《国际政治研究》(双月刊)2018 年 第 1 期

网络地缘政治:中美关系分析的新视角

蔡翠红

内容提要 网络空间正在成为新一轮地缘政治博弈的大舞台,网络地缘政治成为大国博弈的一个分析视角。网络空间组成架构的地缘属性、网络空间活动主体的地缘属性以及主权国家在网络空间日益上升的权力,都构建了网络空间的地缘政治属性。中美关系中的网络地缘政治逻辑包括六大方面:地缘政治思维构建网络安全话语和政策、网络空间人造壁垒与地缘政治空间的重合、网络主权问题强化传统地缘政治理论、网络空间权力争夺重现地缘政治竞争、网络军事化趋势加强地缘政治冲突风险、网络问题逐渐被纳入传统地缘政治格局。由美国引导的大国网络博弈的地缘政治趋势对全球网络安全形势形成了威胁,中国应与各国携手,超越地缘政治并推进“网络空间命运共同体”建设。

关键词 世界政治 网络空间 网络安全 地缘政治 网络地缘政治 “网络空间命运共同体”

在国际政治理论中,地缘政治学占据了非常重要的一席。海权论、陆权

* 蔡翠红:复旦大学美国研究中心教授。(邮编:200433)

** 本文为笔者主持的教育部国别与区域研究课题《美国与网络空间全球治理研究》的成果之一,衷心感谢《国际政治研究》杂志匿名专家的宝贵意见,文中不足与疏漏之处由笔者负责。

论、空权论和天权论等理论流派都属于经典的地缘政治理论。但是,20 世纪 90 年代冷战的结束曾带来了“历史的终结”的说法,[①]加上互联网的全球连通性,有学者认为传统概念的国家和地缘政治已经过时,[②]将网络空间和地缘政治结合在一起研究似乎不太切合实际。这种想法并非毫无根据,因为在大多数人看来,一方面,网络改变了时空距离,信息在网络空间的流动是跨越传统国界的;另一方面,网络空间的一些机制和网络空间利益也同样超越了国家界限,网络空间的国家主权分界线似乎变得模糊,权力也开始分散。此外,互联网发展的早期,技术精英主导了网络空间治理规范,国家政府基本采取的是自由放任的态度,进而使得乐观主义者认为网络空间应该是不受政府管制的空间,并认为网络空间属于“全球公域”,地缘政治概念也不适用于网络空间。

然而,随着近些年的几件重要网络事件的出现,如斯诺登揭露的“棱镜门事件”、中美之间网络攻击的相互指责,地缘政治概念开始慢慢重新回到西方网络空间研究中,学术界关于网络空间地缘政治的各种研讨也开始展开。[③] 一些政策变动也佐证了这样的变化。例如,2015 年美国国家安全战略将大国威胁重新取代恐怖主义成为美国国家安全战略的首要考虑,代表着非传统安全威胁向传统的地缘政治安全威胁的回归。同时,网络威胁也被列在太空安全以及海天安全之前,成为共享空间威胁的首要考虑。[④] 在 2016 年 11 月 1 日英国政府发布的《国家网络安全战略》中,以往所强调的网络空间治理的公私合作关系明显被政府主导所替代。[⑤] 在这样的背景下,有学者认为网络空间大国博弈出现了地缘政治回归现象。也正是因为这一原因,才使得普遍存在的网络安全问题在传统地缘政治竞争对手之间才显得如此突出。换言之,只有地缘政治对手之间的网络问题才会成为冲突点。

---

① Francis Fukuyama, *The End of History and the Last Man*, New York: Maxwell Macmillan International, 1992.

② Andre Ishii, *Geopolitics, the State, and Cybersecurity in a Globalized World*, March 13, 2016, https://www.geopoliticalmonitor.com/geopolitics-the-state-and-cybersecurity-in-a-globalized-world/, 2016-08-20.

③ 例如,笔者应邀参加了 2016 年 7 月 7 日在法国巴黎召开的“亚洲的网络空间地缘政治”(Geopolitics of Cyber in Asia)研讨会。

④ *National Security Strategy*, February 2015, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf, 2016-08-20.

⑤ 这一观点是笔者 2016 年 11 月 14 日就当时英国刚发布的《国家网络安全战略》对英国卡迪夫大学(Cardiff University)从事网络与国际关系研究的马德琳·卡尔(Madeline Carr)教授的采访观点。卡尔教授认为,这是这一战略最明显的一个转变。

本文旨在分析地缘政治在网络空间的适用性，剖析中美博弈中的网络地缘政治现象与逻辑，进而对中国与各国携手，超越地缘政治并推进“网络空间命运共同体”构想与实践进行探讨。

一、网络地缘政治的提出

传统的经典地缘政治学者一般认为：地缘政治学（Geopolitics）研究的是大国的强权政治与其实施的地理范围之间的关系的学问，是“从空间或地理视角出发的国际关系研究”。[①] 按照《大不列颠百科全书》的解释，地缘政治是关于国际政治中地理位置对各国政治相互关系如何发生影响的分析研究，涉及的因素包括国家利益、海上交通线以及战略要地等。[②] 美国地缘政治学家尼古拉斯·斯皮克曼（Nicholas John Spykman）给地缘政治下的定义是“基于地理因素考虑制定一个国家的安全政策规划”。[③] 美国战略家兹比格纽·布热津斯基（Zbigniew Brzezinski）认为：“地缘政治是指那些决定一个国家或地区情况的地理因素和政治因素的相互结合，强调地理对政治的影响。”[④]

一般认为，地缘政治是国家安全与战略的基础。由于在人类社会发展的不同时期交往的内容方式不同，地缘政治呈现不同的阶段性，因而地缘政治学是一种动态发展、与时俱进的理论。有学者认为现代地缘政治学可分为五个发展阶段：争夺帝国霸权、德国地缘政治学、美国地缘政治学、冷战—国家中心与普遍主义的地理学视角、后冷战时代。[⑤] 不同时期、不同学者对地缘政治的理解不同，因此产生了不同的理论，。从马汉（Alfred Thayer Mahan）的海权理论、麦金德（Halford Mackinder）的大陆心脏说到豪雪弗（Karl Haushofer）的生存空间论，从杜黑（Giulio Douhet）的“空权论”到斯皮克曼（Nicholas John Spykman）的“边缘地带论”，从布热津斯基的大棋局和基辛格的大外交到跨世纪的批判性地缘政治学理论，地缘政治学经历了繁荣—低迷—复兴的历史发

① Geoffrey Parker, *Geopolitics: Past, Present, and Future*, London: Pinter, 1998, p. 5.

② 《简明大不列颠百科全书》，北京：中国大百科全书出版社 1998 年版，第 596 页。

③ 〔美〕尼古拉斯·斯皮克曼：《和平地理学》，俞海杰译，上海人民出版社 2016 年版，第 6 页。

④ 〔美〕兹比格纽·布热津斯基：《竞赛方案：进行美苏竞争的地缘战略纲领》，刘晓明等译，北京：中国对外翻译出版公司 1988 年版，第 6 页。

⑤ 〔美〕索尔·科恩：《地缘政治学：国际关系的地理学》，严春松译，上海社会科学院出版社 2011 年版，第 15 页。

展过程。[①] 后冷战时代出现了批判性地缘政治学、情感地缘政治、女性主义地缘政治等主题，但是国家、边境等仍为地缘政治的核心研究方向。[②]

在地缘政治理论中，“地理”不仅涉及国家、领土、边界等要素，还包括民族、资源、人口等要素，这些要素相互牵制相互影响。领土、边界勾画出国家的地理位置、国土形状和面积大小，而资源、人口等则决定着国家的经济权力、政治权力和未来发展的潜力。作为一项思考治国之术（statecraft）的研究，地缘政治学的中心议题是阐释国家在地理空间的权力关系。[③]

（一）网络空间作为地缘政治新领域之阐释

不可否认的是，与传统的陆海空不同的是，网络空间不是大自然的产物，而是人工构造的空间。网络空间突破了传统的地理空间的限制，模糊了传统的国家间地理边界，改变了以自然地理空间为依托的传统地缘政治思维，以往的守住自己的国家边境和天空就能拒敌于国门之外的安全思维受到挑战。但是，不应忘记的是，互联网的诞生本身就是地缘政治的产物，是冷战期间美苏地缘政治斗争的结果。美国曾希望借互联网的前身阿帕网（ARPANet）防止其信息指挥系统免受苏联的核攻击，互联网也因此被称为“冷战的孩子”。[④] 如今，网络空间虽然与最初的阿帕网有所区别，但是它依然具有地缘政治属性，是地缘政治的新领域。

首先，网络空间的地缘政治属性来源于网络空间组成架构的地缘属性。尽管互联网活动看似是个人的，但是却镶嵌在一系列物质基础架构、逻辑秩序以及法规制度中。[⑤] 虽然网络空间力量相比于其他形式的力量（如海洋太空力量）更具有无形特征，同时，信息作为网络空间力量的流通形式看似不可触摸的，但是产生信息、承载信息、传输信息和接受信息的硬件都具有物理属性。例如，链接网络空间的各种海底和陆地光缆、路由器、光纤、服务器、电脑、传感器、导航仪等等各种硬件，以及网络公司、研究机构以及计算机应急反应小组

① 潜旭明、倪世雄：《21 世纪新地缘政治和中美关系》，《美国问题研究》2007 年第 6 辑，第 21 页。

② 宋涛、陆大道等：《近 20 年国际地缘政治学的研究进展》，《地理学报》2016 年第 4 期，第 551—563 页。

③ 许勤华：《评批判性地缘政治学》，《世界经济与政治》2006 年第 1 期，第 15 页。

④ *Internet: A Cold War Baby*, http://www.historywiz.com/internet.htm, 2017-09-22.

⑤ Ron Deibert, “The Geopolitics of Cyberspace After Snowden,” *Current History*, January 2015, p. 10.

（CERTs）等，都具有物理属性。海底光缆的铺设需要考虑许多地理和政治因素，如对跨洋距离的运算以控制成本，对各国过往船只的考虑以防行船对光缆的破坏。通讯卫星虽然在天空中，但其地面基站和发射器都是在地面上，确切地说，属于某一个国家的信号收发控制范围。数据中心也同样是有其物理设施并基于一定的物理地点，如需要靠近能够支持数千台电脑服务器运转的电力资源。[①] 而且，随着物联网时代的即将到来，网络空间的物理基础设施的地缘政治特性将更加明显。

其次，网络空间的地缘政治属性来源于网络空间活动主体的地缘属性。不仅网络空间的许多组成架构都具有地缘属性，而且网络空间的活动主体也有地缘属性，网络力量的使用仍与地缘背景相关。地缘政治属性常可用来分析网络空间行为体的身份、动机与意图。[②] 网络空间设施运行者、使用者、管理者、得益者（受害者）都是基于被物理区隔的现实地缘政治空间。美国麻省理工学院教授戴维·克拉克（David Clark）认为网络空间可以按照重要性递减分为四个层面：一是网络活动参与者，他们参与交流、产生信息、进行决策、执行计划；二是网络空间存储、传输和变化的信息；三是维持网络空间服务和运转的各种逻辑结构；四是支持逻辑结构的物理设施。其中网络活动参与者即人的重要性最大。[③] 人的层面也是社会层面，现实社会中的人还无法脱离传统地缘政治。即使是恐怖分子，也充分利用了网络空间的地缘政治特性来筹款或者招募成员，[④]如针对一些种族离散人权聚居区进行重点动员。大数据时代的到来也不会改变网络空间活动主体的地缘属性。大数据的重要构成部分社交媒体、云计算、移动互联中，[⑤]社交媒体和移动互联的活动主体都是从属于一定的地缘政治空间的人。

再次，网络空间的地缘政治属性还来源于主权国家在网络空间日益上升

---

① John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," *American Foreign Policy Interests*, Vol.36, No.5, 2014, p. 288.

② Ibid., p. 286.

③ David Clark, "Characterizing Cyberspace: Past, Present and Future," *MIT/CSAIL Working Paper*, March 12, 2010, p.1.

④ Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges*, Washington, D. C.: United States Institute of Peace Press, 2006.

⑤ Ron Deibert, "The Geopolitics of Cyberspace After Snowden," p. 9.

的权力。国家日渐增长的权力与影响力是网络空间未来最重要的三个趋势之一。[①] 虽然互联网发展的早期，国家政府基本采取的是自由放任的态度，相应政策规范也较少。因此，一些乐观主义者一度认为互联网是一种脱离政府管制的特殊技术。但是，对人们生活影响巨大的任何事物最后都必须接受政府的管制。[②] 网络带来的全球化虽然可能在某些方面改变了国家安全工具，但是事实上国家通过各种手段维持甚至加强了其对内对外的主权。[③] 正如瑞普斯曼(Norrin M. Ripsman)和保罗(T. V. Paul)两位学者所指出的，关于全球化所带来的国家边界的过时论被夸大，特别是在国家安全方面。[④] 国家是一个适应力很强的机制，其弹性足以应对各种社会的、地区的和全球的变化。而且，不论国家的应对措施多么不完善，国家在网络安全中的地位无法替代，因为只有国家才会最在意网络空间发展带来的政治风险，而政治稳定又是社会和经济稳定发展的前提。物理概念的国家边境的本质是划分了“内部稳定”与“外部干扰因素”的界限。[⑤] 从这个角度看，信息边疆同样是国家致力于安全防范的新的国家疆域。所以，国家会动用国家力量来应对网络威胁，同时网络战争也逐渐浮现出来，而网络战是最能体现网络空间地缘政治性的趋势之一。

地理环境是地缘政治理论架构的基础。网络空间虽然没有固定地缘和实体空间位置，但它可以通过对其他领域的影响改变地缘政治权力的重心。网络已经成为一个新的空间，而不再是传统四大领域的附属物。它既是一个独立的领域，又像一条无形的引线，把以往四大空间领域联结起来，构成多维之间互动互补的动态构造。这个新的网络空间看似非物质的、虚拟的，但是又在物质世界中无所不在。[⑥] 网络空间不再是一个信息自由交换的乌托邦的地盘，

① 网络空间未来最重要的三个趋势是：国家日渐增长的权力与影响力、大数据爆炸、网络人口向南转移。Ron Deibert, “The Geopolitics of Cyberspace After Snowden,” p. 9.

② Ron Deibert, “The Geopolitics of Cyberspace After Snowden,” p.10.

③ Andre Ishii, *Geopolitics, the State, and Cybersecurity in a Globalized World*, March 13, 2016, https://www.geopoliticalmonitor.com/geopolitics-the-state-and-cybersecurity-in-a-globalized-world/, 2016-08-20.

④ Norrin M. Ripsman and T. V. Paul, “Globalization and the National Security State: A Framework for Analysis,” *International Studies Review*, Vol.7, No.2, June, 2005, pp. 199-227.

⑤ Iulian F. Popa, “Cyber Geopolitics and Sovereignty: An Introductory Overview,” *National and International Security 2014*, published by Armed Forces Academy of General Milan Rastislav Štefánik, 2014, p. 414.

⑥ 张妍：《信息时代的地缘政治与“科技权”》，《现代国际关系》2001 年第 7 期，第 19 页。

而是地缘政治的新领域,网络空间博弈也与地缘政治无法脱离。[①] 网络空间也不再是一个全球公域(global commons),而最多只能算一个具有全球性的领域(global domain)。[②]网络空间的这些地缘政治特性不仅影响网络入口、网络速度、可靠性,而且影响着网络空间的全球治理,[③]并进而影响着各国之间的网络空间博弈的性质。

(二)网络地缘政治的产生

与以前对陆地、海洋、太空的争夺一样,一场对于网络空间的地缘政治争夺正在上演。[④] 虽然网络空间博弈中出现了许多非国家行为体,但是民族国家仍然是全球层面上最重要的政治行为体。互联网的最初设想是一个不受阻拦的通讯平台。然而,现实与这一设想越来越遥远。网络空间在国际地缘政治格局与国家安全中发挥着越来越重要的作用,各个国家行为体都在设法对信息获取、网络准入等等进行控制,网络空间某种程度上正在成为新一轮地缘政治博弈的大舞台,网络地缘政治初现端倪。[⑤]

西方学术界曾提出许多名词解释网络空间与地缘政治的关系。有学者称之为"信息地缘政治"(Information Geopolitics),认为 2014 年朝鲜对索尼公司的黑客攻击似乎模糊了政治和网络之间的界限,开启了信息地缘政治的时代。[⑥] 有学者称之为"网络控制的地缘政治"(Geopolitics of Internet Control),强调各个国家对于信息流动的控制之于主权以及世界稳定的重要性。[⑦] 有学者提出了"地缘政治 2.0"(Geopolitics 2.0)概念并指出其三个变化:国家到个

---

① Leonid Savin, "Cybergeopolitics: Emergent Set of Practices, Phenomenon and Discipline," December 29, 2014, http://www.geopolitica.ru/en/article/cybergeopolitics-emergent-set-practices-phenomenon-and-discipline#.V7Z9f0vqC1I, 2016-08-20.

② John B. Sheldon, "The Rise of Cyberpower," in John Baylis, James J. Wirtz, and Colin S. Gray, eds., *Strategy in the Contemporary World*, 4th ed., Oxford: Oxford University Press, 2013, pp. 310-311.

③ John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," p. 287.

④ Ron Deibert, "The Geopolitics of Cyberspace After Snowden," p. 9.

⑤ 王川:《网络地缘政治:定义、特征及其对中国西北边疆安全的影响》,《喀什师范学院学报》2012 年第 4 期,第 12 页。

⑥ Chris Bronk, "Cyber Threat: The Rise of Information Geopolitics," 2016, https://strategyconnections.com/cyber-threat-information-geopolitics/, 2016-08-20.

⑦ Ronald J. Deibert and Rafal Rohozinski, "The Geopolitics of Internet Control," *Conference Papers—International Studies Association*, 2007 Annual Meeting, pp. 1-38. 类似观点可见:Anthony Smith, *The Geopolitics of Information: How Western Culture Dominates the World*, New York: Oxford University Press, 1980.

人、物理世界到虚拟动员和虚拟力量、旧媒体到新媒体。[①] 有学者提出了“后现代地缘政治”(Postmodern Geopolitics),认为全球化、信息化以及风险社会的出现使得传统地缘政治向后现代地缘政治转变。[②] 更多的学者则提出了“网络地缘政治”(Cyber Geopolitics 或者 Geopolitics of Cyberspace)的概念。[③] 网络地缘政治强调网络空间作为一个独立的空间体系而成为地缘政治博弈的新领域,是继海权论、陆权论、空权论和天权论之后的一个新的地缘政治理论体系,是传统地缘政治在网络时代的继承和发展,其理论核心是“网络权”理论。[④]

网络地缘政治的理论支柱是地缘政治权力与网络技术的关系。作为影响地缘政治的活跃因素,技术对地缘政治的作用主要有两大途径。一是技术通过对国际政治经济关系的影响改变地缘政治;二是技术通过改变地理空间的性质及其政治意义,进而改变地缘政治。[⑤] 关于第二点,前文已经对网络空间的地缘政治性质进行了说明。其实,两条途径的核心都是技术如何通过权力形式影响地缘政治关系。前者是通过改变政治本身改变了地缘政治,后者则通过改变空间性质改变地缘政治。[⑥]同样,网络空间不仅是地缘政治竞争的新舞台,还是地缘政治的工具与力量。

网络空间对于地缘政治的意义首先在于网络力量可以作为权力工具来实现传统地缘政治目标。因为直接的军事打击成本日渐高昂,而且危险很大,国家将越来越多地利用网络力量来实现地缘政治目标。阿拉伯之春充分说明了网络技术和政治之间不可分割的联系。但最好的例子莫过于针对伊朗核设施的震网病毒。[⑦] 2009 到 2010 年期间,伊朗指责美国和以色列利用震网病毒攻击其核设施。随后作为报复,据报道,美国认为伊朗黑客发动了一场针对沙特阿拉伯国有沙美石油公司(Saudi Aramco)的大规模攻击,删除了其三万台电

① Matthew Fraser, “Geopolitics 2.0,” *ARI*(Real Insitituto Elcano), 144/2009, p. 3.

② Gearóid Ó Tuathail, “The Postmodern Geopolitical Condition: States, Statecraft, and Security at the Millennium,” *Annals of the Association of American Geographers*, Vol. 90, No. 1, March, 2000, p. 167.

③ Leonid Savin, “Cybergeopolitics: Emergent Set of Practices, Phenomenon and Discipline,” p. 9.

④ 王川:《网络地缘政治:定义、特征及其对中国西北边疆安全的影响》,第 14 页。

⑤ 陆俊元:《论地缘政治中的技术因素》,《国际关系学院学报》2005 年第 6 期,第 7 页。

⑥ 同上,第 8 页。

⑦ Ian Bremmer, “The Geopolitics of Cybersecurity,” January 12, 2011, http://foreignpolicy.com/2011/01/12/the-geopolitics-of-cybersecurity/, 2016-08-20.

脑上的关键公司数据。[①] 朝鲜被认为是2014年索尼电影公司黑客事件的幕后指使人。随后据称美国作为报复,攻击了朝鲜的网络并使之失效数天。此外,2007年爱沙尼亚指控俄罗斯对爱沙尼亚的黑客攻击、2008年格鲁吉亚指控俄罗斯对格鲁吉亚的黑客攻击等都可以说明网络力量已经越来越多地用来为传统地缘战略服务。

其次,以信息网络技术为基础的网络力量构成各国的综合国力基础,也成为争夺地缘政治权力的基本条件和竞争成败的决定性因素。网络力量改变几乎所有其他领域的博弈特点,改变了外交、经济、文化表达,成为了国家之间的竞争核心之一,[②]网络空间事实上成为技术大国有效控制实体领域的新工具。而且,网络行动可以运用到所有的战争领域:海洋、陆地、天空、太空和网络空间。网络行动是"指挥者武器库中的另一套工具。"[③]对信息的控制权不仅是一种新形式的权力,而且是一种驾驭其他形式的上层权力,制信息权已成为当代和今后地缘政治竞争的高端目标。[④] 任职于美国空军部队的研究人员罗伯特·李(Robert M. Lee)指出,网络力量对现代战争的作用与以前空中力量同样具有革命性意义,网络空间博弈决定了今后处于网络优势地位的程度。[⑤]正如地缘政治之前强调的海权、陆权和空权一样,网络权力是地缘政治主体之间新的地缘政治格局走向的核心要素之一。这也印证了长期以来地缘政治博弈的公式,即地缘政治主导权意味着对最前沿科技的掌握与对关键地区或区域的控制。

网络地缘政治与传统地缘政治相比,有继承但也有变化。"随着全球化时代的到来,全球网络结构的出现以及信息技术的发展与进步使地缘政治的内涵、外延以及逻辑上都出现了相关变化"。[⑥] 第一,地理空间位置的重要性相对降低。因为网络空间攻击只需要一条畅通的网线即可,与内陆、海洋地形或距离远近无关,实体的地理位置障碍作用基本可以忽略,取而代之的是,网络空

---

① Anett Madi-Nator, "Geopolitical Rivalries in Cyberspace," http://www.gatewayhouse.in/geopolitics-and-cyber-attack-in-ukraine/, 2016-08-20.

② John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," pp. 291-292.

③ Eric D. Trias and Bryan M. Bell, "Cyber This, Cyber That... So What?" *Air & Space Power Journal*, Spring, 2010, p. 91.

④ 陆俊元:《论地缘政治中的技术因素》,第10页。

⑤ Robert M. Lee, "The Interim Years of Cyberspace," *Air & Space Power Journal*, January-February 2013, p. 58.

⑥ 王勇:《信息技术的地缘政治影响探析》,《情报科学》2009年第4期,第593页。

间的拓扑关系成为网络地缘政治的新元素;第二,网络地缘政治博弈的非对称性和普及性。传统地缘政治的博弈主体往往是国家行为体,但网络地缘政治的博弈双方可以是现实中实力非对称的个人或组织。这一变化对传统的政治生态有着巨大的影响;第三,国土大小与国家实力的泛对称性消失。[①] 传统的国家综合实力指标体系中,国土面积大小是国家实力的重要象征,国土面积意味着战略纵深和缓冲生存空间的大小,国土大国等于实力强国。换言之,国土面积与国家综合实力呈现泛对称现象。然而,网络战争无战场的前后方之分,不需要军队调动、后勤保障等,因为不像传统战争那样需要战略纵深,国土与国家实力的泛对称性消失。

二、中美博弈中的网络地缘政治逻辑

一些西方学者认为,中美网络博弈开始超越"双边议题导向型"的关系,正在变成越来越具有地缘政治为导向的关系,地缘政治的传统逻辑基本都可以用于中美网络空间博弈,地缘政治框架在网络空间出现后依然适用。[②] 地缘政治在本质上是行为体通过控制空间而获取权力和利益的竞争,而竞争的关键在于对空间争夺能力的掌握。因此,地缘政治首先直观地表现为争夺空间的政治,而背后则是空间控制能力的竞争。[③] 同样,中美网络空间博弈不仅仅是对网络空间这一新的地缘政治空间的争夺,更是对网络空间控制能力、影响能力以及网络力量的综合竞争。中美网络空间的博弈本质上就是中美在其他领域的地缘政治博弈的延续,[④]地缘政治思维与逻辑在中美网络空间博弈中无处不在。

"斯诺登事件"是中美网络博弈的地缘政治回归思维的催化剂。"斯诺登事件"前,网络军事化及国家管控趋势已经存在,但是"斯诺登事件"给这种趋势添加了巨大动力。[⑤] 如果"斯诺登事件"之前,美国还能够因其所谓的"互联网自由"而居高临下,那么"斯诺登事件"则撕下了其面纱,揭露了美国在网络

① 王川:《网络地缘政治:定义、特征及其对中国西北边疆安全的影响》,第 13 页。

② Colin S. Gray, "In Defence of the Heartland: Sir Halford Mackinder and His Critics a Hundred Years On," *Comparative Strategy*, Vol.23, No.1, Spring, 2004, pp. 9-25.

③ 陆俊元:《论地缘政治中的技术因素》,第 7 页。

④ John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," p. 291.

⑤ Ron Deibert, "The Geopolitics of Cyberspace after Snowden," p. 15.

安全上双重标准的真面目。斯诺登所揭露的美国对其他国家甚至盟国的领导人的多方位监听,严重伤害了国家之间的网络空间互信,使得网络安全问题成为传统地缘政治的核心议题。中美在网络空间的紧张关系主要集中在几个方面:互联网治理、大规模监控以及网络军事化发展。[①] 这几个方面与地缘政治思维都密不可分。

传统地缘政治理论研究有两个视角:空间视角与权力视角。[②] 这两个视角是解读传统地缘政治理论的出发点,也是构建解读分析框架的基础。事实上,空间视角和权力视角也可以用来分析网络地缘政治博弈。中美博弈的网络地缘政治逻辑的下述六个方面可以分别归属于这两大视角及其结果,它们以立体形式呈现了中美关系的网络地缘政治模型:从空间视角看,中美网络空间壁垒与地缘政治空间的重合是事实,而网络主权的提出则从概念上了默认了网络空间的地缘政治性质;从权力视角看,不仅中美网络空间权力争夺重现地缘政治竞争,而且网络军事化趋势加强了地缘政治冲突风险。最后从结果视角看,在思想认识上,地缘政治思维构建了中美网络安全话语和政策;在权力格局上,网络问题逐渐被纳入传统地缘政治格局。

(一) 地缘政治思维构建中美网络安全话语和政策

网络安全话语虽然不是传统地缘政治的研究内容,但是网络安全话语直接影响着地缘政治的战略和政策选择。事实上,以奥图泰尔(Gearoid O. Tuathail)开创的批判地缘政治学中,[③]"话语"分析是很重要的地缘政治变量,他将地缘政治的两大要素即地理空间和政治权力话语化,突破了通常所理解的地缘政治学的西方中心视角和物质决定论倾向,[④]指出网络时代的大众传媒和市民社会也是生产地缘政治话语的主体,为网络时代的地缘政治研究提供了新视角。

中美网络安全话语无论是在两国国内还是两国之间都未跨越地缘政治

---

① Ron Deibert, "The Geopolitics of Cyberspace after Snowden," p. 13.

② 胡志丁、骆华松、葛岳静:《经典地缘政治理论研究视角及其对发展中国新地缘政治理论的启示》,《热带地理》2014 年第 2 期,第 184—190 页。

③ Gearoid O. Tuathail and John Agnew, "Geopolitics and Discourse: Practical Reasoning in American Foreign Policy," *Political Geography*, Vol.11, No.2, 1992, pp. 190-204.

④ 葛汉文:《批判地缘政治学的发展与地缘政治研究的未来》,《国际观察》2010 年第 4 期,第 42—48 页。

思维。

首先，中美的网络博弈未脱离国家安全利益、经济利益、政治意识形态、宗教信仰等传统地缘政治目的。而且，网络空间并未改变二者的地缘政治目标。正如 20 世纪上半叶美国的目标是维持其欧洲及太平洋强国地位一样，美国现在受同样的地缘政治思维的驱动，尽力保持其网络空间霸权的地位。[①] 中国近年来虽然网络空间发展迅速，国民经济、社会发展也深深得益于网络发展，但中国国家利益的优先次序也并未因此改变，国内政治稳定依然位于中国网络空间战略利益之首。[②]

其次，两国国内的网络安全话语被地缘政治所塑造。例如，美国的网络安全话语中所体现的脆弱性和威胁的安全化话语，[③]比如，对不对称性网络威胁的担忧，对竞争对手夺取优势的担心、对自身竞争能力的担忧，等等。最典型的莫过于“中国威胁论”，认为“对美国国家安全威胁最大的网络攻击来自中国”“中国的网络战能力对美军构成真正威胁”“中国军队是一系列高级持续性威胁黑客攻击的幕后操纵者”，等等。[④] 同样，中国的网络安全话语中使用最多的词语则是美国的网络霸权，甚至有学者认为互联网设计之初就融入了美国的霸权思维，并详细列举了美国网络霸权的实现路径。[⑤]

再次，两国网络脆弱性和安全事故常被解读为地缘政治原因。美国的网络安全地缘政治思维尤其严重。在 2015 年美国人事管理局（OPM）的网络黑客攻击事件中，不仅中国被美国认为是幕后指使者，而且虚构出这种可能的行为与中美在南中国海的冲突升级密切相关，甚至宣称是来自中国的“网络珍珠港”事件。[⑥] 2016 年初，美国学者对美国网络安全形势的预测首先想到的也是

① Noah Rothman, “The Cyber Pearl Harbor and the Inescapable Gravity of Geopolitics,” June 5, 2015, https://www.commentarymagazine.com/american-society/military/chinese-cyber-attack-geopolitics/, 2016-08-20.

② Cuihong Cai, “Cybersecurity in the Chinese Context: Changing Concepts, Vital Interests, and Prospects for Cooperation,” *China Quarterly of International Strategic Studies*, Vol.1, No.3, 2015, p.481.

③ John B. Sheldon, “Geopolitics and Cyber Power: Why Geography Still Matters,” p.286.

④ 蔡翠红：《美国网络空间先发制人战略的构建及其影响》，《国际问题研究》2014 年第 1 期，第 45—46 页。

⑤ 杜雁芸：《美国网络霸权实现的路径分析》，《太平洋学报》2016 年第 2 期，第 65—75 页。

⑥ Noah Rothman, “The Cyber Pearl Harbor and the Inescapable Gravity of Geopolitics.”

地缘政治性质的网络攻击,甚至认为2016年将是地缘政治网络攻击年。[①] 同时,美国在对这些网络安全事故解读时还有个独特现象,即将来自个人和来自政府支持的黑客攻击不加区分,硬是把可能来自中国的网络攻击都认为是有政府支持背景的。这种思维的背后显然是地缘政治思维在起作用。

网络安全话语是国家网络相关政策的构建基础。上述这些融入地缘政治思维的网络安全话语同样塑造了中美两国的网络政策,网络政策也逐渐与传统地缘政策相结合。经过研究比对可以发现,美国网络作战的重点与其国家安全战略的地缘政治中心基本一致。[②] 美国国防部2015年的《网络战略》将未来五年网络作战的重点放在中东、亚太和欧洲,并将中国、俄罗斯、伊朗和朝鲜等列为构成网络威胁的重点国家。[③] 在2015年的《美国军事战略》的第一部分战略环境分析中,俄罗斯、伊朗、朝鲜、中国被依次重点列出,并认为这些国家是对美国国家安全利益构成威胁的国家。[④] 二者的高度重合正说明了网络博弈的地缘政治化。

(二)中美网络空间壁垒与地缘政治空间的重合

虽然网络空间看似一个乌托邦式的全球通讯空间,信息跨越国界流动,人们跨越国界交流,但是学者们不无遗憾地看到如今的网络空间壁垒与传统地缘政治空间的重合趋势。这种重合来源于下述几个方面的解释:

第一,网络空间的物质基础架构无法脱离传统地缘政治空间。前面已经讲述过网络空间的物质基础架构基本分属各国领土。或许有人会说信息或者说数据是无法界定其来源地的。但是,随着技术的进步,数据也逐渐具备了地域属性。传统司法领域的"属人"和"属地"原则并不是完全不适用。"属人"原则是指根据数据来源或者数据主体来判断权利行使范围,当然"人"是指泛化

---

① Dan Holden, "Cybersecurity Predictions 2016: Expect Geopolitical Cyber Attacks in the Wake of the US Presidential Election and the Rio Olympics," January 5, 2016, http://www.cityam.com/231754/cybersecurity-predictions-2016-expect-geopolitical-cyber-attacks-in-the-wake-of-the-us-presidential-election-and-the-rio-olympics, 2016-08-20.

② 汪晓风:《美国网络安全战略调整与中美新型大国关系的构建》,《现代国际关系》2015年第6期,第20页。

③ U. S. Department of Defense, "The Department of Defense Cyber Strategy," April 15, 2015, p. 9.

④ U. S. Department of Defense, "2015 National Military Strategy of the United States of America," July 1, 2015, p. 2.

的对象，也可能是指物。“属地”原则是指根据数据存在的地理位置来判断。[①] 在“属人”和“属地”原则基础上的领域管辖原则、国籍管辖原则等都逐渐被用在跨界数据流动有关的犯罪行为管理。

第二，网络技术壁垒与地缘政治空间的重合。这体现在两方面：一是网络过滤技术和防火墙的应用。各国对于网络空间进入和信息的控制已经成为一种潜规则。网络技术的国内控制甚至被认为是一种“技术主权”（technological sovereignty）。[②] 数年前，针对中国的网络过滤，许多西方国家都持批评态度。但是，如今看来，许多当时批评中国的国家也开始应用过滤技术和防火墙，从而人为建立了基于 IP 地址的网络空间国家界限。[③] 其实，美国也有类似的网络过滤，只是过滤的内容不同而已。早在 2000 年，就有部分美国媒体披露了“食肉动物系统”，即美国司法部下属联邦调查局开发并使用的一套信息监控系统。而“9·11”之后，美国国会更是通过新法案并增加对“食肉动物系统”的拨款。[④] 防火墙应用的一个典型地缘政治结果是中美搜索引擎的分裂。谷歌和百度在中国市场的情形并认为是一种“搜索引擎的地缘政治”。[⑤] 两者的分裂不仅仅影响搜索引擎的使用者习惯，更是影响到市场份额、经济利益以及其中所蕴含的政治和文化价值观。这也导致了中美网络经济博弈相对被限制在各自的传统地缘政治领域。此外，中美常用社交媒体平台也不同，中国网民偏好使用微信，而脸书（Facebook）、谷歌（Google）、推特（Twitter）等社交媒体则在美国等西方国家被广泛使用；二是技术本土化趋势。“棱镜门事件”的一个附带效果是越来越多的网络安全技术和网络产品的本土化倾向。[⑥] 网络产品和技术在最初大部分是一些跨国公司进行开发的。然而，随着国家在网络空间利益的上升，各国开始投入更多的资金以开发自主知识产权的网络技术。国家开始更多介入原来属于私营企业的网络安全领域。火眼（FireEye）公司的首席执行官戴维·德沃（Dave DeWalt）表示，以前网络安全公司基本都是私营的，但是现在的趋势是，几乎所有大国都有国家支持甚至国家成立的安全公

① 蔡翠红：《云时代数据主权概念及其运用前景》，《现代国际关系》2013 年第 12 期，第 58—65 页。

② Ron Deibert, “The Geopolitics of Cyberspace After Snowden,” p.13.

③ Helas Vuo, “The Geopolitics of Networks,” December 10, 2015, https://www.liquidvpn.com/geopolitics-of-networks/, 2016-08-20.

④ 沈逸：《美国国家信息安全战略》，北京：时事出版社 2013 年版，第 184—187 页。

⑤ Shin Joung Yeo, “Geopolitics of Search: Google versus China?” *Media, Culture & Society*, May 2016, Vol.38, Issue 4, pp. 591-605.

⑥ Ian Bremmer, “The Geopolitics of Cybersecurity.”

司。所以，最后的博弈结果就是网络大国之间的优势争夺。[①]

第三，网络空间法规制度成为网络空间的人造地缘政治壁垒。虽然网络公司大多是私营企业，但是这些企业面临着越来越多的来自政府的压力。正如斯诺登所揭露的一样，大部分公司在政策法规、法庭传唤、国家安全函件、营业执照审核、利诱等正式或非正式压力下与政府合作。即使是在网络空间治理中举足轻重的跨国网络公司，也自觉地遵循地缘政治的逻辑。例如英国大东电报局(Cable & Wireless 公司，现在被 Vodafone 收购)据传从英国政府情报总部(The Government Communications Headquarters，GCHQ)获得数十亿英镑并因此同意在其系统内安装监控设备。[②] 当然有时政府也会利用隐密手段，例如美国国家安全局(NSA)有足够的技术以黑客方式进入谷歌公司的数据库。中美两国对各自的网络空间设立了各种规章制度和机构以加强对本国网络空间事务的管理。2009 年 5 月，奥巴马宣布在白宫设立网络安全办公室，并任命一名网络安全协调主管。中国也于 2014 年 2 月成立了中央网络安全和信息化领导小组以及相应的中央网信办。最有代表性的制度壁垒则是网络审查制度。美国众议院情报委员会于 2011 年对中兴、华为进行特别调查并发布调查报告，最后中兴、华为不得已退出美国市场。2013 年，美国国会通过的《2013 财年综合继续拨款法》又限制美四家政府部门购买中国企业生产的信息技术设备。[③] 中国也在信息安全产品认证制度的基础上被迫思考如何进一步推进网络安全审查制度。2017 年 5 月，国家互联网信息办公室公布了《网络产品和服务安全审查办法(试行)》，[④]并已于同年 6 月 1 日开始实施。依据该办法，国家网信办会同有关部门成立了中国首个网络安全审查委员会。

第四，中美语言的天然差异也造就了中美网络空间的语言壁垒。虽然网络空间发展使得全球交流异常便利，中美两国通晓对方语言的人数也在增加，但是，对于大部分民众来说，中美语言的天然差异也是中美网络空间地缘政治分裂难以弥合的语言壁垒。也就是说，母语为中文的人群的网络浏览内容以

---

① Danny Yadron，“When Cybersecurity Meets Geopolitics，” March 23，2015，http://blogs.wsj.com/digits/2015/03/23/when-cybersecurity-meets-geopolitics/，2016-08-20.

② Ron Deibert，“The Geopolitics of Cyberspace after Snowden，” p. 11.

③ 左晓栋：《近年中美网络安全贸易纠纷回顾及其对网络安全审查制度的启示》，《中国信息安全》2014 年第 8 期，第 69—72 页。

④ 《网络产品和服务安全审查办法(试行)》，2017 年 5 月 2 日，http://www.cac.gov.cn/2017-05/02/c_1120904567.htm，2017-09-20。

中文为主,母语为英文的同样则以英文为主。即使都是用英语,各国的媒体的受众也基本集中在本国国内。《中国日报》英文网站 98.3%的用户来自中国国内,美国用户仅占 0.4%。《华盛顿邮报》网站 78.9%用户来自美国本土,2.1%来自英国,2.0%来自中国,1.9%来自加拿大,1.4%来自印度。[①] 可见,各国国民浏览的网络内容基本以本国语言和本国产生的内容为主。这些因素都造就了网络空间无形的地缘政治壁垒。

(三) 网络主权的提出与传统地缘政治印象

在西方语境中,中国所倡导的"网络主权"概念被认为是对传统地缘政治理论在网络空间的延伸,因为主权理论是传统地缘政治学的支柱之一,而民族国家是地缘政治结构的重要方面。[②] 网络空间的出现促进了一种新型国家主权即网络主权的出现。[③] 主权的涵义其实是一个国家保障其政治、经济、军事的安全、稳定与发展的权力。在网络信息时代,国家主权的概念已经悄悄发生了变化。"网络主权"成为国家主权概念中的重要内容,从而扩大了国家主权的外延。

网络空间是否拥有主权在国际上早有定论。2003 年,联合国提议召开的信息社会世界峰会早就明确指出了"制定与互联网相关的公共政策属于一国主权范围"。2013 年 6 月,联合国大会通过的"从国际安全的角度来看信息和电信领域发展政府专家组"的第三次报告决议中也有相关内容:"国家主权和源自主权的国际规范和原则适用于国家进行的信息通讯技术活动,以及国家在其领土内对信息通讯技术基础设施的管辖权。" 2015 年 7 月,这一政府专家组再次在发布的报告中指出"尊重各国在网络空间的主权"。这说明在联合国层面"网络主权"理念已被认可和接受。此外,"网络犯罪公约"也认为民族国家对其领土内的网络进入有规制、限制等主权权力。

中国提出"网络主权"只是重申了联合国和国际层面的立场。中国国务院新闻办公室早在 2010 年 6 月发布的首份《中国互联网状况》白皮书就提出了"中国境内的互联网属于中国主权管辖范围,中国的互联网主权应受到尊重和维护"。2014 年 7 月,习近平主席访巴西期间在演讲中阐述了中国对于信息主

① 数据来源于 Alexa 网站:http://www.alexa.com,2016-09-12。

② 〔美〕索尔·科恩:《地缘政治学:国际关系的地理学》,第 38 页。

③ Iulian F. Popa, "Cyber Geopolitics and Sovereignty: An Introductory Overview," pp. 413-417.

权的看法:“虽然互联网具有高度全球化的特征,但每一个国家在信息领域的主权权益都不应受到侵犯,互联网技术再发展也不能侵犯他国的信息主权”。2014 年 11 月,习近平同志在致首届世界互联网大会开幕式贺词中郑重呼吁国际社会“尊重网络主权、维护网络安全”。2015 年 12 月,国家主席习近平在第二届世界互联网大会上再次提出“互联网治理四项原则”,其中第一条即是尊重网络主权。而 2015 年 7 月 1 日颁布实施的新版《中华人民共和国国家安全法》中第一次明确提出“网络主权”概念,主张要“维护国家网络主权”,从而以法制形式表明了中国的原则立场。

美国官方从未表态赞成“网络主权”,因为这和他们主张的网络自由相悖。然而,美国民间也不乏对网络主权概念的拥护。2016 年 2 月 29 日,美国智库战略与国际研究中心举办了题为“中国的‘网络主权’提议:起源与影响”的专题研讨会。该中心资深副主任与战略技术项目主管刘易斯(James Andrew Lewis)博士表示,互联网治理理应被纳入国家主权的适用范围。事实上,尽管美国官方没有表态,美国政府的许多做法依然体现了主权思想。如制定各种法律法政策规范来对其网络空间进行管理,同时制定国家行动计划等。2016 年 2 月 9 日,奥巴马总统宣称,在对网络安全环境进行了七年的观察之后,决定推行“网络安全国家行动计划”(Cybersecurity National Action Plan,CNAP)。[①] 2017 年 5 月 11 日,美国总统特朗普也签署了一项期待已久的“关于加强联邦政府网络和基础设施网络安全的总统行政命令”,[②]这项行政命令列出了特朗普政府的三项优先任务:保护联邦政府的网络、升级已经老化过时的系统和保护美国民众的网络安全。事实上,国家政府对内通过建立和完善网络监管的法律和制度体系,对外通过发展网络空间攻防、制定网络安全战略,从而以主权内部性和外部性的重构推动了网络空间再主权化的事实。[③]

(四)中美网络空间权力争夺重现地缘政治竞争

网络地缘政治的理论支柱在于网络与地缘政治权力的关系。网络不仅对

---

① “Fact Sheet: Cybersecurity National Action Plan,” http://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, 2016-09-02.

② The White House, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” May 11, 2017, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal, 2017-09-22.

③ 刘杨钺、杨一心:《网络空间“再主权化”与国际网络治理的未来》,《国际论坛》2013 年第 6 期,第 1—7 页。

传统权力工具有变革性影响，而且网络权力本身也可用来实现传统地缘政治目标。因此，网络空间权力的争夺成为又一地缘政治竞争内容。中美地缘政治竞争同样体现在双方对网络空间权力的争夺，主要体现为以下几方面：

第一，大数据资源的争夺服务于地缘政治目标。网络空间大数据蕴含着许多社会、政治、文化甚至国防信息，对于大数据的争夺可以发现一些战略优先信息，从而服务于其地缘政治目标。大数据时代已经来临，大数据将成为21世纪国际关系的新挑战和新竞争领域。[①] 如“棱镜门事件”所揭示的一样，美国借助其网络公司的全球业务范围与能力在全球收集数据，展开大数据的角逐，并在某种程度上成为了“地缘信息帝国”(geoinformational empires)。在这里，传统的世界政治空间和各种电子网络和数据节点共同构建了真实的社会空间。[②] 美国政府2012年投资大量资金启动了《大数据研究和发展计划》。对于信息和数据的管理和操控已经成为至关重要的地缘政治实践。中国于2015年8月19日的国务院常务会议通过了《关于促进大数据发展的行动纲要》(以下简称《行动纲要》)并2015年于9月5日正式发布。[③]《行动纲要》是到目前为止我国促进大数据发展的第一份权威性、系统性文件。2015年11月发布的《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》进一步强调了推进数据资源开放共享，实施国家大数据战略。[④] 这些都显示大数据发展和竞争达到了国家战略全局的高度。

第二，网络外交创造地缘政治新平台。美国在外交中尽显其网络优势，如在伊朗建立虚拟大使馆等以进行文化宣传、心理攻势等。而中国则是美国网络外交尤其是运用社交媒体开展外交的重点对象，美国国务院及其驻华使团展开各种信息发布和与中国公众互动的活动，意在传递信息、监测舆情、引导舆论，呈现出全面覆盖、中文内容、直面公众、潜移默化等特点。[⑤] 许多词语可用来形容这一倾向，如数字外交(digital diplomacy)、互联网外交(Internet diplomacy)、推特外交(Twitter diplomacy)等等。中国也在网络外交领域积极

① 蔡翠红：《国际关系中的大数据变革及其挑战》，《世界经济与政治》2014年第5期，第124—143页。

② Gearóid Ó Tuathail, “The Postmodern Geopolitical Condition: States, Statecraft, and Security at the Millennium,” p. 171.

③ 《国务院关于印发促进大数据发展行动纲要的通知》，2015年8月31日，http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm，2017-09-22。

④ 《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》，2015年10月29日，http://cpc.people.com.cn/n/2015/1103/c399243-27772351.html，2017-09-22。

⑤ 汪晓风：《社交媒体在美国对华外交中的运用》，《美国研究》2014年第1期，第47—62页。

推进。如美国对外关系委员会研究员亚当·西格尔(Adam Segal)撰文指出,在习近平主席的领导下,中国已经开始改变过去在网络空间全球治理中的防御性和反应性的相对立场,而代之以更加积极的网络外交。他还分析了中国的网络外交三大目标,除了控制可能威胁政治稳定的网络信息和利用网络空间拓展中国各方面影响力外,专门提到了对抗美国在网络空间的优势以及提升中国的操作空间这一目的。① 虽然他的观察不一定准确,但是却反映了中美在网络外交方面的较量。一方面,中美两国在尽力发展电子政府,在政府和民众之间建立网络形式的管理,在网络空间强化政府的角色;另一方面,中美两国都利用网络作为政治文化的宣传工具。

第三,中美网络间谍的争议延续了地缘政治竞争。2014 年 5 月,美国政府以五名中国军人涉嫌通过网络从六家美国企业窃取机密信息为由,对其进行起诉,使中美间谍问题重回两国博弈的聚焦镜中。间谍活动古已有之,各国多少都有间谍活动的介入。间谍活动是指一国在另一国不知情和未许可的情况下通过侦察、偷窃、监视等秘密方式从该国获取军事、政治、经济及其他机密信息的行为。各国也都难以摆脱网络途径这一非常有诱惑力的间谍手段。某种程度上,各国网络间谍活动的开展成为了地缘政治竞争的重要内容。②然而,在网络间谍问题上,美国作为该领域唯一的超级大国,却对经济间谍与其他间谍行为加以区别,认为经济网络间谍应当受到禁止,而其他网络间谍行为则不受规制。事实上,经济间谍并未在国际法上受到区别对待,无论是在世界贸易组织法还是其他现有国际法上也都找不到依据。③美国的起诉带来的直接后果是中国政府决定中止中美网络工作组活动,中美网络空间关系一度紧张。

第四,网络治理权力的争夺是中美之间新的地缘政治斗争形式。两国之间针对网络治理的分歧与权力争夺一直在继续,“在网络治理问题上也出现了地缘政治现象”。④ 网络发展早期,网络治理基本是非正式的形式,并由非国家行为体所主导。但是政府越来越多地开始介入,有关网络空间的话题也越来

---

① Adam Segal, “Chinese Cyber Diplomacy in A New Era Of Uncertainty,” June 2, 2017, http://www.hoover.org/research/chinese-cyber-diplomacy-new-era-uncertainty, 2017-09-22.

② Munish Sharma, “The Geopolitics of Cyber Espionage,” *Journal of Defence Studies*, Vol.9, No.1, January-March 2015, pp.83-101.

③ 黄志雄:《论间谍活动的国际法规制:兼评 2014 年美国起诉中国军人事件》,《当代法学》2015 年第 1 期,第 143—145 页。

④ Julien Nocetti, “The Complex Geopolitics of Internet Governance,” http://valdaiclub.com/opinion/highlights/the_complex_geopolitics_of_internet_governance/, 2016-08-20.

越多地在各种国际会议中成为政治斗争的内容。[①] 有西方学者认为，全球治理已经被地缘政治所取代，许多全球问题最后还是需要在地缘政治体系内解决，并不存在真正的全球治理模式。[②] 在互联网治理态度方面，主要有两类观点，一类主张政府有限作用的多利益攸关方模式，另一类主张由联合国牵头并由国家主导的多边主义模式。美国、英国等国家属于第一类；中国、俄罗斯等国家属于后一类；而一些新兴经济体如巴西、印度、印度尼西亚等则被认为是“摇摆国家”(Swing states)。[③] 尽管“斯诺登事件”使得第一类阵营被弱化，以美国为首的第一阵营和以中俄为代表的第二阵营之间的网络空间治理模式之争一直是这些年来网络空间全球治理竞争的重要内容。

(五) 网络军事化趋势加强地缘政治冲突风险

网络战被认为是最能体现网络空间地缘政治性的趋势之一。网络军事化代表了狭义的网络战趋势，即将网络发展为武器而应用到军事目的。网络战作为新的战争形式，在军事和政治领域开始被广泛运用。事实上，网络空间这一新的地缘政治领域频频上演各种广义上的网络战形式，如信息情报战、舆论民意战、文化和意识形态战、网络攻防战等等。但因篇幅有限，本文仅讨论狭义网络战。

网络军事化和武器化的加速发展加强了地缘政治冲突风险。互联网发展初期，人们对网络空间安全威胁来源的认知往往以蛰伏在暗处的某个黑客或犯罪组织为基本假想敌，这也就是巴里·布赞所指的“威胁代理”。然而，随着网络武器化和军事化趋势的出现，以及媒体对这些事态的进一步宣传，网络威胁的主观建构由模糊的、超国家的非传统安全概念向具体的、以国家性为内涵的传统安全概念转变，[④]民族国家间的地缘政治敌我身份认同在网络空间也进一步被明确。

世界各国都相继在做网络战的准备。[⑤] 联合国裁军研究所早在 2013 年的

① Ron Deibert, “The Geopolitics of Cyberspace After Snowden,” p. 13.

② Stewart Patrick and Isabella Bennett, “Geopolitics Is Back and Global Governance Is Out,” May 12, 2015, http://nationalinterest.org/blog/the-buzz/geopolitics-back-global-governance-out-12868, 2016-08-20.

③ Ron Deibert, “The Geopolitics of Cyberspace After Snowden,” p. 13.

④ 刘杨钺、杨一心：《网络空间“再主权化”与国际网络治理的未来》，第 4 页。

⑤ Ron Deibert, “The Geopolitics of Cyberspace After Snowden,” p. 11.

调查数据显示,已有 46 个国家组建网络作战部队。在这轮网络军事化潮流中,美国可以说是领头羊。美国网络司令部的诞生可以作为美国的一个例证。美国将网络空间列为继海陆空天之后的第五大领域,并发展相应进攻性能力。2014 年 3 月 5 日,美国防部发布《四年防务评估报告》,在精简部队结构、实行国防投入"自动消减机制"的大背景下,明确提出"投资新扩展的网络能力,建设 133 支网络任务部队",引起世界担忧。美国总统特朗普 2017 年 8 月 18 日宣布,把战略司令部旗下的"网络司令部"升级为与战略司令部同级的第十个联合作战司令部。网络司令部的升级,意味着今后它将无需通过各相关军种,可直接指挥麾下所属各个军种部队,美军网络部队也因此成为一个独立军种。此举说明网络空间正式与海洋、陆地、天空和太空并列成为美军的第五战场。在该形势下,中国也不敢对此掉以轻心。2016 年 4 月 25 日,习近平主席在网络安全和信息化工作座谈会上的讲话中指出,中国需要增强网络安全防御能力和威慑能力。其中,网络威慑能力的提出的确也引起了外方对中国增强网络军备的猜测。

地缘政治思维决定了网络战争行为背后的逻辑。例如对于针对伊朗核设施的震网病毒(Struxnet)的来源,远离相关地缘政治博弈的国家,例如蒙古、乌干达或者希腊,都不可能被认为是背后的始作俑者。沙特阿拉伯和阿联酋等海湾阿拉伯国家虽与伊朗关系紧张,但是缺乏一定的技术能力。俄罗斯虽然有技术储备,但是与伊朗紧密的经济和商业联系则大大降低了这种可能性。[①] 而 1979 年以来伊朗和美国及以色列等邻国紧张的地缘政治关系则使之值得怀疑。尽管两国从未承认,但是有情报泄露了美国和以色列的一项耗资巨大的网络合作。[②] 因此,地缘政治决定了网络战的对象,网络战的目的也是用来实施传统地缘战略的工具。

网络战还往往和传统地缘政治的冲突热点相结合,作为其他地缘政治工具的补充。根据斯诺登披露的材料,美国情报部门曾对中国的高校、军队及政府机关发动过黑客攻击。2001 年"中美撞机事件"后,中美也上演了一场黑客大战。美国黑客组织不断袭击中国网站,中国一些黑客组织也积极进行"黑客

① John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," pp. 288-289.

② See Greg Miller and Sari Horwitz, "Justice Dept. Targets General in Leak Probe," *Washington Post*, June 27, 2013, http://www.washingtonpost.com/world/national-security/justice-dept-targets-general-in-leak-probe/2013/06/27/9ad8bc4e-df7c-11e2-b2d4-ea6d8f477a01_story.html, 2016-08-20.

反击战”。在“撞机事件”发生后的一段时间,中美两国网站上的黑客攻击事件数量陡然上升。这也因此称为中美黑客大战的经典案例。1999 年,中国驻南斯拉夫大使馆遭到以美国为首的北约轰炸后也发生了为期大约一周的中美黑客大战。网络攻击手段的便利性、快速性、廉价性等特点将使其在地缘政治冲突中的作用越来越大,也因此常成为民族主义的非理性工具。网络民族主义是“网络+民族主义”的结合体,是民族主义思潮在网络时代的最新表现。[①] 除互联网技术的发展与传统民族主义的继续发展外,网络民族主义的出现还受综合国力提升、国际环境变化、普通大众的政治参与性提高等深层原因影响。但就其本质而言,网络民族主义拓展了国家民族主义和族裔民族主义的表现平台,[②]是民族主义在网络空间的延伸与发展,它源于民族主义与全球化冲突,其实质是民族或国家之间利益关系在全球化过程中的相互影响和冲突,[③]因而也是传统地缘政治冲突在网络空间的表现形式。

此外,面对网络博弈,国家也可能会动用传统地缘政治手段进行回击。例如,美国国防部 2011 年出台的《网络空间行动战略》就指出,一些严重网络攻击行动将被视同为战争行为,美国将以传统的军事打击,包括使用导弹和其他高技术武器对敌对国家进行攻击。2015 年版的《网络空间战略》则公开表示,美国军方将把“网络战”用作针对敌人的作战方式,当美军在与敌人发生冲突时,可以考虑实施“网络战”。[④]

(六) 网络问题逐渐被纳入传统地缘政治格局

首先,网络问题被纳入到传统地缘政治盟友体系中。美国非常注重强化与同盟国家的网络空间合作。除联合同盟国家进行大规模的“网络风暴”演习外,美国格外注重加强与同盟国家的双边关系。在东亚,美国将网络问题纳入美日同盟、美韩同盟、美澳同盟,以所谓传统的“北锚”“南锚”加固对中国的网络地缘战略封锁线。2013 年 5 月,美日在东京举行首次“安全对话”,双方决定

① 葛素华:《国内网络民族主义研究:现状与问题》,《现代国际关系》2014 年第 4 期,第 57 页。

② 王军:《网络民族主义、市民社会与中国外交》,《世界经济与政治》2010 年第 10 期,第 142—147 页。

③ 葛素华:《国内网络民族主义研究:现状与问题》,第 58 页。

④ “The Department of Defense Cyber Strategy,” April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, 2016-08-20.

把网络安全作为美日双边关系的基石,把双边网络安全合作提高到极高的地位。[①] 在南亚,美国强化与东盟的网络关系,推进美印网络合作。2015 年 8 月美印网络对话之后,双方发布联合公告称,美印双方确定了在网络安全能力建设、网络安全技术研发、打击网络犯罪、国际网络安全及互联网治理等诸多方面的合作机会,并拟打造双方在网络安全方面的合作伙伴关系。[②] 在欧洲,美国则与北约联合对抗俄罗斯,将网络战纳入北约作战体系。2016 年 7 月,北约各成员国共同签署文件,同意将网络空间等同于海陆空的行动领域加以保护。[③]

在美国的网络空间地缘政治思维的刺激下,中国被迫开始在其外交平台中推进网络空间利益,网络问题成为上海合作组织、金砖国家、东盟的重要话题和讨论点。早在 2009 年,为了加强执法合作,上海合作组织成员国就签订了《上合组织成员国保障国际信息安全政府间合作协定》。2013 年 12 月在南非召开的金砖国家安全事务高级代表第四次会议则决定成立金砖国家网络安全问题工作组。2014 年 9 月,为了促进区域内的多边发展与合作,中国与缅甸、印度尼西亚、马来西亚等东盟十国达成了共建"中国—东盟信息港"的倡议。此外,网络问题也被纳入中国的一带一路周边建设规划中。"中国—东盟信息港"的目的之一就是使之成为建设 21 世纪"海上丝绸之路"的信息枢纽。[④] 作为落实"一带一路"倡议的具体措施,工业与信息化部还于 2014 年 11 月提出数字丝绸之路构想,其主要内容是促进一带一路沿线国家在数据信息服务、互联网业务和国际通信业务的互联互通。[⑤]

其次,网络空间力量分布没有逃出传统地缘政治格局。"一超多强"的全球网络空间格局出现。随着网络技术的迅猛发展,国际政治权力与利益的争

---

① Mihoko Matsubara, "A Roadmap for U. S. - Japan Cybersecurity Cooperation," May 2013, http://blogs.cfr.org/asia/2013/05/21/roadmap-for-u-s-japan-cybersecurity-cooperation/, 2016-08-20.

② White House, "Joint Statement: 2015 United States-India Cyber Dialogue," August 14, 2015, https://www.whitehouse.gov/the-press-office/2015/08/14/joint-statement-2015-united-states-india-cyber-dialogue, 2016-08-20.

③ In July 2016, Allies Reaffirmed NATO's Defensive Mandate and Recognized Cyberspace as a Domain of Operations in which NATO must Defend Itself as Effectively as It Does in the Air, on Land and at Sea. Available at http://www.nato.int/cps/en/natohq/topics_78170.htm, 2016-08-20.

④ 《首届中国—东盟网络空间论坛开幕》,《南宁日报》2014 年 9 月 19 日第一版。

⑤ "数字丝绸之路"构想是国务院《周边国家互联互通基础设施建设规划》的一部分,由信息与工业化部参与制定,2014 年 11 月制定完毕,迄今正式文本尚未公布。汪晓风:《数字丝绸之路与公共产品的合作供给》,《复旦国际关系评论》2015 年第 16 辑,第 171—172 页。

夺也将必然进入到全球网络政治空间。世界各国不断加大对网络空间的人力、物力、财力、技术等投入，不断加快建立网络空间的国家安全战略，促使全球网络空间“一超多强”的新格局初步显现。在这一格局中，美国占领着“一强独大”地位：美国掌握全球网络空间的核心控制权；美国拥有丰富的网络空间资源；美国还确立了全方位网络空间战略执行体系。中国则在全球网络空间迅速崛起过程中：中国积极推进信息网络技术的研发，不断完善网络基础设施建设。同时，中国国家高层领导人也高度重视网络空间。此外，俄罗斯、日本、印度、巴西等国也在迎头赶上，并在全球网民分布与网络力量中占有重要一席。①

之所以网络空间力量分布没有跳出传统地缘政治格局的原因在于，作为一种高科技，其优势可强化地缘优势、弥补地缘劣势。领先进行信息革命的国家可以迅速增强本国的经济实力，相应增强军事实力，拉开与其他国家的实力差距；开发、利用最先进的信息网络技术能最大限度地保护本国经济、政治、军事信息设施和国防秘密的安全，更广泛地传播本国的政治思想，争取参与处理世界事务的主导权。② 21 世纪已经形成了英国地缘政治学家哈尔福德·麦金德所说的大陆国家（处于欧亚大陆心脏地带的俄罗斯和中国）与作为海洋国家的美国、英国、日本两大阵营之间的竞争格局。似乎网络空间的出现并没有改变这样的竞争格局，相反，是某种程度上对原有格局的加深。

三、超越地缘政治“网络空间命运共同体”构想及实践

网络地缘政治虽然与传统地缘政治存在一定的区别，但还是难以摆脱传统地缘政治思维的影响。传统地缘政治学中将冲突与对抗视为逻辑起点。地缘政治思维在中美网络空间博弈中的存在大大影响了中美在网络空间的互信。可以说，中美网络空间互信程度很低的最主要原因仍然在于中美在地缘政治上的对抗思维。换言之，传统地缘政治框架中中美关系本身的结构性矛盾和功能性问题是中美网络空间互信缺失的基础原因。③ 因而，过分强调网络

① 互联网用户最多的前六个国家依次是中国、印度、美国、巴西、日本、俄罗斯。http://www.internetlivestats.com/internet-users-by-country，2016-08-20。

② 张妍：《信息时代的地缘政治与“科技权”》，第 21 页。

③ 蔡翠红：《论中美网络空间的战略互信》，《美国问题研究》2013 年第 1 期，第 93—118 页。

地缘政治于中美网络空间关系的良性发展很不利。

作为网络空间长远发展的愿景,“网络空间命运共同体”比“网络地缘政治”更加有利于网络空间的和平与稳定。“网络空间命运共同体”是习近平主席于2015年12月在第二届世界互联网大会上提出的概念。这一概念可以认为是中国智慧在网络空间问题上的发挥。其核心观点认为网络空间是人类共同的活动空间,网络空间前途命运应由世界各国共同掌握,各国应该加强沟通、扩大共识、深化合作,共同构建网络空间命运共同体。习主席同时提出建设“网络空间命运共同体”的五点主张。①

但是,我们也需要看到大国网络空间竞争已烙有地缘政治之印。中国的网络空间战略选择也必须在大力推进“网络空间命运共同体”建设的同时积极应对已经客观存在的网络地缘政治倾向。具体来说,中国可以在如下四个方面着力:

(一)重塑网络地缘政治时代的地缘战略体系

重塑网络地缘政治时代的地缘战略体系意味着在宏观上将网络空间上升到国家战略高度,将网络空间竞争纳入国家总体的地缘战略体系。中国需要摒弃以往的战术性应急策略,转而采取长远性的战略规划。传统的地缘战略体系以追求“陆权”“海权”“空权”“天权”等物理空间权力为地缘战略目标,强调地理环境和物质空间对国家生存发展的重要性。如今,虽然传统物质空间的地缘战略性依然存在,但是信息网络空间的战略重要性日益上升。因此,网络地缘政治时代的地缘战略重心应建立陆、海、空、天、网五位一体的全方位、立体化的地缘战略体系,以信息权为先导,以陆权、海权、空权、天权为基础,牢牢掌握地缘政治的“网络权”。②

中国已经充分认识到网络权的重要性。党的十八届五中全会提出了“网络强国战略”。2014年2月,国家主席习近平主持召开中央网络安全和信息化领导小组第一次会议强调,要努力把我国建设成为网络强国,而且建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进。而“互联网+”行动计划

① 五点建议分别为:第一,加快全球网络基础设施建设,促进互联互通;第二,打造网上文化交流共享平台,促进交流互鉴;第三,推动网络经济创新发展,促进共同繁荣;第四,保障网络安全,促进有序发展;第五,构建互联网治理体系,促进公平正义。参见国务院新闻办公室网站,http://www.scio.gov.cn/zhzc/10/Document/1459368/1459368.htm,2016-12-10。

② 王川:《网络地缘政治:定义、特征及其对中国西北边疆安全的影响》,第14—15页。

则是加快建设网络强国战略的落实行动和重大举措。同时，我国也在机制上为网络强国战略进行构思，例如 2016 年《网络安全法》和《国家网络空间安全战略》，以及 2017 年 3 月《网络空间国际合作战略》的推出。但是，网络强国战略的实施将是一个长远的、复杂的系统工程，需要各个方面的协同、推动和努力。

（二）坚持立足亚太和稳定周边的地缘战略思想

中国传统的地缘政治思想是一种防御性的和平地缘观，追求和睦的周边关系，强调周边安定和谐。同样，在网络空间战略发展上，这一战略思想依然适用。具体而言，这一思想可以结合两个方面得到实现：

一是通过“数字丝绸之路”积极构筑稳定的周边信息环境。与周边国家的良好关系是中国稳定的地缘战略依托，事关中国能否和平发展的连续性。数字丝绸之路构想的实施可以通过促进“一带一路”沿线国家的网络基础设施互联互通、网络应用服务平台共享、电子商务在线贸易融合等多个方面的发展来提升中国的吸引力和影响力，并对接中国“一带一路”区域发展合作倡议、网络强国战略部署、“互联网＋”行动计划、“中国制造 2025”等多项战略举措。①

二是以网络地缘经济为依托，以东盟和上合组织为支柱，拓展战略大周边。上合组织和东盟是中国经略周边的两大支柱，也是中国周边环境的稳定两翼。通过将信息网络合作整合到这两大体系中有助于推动网络时代的中国周边外交，从而有利于塑造良好的地缘战略态势，有利于扩大中国在周边国家间的影响力。

（三）加强网络空间防御能力和威慑能力

中国不赞成网络军事化的立场。但是，在全球各国都在发展网络军事化和武器化应用的国际背景下，中国也不得不做好相应的能力建设和准备。2016 年 4 月，习近平主席在网信工作座谈会发言中专门提到加强网络空间防御能力和威慑能力，特别是威慑能力的建设。这是第一次出现在中国领导人的讲话中，表明中国充分意识到了网络空间实力储备的重要性。

网络空间防御能力的增加是一个综合系统工程。它既包括加强公众教

① 汪晓风：《数字丝绸之路与公共产品的合作供给》，第 171—172 页。

育,培养网络安全意识和树立“网络边疆”意识,也包括加强网络空间立法,做到有法可依,还包括安全技术创新、专业人才培养,以及突发事件快速反应机制的建立,等等。

有学者在分析了网络空间的威慑战略可行性效果后认为,“惩罚威慑”(deterrence by punishment)用于网络安全领域存在很大问题,因为传统有效的惩罚威慑建立在“确保相互摧毁战略”之上,而网络攻击没有明确的巨大的附带伤亡预期,不能让对手明确意识到遭受报复的后果。“拒止威慑”(deterrence by denial)应用在网络空间也有局限性,因为网络攻击成本相对较低,攻击者即使可能预期到不能成功也可能还会尝试发起网络攻击。[①] 但是,随着国家关键基础设施的信息网络化,网络攻击的后果严重性预期也逐渐上升,惩罚威慑成为可能。同时,网络安全技术的进步也使防御能力为主的拒止威慑成为各国网络策略优先项。

(四) 塑造与提升国际认同力和网络空间软实力

大国网络搏弈还需破除“唯实力论”的迷思,塑造与提升国际认同度。国际认同和软实力的塑造决定了中国所倡导的“网络空间命运共同体”能否最终实现。决定中国在大国网络空间战略竞争地位的主要因素,除了不断增长的网络空间力量之外,更重要的是在向网络强国发展过程中中国的战略规划、执行和运作能力,问题和挑战的应对与化解能力,以及制度、观念和政策的内在更新和进步的能力。正如汉斯·摩根索所言:“国家的权力不仅依赖于外交的技术和武装力量的强大,而且依赖于它的政治哲学、政治机构和政治政策对其他国家的吸引力。”[②]

事实上,“网络空间命运共同体”与网络地缘政治并不完全对立。如果说网络地缘政治更偏重于当前的现实,那么“网络空间命运共同体”则更大程度上是一种愿景。事实上,二者同时存在于当前的大国网络关系中,体现在当前网络空间相互依赖和斗争冲突并存的现实。软实力战略既是“网络空间命运共同体”的构建路径,也是获取地缘政治优势的常用手段。地缘政治竞争对手之间的信息优势获取可以分为两类战略:一类旨在提高吸引力的软权力战略;

① 任琳、龚伟岸:《网络安全的战略选择》,《国际安全研究》2015 年第 5 期,第 51—52 页。

② 〔美〕汉斯·摩根索:《国际纵横策论》,卢明华译,上海译文出版社 1995 年版,第 203 页。

另一类旨在通过控制力途径的信息地缘政治。前者可促进合作和相互理解，长远而言可能产生相互的正面形象；后者则更多可能产生冲突和相互的负面形象。从短期而言，作为一个政治行为体的国家可以两种战略并用。但是从长远看来，软权力战略更加有效。①

中国在历史上曾经具有强大的对外吸引力和国际认同度。然而，中国当今在国际上的认同度却没有得到很好的发挥，尤其是在网络空间领域的国际认同度并不是很理想，常被西方塑造成“咄咄逼人的网络安全攻击者”以及“网络自由威胁者”的国际形象。美国以维护“网络自由”为名，多次在公开场合抨击中国是“没有言论自由、压制人权”的国家，直言批判中国所实行的网络审核制度；美国方面还极力渲染“中国网络威胁论”，对中国进行负面宣传报道，强加给中国极为不利的国际舆论压力，直接损害中国的国际形象。中国在国际上被塑造的这些负面形象加深了外部世界对中国“网络强国”目标的疑虑和不确定感，严重制约着中美之间的良性沟通，也增加了中国和平崛起为网络强国的成本。中国可从学者引导、事实数据、外交宣传以及成功的中国故事等各个角度改善国际形象从而提高国际认同的角度，促进中美认知的正向转变。

结　　语

综上所述，网络空间是地缘政治的新领域。网络空间组成架构的地缘属性、网络空间活动主体的地缘属性，以及主权国家在网络空间日益上升的权力，构建了网络空间的地缘政治属性。网络空间正在成为新一轮地缘政治博弈的大舞台，网络地缘政治初现端倪。网络空间对于地缘政治的意义不仅在于网络力量可以作为权利工具来实现传统地缘政治目标，而且网络力量对于地缘政治还有特殊意义，即网络力量本身不仅是一种权力工具，而且能对传统权力工具产生巨大影响，并成为各国综合国力竞争的决定性因素。

中美网络博弈正在变成越来越具有地缘政治为导向的关系，而“斯诺登事件”是中美网络博弈的地缘政治回归的催化剂。中美网络博弈中的地缘政治逻辑包括六大方面：地缘政治思维构建中美网络安全话语和政策、中美网络空

① Nerijus Maliukevicius, “Russia's Information Policy in Lithuania: The Spread of Soft Power or Information Geopolitics?” *Baltic Security & Defence Review*, Vol.9, 2007, p.153.

间壁垒与地缘政治空间的重合、网络主权的提出强化传统地缘政治理论、中美网络空间权力争夺重现地缘政治竞争、网络军事化趋势加强地缘政治冲突风险、网络问题逐渐被纳入传统地缘政治格局。

根据网络地缘政治理论,网络并不是运行在现有国际体系之外,网络空间力量还不足以改变传统地缘政治,是网络适应传统地缘政治而不是反过来,网络问题从属于地缘政治关系,地缘政治关系决定了网络空间关系。同时也说明现有的民族国家体系强大的承受力和弹性。与全球化一样,网络力量是"民族国家体系的女仆,影响到国家政策,但不会削弱民族主义的程度","民族国家依然是国际体系的黏合剂,是使得一个民族能够取得与其领土属性意识密不可分的自我实现的主要机制。"①

但是网络地缘政治理论并不是说网络空间没有超越传统地缘政治之处。传统地缘政治学将冲突与对抗视为逻辑起点。网络空间的新地缘政治特征决定了中美地缘政治博弈下的网络关系既有竞争也有合作,既相互借重又相互牵制。这也是网络时代的地缘政治与传统地缘政治的不同。② 此外,传统地缘政治的风险主要来自国家力量,而网络地缘政治的风险则不仅是国家力量,还包括许多非国家行为体的威胁,如恐怖主义威胁等。

总而言之,由美国引导的大国网络博弈的地缘政治趋势对全球网络安全形势形成了威胁,中国应与各国携手,超越地缘政治并推进"网络空间命运共同体"建设。在中美关系中,中美两国都无法单方面推动网络安全秩序朝着自身意愿的方向发展,无法按照自身的意志单独来塑造网络空间秩序。网络地缘政治博弈中的中美可以是战略竞争者但并非注定是敌人,中美在网络博弈中不应该互相为敌,而应寻求深化合作领域、拓展合作空间、建立合作机制、增进网络空间战略互信,从而为网络空间的中美新型大国关系和"网络空间命运共同体"建设打好基础。

---

① 〔美〕索尔·科恩:《地缘政治学:国际关系的地理学》,第52—53页。

② Alexander Sword, "The Future of Cyber Security Collaboration between Nation States: Can the USA and Russia Really Work Together?" May 20, 2016, http://www.cbronline.com/news/cybersecurity/data/the-future-of-cyber-security-collaboration-between-nation-states-can-the-usa-and-russia-really-work-together-4899785, 2016-08-20.