/70/174, July 22, 2015.

⑤ The White House, “International Strategy for Cyberspace,” May 2011, pp.3-6, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf，访问时间：2019 年 12 月 1 日。

⑥ Martin Libicki, *Cyber Deterrence and Cyberwar*, Santa Monica: RAND Corporation, 2009, pp.102-134.

⑦ 刘永涛《国家安全指令：最为隐蔽的美国总统单边政策工具》，载《世界经济与政治》，2013 年第 11 期，第 29—30 页。

成不同的损害。但是当受害国发现自己被网络攻击时,很难精确判断对方破坏行为的目的并给予适当回应,往往过度反应并导致冲突升级。再如,网络安全在核领域引发冲突的风险越来越大,而大国之间并未就此展开讨论。核武器的指挥、控制及通信系统都面临着网络攻击的风险。由于核领域的高度敏感性,任何层次的网络行动都可能引起过度反应。① 随着网络空间军事化的步伐不断加快,各种不确定性急剧上升,在这种情况下,大国之间的首要任务是要探讨如何避免网络攻击,建立信任措施,而非一味发展进攻性网络军事力量。②

最后,网络空间军事化引发的连带伤害(collateral damage)愈发严重。"想哭(WannaCry)"病毒源自美国国家安全局(NSA)的武器库中"永恒之蓝"漏洞的扩散,它给全球带来了几百亿美元的损失,但是受害者难以追究 NSA 的责任,也无法获得相应的赔偿。此外,美国与以色列联合开发的"震网(Stuxnet)"病毒在对伊朗的核设施造成毁灭性破坏之后,也开始在全球的电站中扩散,多个国家已经发现了类似的病毒。由于美国在物理和网络世界中的强大实力,受害国敢怒不敢言,但国际社会不能因为受害国无法声讨和制裁美国就低估连带伤害给国际安全带来的重要影响。可以预见,随着美国在网络空间军事化的道路上越走越远,其带来的连带伤害和负面溢出效应会越来越多,成为国际安全、经济、政治领域新的不稳定来源。

(三)导致网络空间国际秩序失范

特朗普政府的保守主义网络空间战略理念和进攻性的网络安全政策进一步加剧了网络空间秩序的失范,网络空间的"巴尔干化"风险进一步上升。在规则体系缺失、各方认知理念差异较大的情况下,随着大规模监听、情报收集、知识产权窃密、社交媒体操纵、关键基础设施漏洞等网络安全事件的不断增加,国家在网络空间中面临的风险和挑战也在上升:一方面,政府面临与日俱增的应对压力,亟须新的应对手段和方法;另一方面,考虑到网络空间的不确定性和后果,大国在开展网络行动尤其是进攻性网络行动时仍极为谨慎。奥巴马政府对于网络空间行动总体上采取了较为克制、审慎的理念,客观上避免了大国之间激烈冲突的发生。但特朗普政府以"黑客干预大选"为由大幅调整网络安全战略,采取激进、破坏性的方式,对原本脆弱的网络空间秩序构建进程带来了极大冲击,加剧了网络空间的秩序失范。

① Beyza Unal and Patricia Lewis, "Cybersecurity of Nuclear Weapons Systems," Chatham House, January 11, 2018, pp.6-9, https://www.chathamhouse.org/publication/cybersecurity-nuclear-weapons-systems-threats-vulnerabilities-and-consequences,访问时间:2019 年 12 月 26 日。

② Mark D. Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law & Policy*, Vol.4, No.1, 2010, pp.173-176.

网络空间的秩序必须建立在全球性、普遍性和平等性等基本前提之上，才能被所有行为体认可和接受。奥巴马政府虽然也强调美国例外，但并不否认这一基本前提，认同在多方谈判的基础之上不断推进网络空间秩序的构建。也就是说，各国不仅应看到其他国家带来的风险，也要注意到己方行动对对方造成的安全威胁，对网络安全威胁的应对应基于国家之间在网络空间中深度纠缠(entanglement) 这一现实。① 特朗普政府对网络空间霸权的重视大于对稳定性的重视，过度强调自身“受害者”的身份，忽视了美国才是最大的监听大国并不断推动网络空间军事化来威胁他国国家安全的事实。这种偏颇的认知和战略思想不仅拉大了美国自身对网络安全的认知与他国对美国认知之间的差距，而且使得已经具有强大实力的网络安全机构更加放任自流、不加约束，这无论是对美国国内政策还是对网络空间国际秩序都将带来极大的破坏性，急剧提升大国之间的冲突风险。

在网络空间治理进程中，美国不仅不积极，还试图以意识形态划线，抛开国际社会的共同努力，构建所谓“理念一致国家”联盟，加强盟友之间在网络军事领域的合作，加剧网络空间的分裂，甚至是催生阵营化的对抗。② 这种做法对原本已经较为脆弱的构建网络空间秩序的努力带来伤害，影响了网络空间的稳定和秩序。网络空间秩序失范还会进一步威胁经济发展。数字经济正在成为全球经济转型的新范式，构建数字经济规则是国际社会面临的共同任务。网络安全与数字经济发展之间存在着辩证的关系，过度追求自身网络安全会陷入封闭的数字经济体系。③ 网络空间的主权疆界模糊，互联网是全球一体的，数据是全球流通的，主权国家特别是网络大国的行为的外部性很大。如果美国开展大规模网络监听，无论是基于美国的互联网企业，还是通过流经美国的光缆，都会成为美国获取他国信息的渠道，这将迫使其他国家不得不采取更加严格的数据本地化措施，从而进一步增加全球网络空间“巴尔干化”的风险。

五　结论

保守主义网络安全战略的形成是美国国内政治与网络安全风险认知互动的结果，

① Scott Warren, Martin Libicki and Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica: RAND Corporation, 2016, pp.15-30.

② 鲁传颖《网络空间大国关系面临的安全困境、错误知觉和路径选择——以中欧网络合作为例》，载《欧洲研究》，2019 年第 2 期，第 113—118 页。

③ 方芳、杨剑《网络空间国际规则: 问题、态势与中国角色》，载《厦门大学学报(哲学社会科学版) 》，第 22—32 页。

站在美国政府的角度有其自身的逻辑。但是美国作为网络空间中实力最强大的国家，其战略和政策对于全球网络安全整体形势、网络空间秩序构建具有举足轻重的影响。① 保守主义网络安全战略在一定程度上试图打破现有国际政治体系对国家网络行动的约束，最大限度发挥美国在网络实力上的优势。这导致国际网络安全中外交与国际法不断式微，网络军事、情报等强力机构在网络空间秩序构建的影响力不断增加。

保守主义试图追求绝对的网络安全，引起了对于网络空间的“巴尔干化”的种种担忧。美国对俄罗斯采取的“持续交手”行动使俄罗斯更加坚决地维护网络主权。俄罗斯开始测试在断开互联网的情况下建立自身“主权互联网”的可能性，并呼吁在金砖国家之间建立独立的“互联网”。② 如果说“逻辑层面”的互联网分裂还只是一种实验和在做“最坏的打算”，数据层面的网络空间分裂则在斯诺登事件后就已经开始。欧盟出台了《通用数据保护规则》(GDPR)，最大程度展示了欧盟的数字主权。中国也正在加紧制定《个人信息和重要数据出境安全评估办法》。随着越来越多的国家开始提出数据主权战略，网络空间的数据本地化只会愈演愈烈。然而，保守主义网络安全战略最大的影响是让网络空间在物理层面产生了裂缝。特朗普政府试图重塑 ICT 全球创新体系和供应链体系，有可能在硬件层面产生两个生态系统，从而加剧物理层面的“巴尔干化”。

对此，国际社会只能将更多的希望寄托在网络安全技术的突破上，通过更加安全、有韧性的信息通信技术改变人们对于网络安全的认知，以更加理性、务实的态度来看待网络安全问题，把重心放到发展、繁荣一端，这才是网络空间真正的价值所在。无论是中国发布的《携手共建网络空间命运共同体》概念文件，还是西方国家倡议的《数字日内瓦公约》《网络空间信任宪章》《网络空间信任和安全巴黎倡议》，都在大力呼吁建立更加安全的互联网，认识到网络空间中信任、安全和稳定重要性，欢迎各国政府、私营部门和公民社会合作，增强数字流程、产品和服务安全性的倡议，制定使基础设施和相关组织得以强化网络保护的网络安全新标准。③

(截稿：2019 年 12 月　责任编辑：郭　枭)

① 张腾军《特朗普政府网络安全政策调整特点分析》，载《国际观察》，2018 年第 3 期，第 67—69 页。

② Jane Wakefield, “Russia ‘Successfully Tests’ Its Unplugged Internet,” BBC, December 24, 2019, https://www.bbc.com/news/technology-50902496，访问时间：2019 年 11 月 26 日。

③ Kate Conger, “Microsoft Calls for Establishment of a Digital Geneva Convention,” Tech Crunch, February 14, 2017, https://techcrunch.com/2017/02/14/microsoft-calls-for-establishment-of-a-digital-geneva-convention/，访问时间：2019 年 11 月 26 日。

trend for a long time, but from 2016 to 2018, Sino-Australian relations have declined by a large margin, which is mainly the result of Australia's political behavior. Under the circumstances that China does not pose a security threat to Australia, the economic cooperation between the two sides has brought great economic benefits to Australia, and China is willing to continue to develop Sino-Australian relations. The turn in Australia's attitude towards China from 2016 to 2017 is unusual. This paper holds that the main reason for the change in Australia's attitude towards China is not the strategic pressure of the United States on Australia, but that Australia attaches great importance to the stability of the international order under the increasing uncertainty of the international system. Australia regards China as a major country that may impact on the stability of the existing rules-based international order. With the Trump administration adopting a series of measures to impact on the stability of the existing international order, especially the stability of the existing international economic and trade order, in 2018, Australia has changed its understanding as to which country is the greater challenge to the international order. Its policy towards China has also been adjusted accordingly, resulting in new opportunities for the development of Sino-Australian relations. The analysis of this paper is helpful to get a better understanding of the international behavior of some middle powers with beneficial security and economic environment, and provides different approach to thinking for the improvement of Sino-Australian relations.

【Key Words】international order, Sino-Australian relations, US-Australia alliance, threat cognition

【Author】Zhou Fangyin, Professor, School of International Relations, Guangdong University of Foreign Studies.

The Return of Conservatism and the Transition of Trump Administration's Cybersecurity Strategy

Lu Chuanying (60)

【Abstract】When Donald Trump became the president, the return of conservatism led the transition of the US cybersecurity strategy, and guided the formation of "whole of

government" cybersecurity policies. The conservative cybersecurity strategy has evolved based on two major dynamics: one is top-down adjustment of the "America First" and traditional republican conservatism, and another one is bottom up of the "election meddling" event. The characteristics of the conservative cyber strategy includes: assertive cyber force doctrine like persistent engagement and defense forward, which try to break the constrain of the sovereignty, and expand their cyber operations into other states; dysfunctional cyber diplomacy, which includes the suspension of the US cyber dialogues with other major powers and a negative attitude toward cyberspace global governance; enhancing the DHS's role in cybersecurity protections; embracing the ICT policy in the cybersecurity strategy and the big power competitions in assuring the supply chains. While it is still too early to judge whether the conservative cybersecurity strategy can achieve the expected benefits, it has already brought about negative effects on the US and global cybersecurity. The unilateralism drags the US into double cybersecurity dilemma: offensive cyber operations increases big power conflicts, while diminishing efforts toward cyber diplomacy and global governance make the cyberspace even more disorderly.

【Key Words】conservatism, persistent engagement, defense forward, cybersecurity strategy

【Author】Lu Chuanying, Senior Fellow and Director of Research Center of Global Cyberspace Governance, SIIS.

The Development of International Relations Theories in Europe and Sino-Euro Dialogue

【Italy】Mario Telò (80)

【Abstract】The roots of European International Relations (IR) theory lie not only in the paradigm of realism, but also in the thoughts of Christianity, liberalism and Marx. With the development of European integration, the principle of realism has been directly, deeply and fundamentally questioned in Western Europe, which is conducive to