网络空间大国关系演进与战略稳定机制构建*

鲁 传 颖

提 要 | 随着网络空间中权力与财富的不断集聚，大国之间围绕权力划分和资源分配的博弈也在加剧。在缺乏国际秩序和规则约束的状况下，国家在网络中的行为具有战略上的进攻性、行为上的不确定性、政策上的矛盾性等特点，使得网络空间大国关系处于一种缺乏互信，竞争大于合作，并且冲突难以管控的状态。大国关系的无序竞争进而导致了网络空间处于脆弱战略稳定的状态，深刻地影响了国际体系的秩序。本文首先从力量格局、行为模式两个层面描述了网络空间大国关系的现状；其次，进一步分析了大国关系对网络空间战略稳定和全球战略稳定两个层面所造成的负面影响；最后，从建立大国网络空间战略稳定观，构建网络空间国际安全架构的角度探索如何建立网络空间战略稳定的制度体系。

关键词 | 网络空间 大国关系 战略稳定 国际安全架构

中图分类号 | D815

作者信息 | 鲁传颖，1983 年生，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，200003。

大国关系与战略稳定是传统国际战略研究的重要领域，正在成为影响网络空间秩序构建与和平发展的重要变量。将这两个概念应用到网络空间全球治理领域首先需要对其基本概念进行界定和明确。这是由于很多学者否认“国家”是网络空间中的主导行为体，秉持自下而上、公开透明的“多利益攸关方”治理模式。“多利益攸关方”曾是网络空间全球治理领域的主导理论范式，由此导致对网络空间大国关系的研究在国际上处于“非主流”的境地。① 另一方面，“战略稳定”具有深刻的“核武器”“冷战”烙印，有学者将“网络”与“核”进行类比，试图将核稳定的经验应用于网络空间，但两者之间存在的诸多截然相反的属性增加了类比研究的难度。② 近年来，国际社会开始关注“网络空间稳定”问题，如联合国裁军研究所会举办年度“网络稳定研讨会”，从军控角度来探讨网络空间冲突与稳定问题。由荷兰政府支持的全球多利益攸关方组织“全球网络稳定委员会”将关注点放在如何提升网络空间的可用性、完整性，以及和平解决网络冲突等议题上。国内学者对网络空间战略稳定的研究主要是从网络技术视角、危机管控经验、核稳定观、

* 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”（19BGJ083）的阶段性成果。

① Laura DeNardis & Mark Raymond, “Thinking Clearly about Multi-Stakeholder Internet Governance”, Paper Presented at Eighth Annual GigaNet Symposium, November 14, 2013, pp. 1 – 2.

② Joseph S. Nye, “Nuclear Lessons for Cyber Security”, *Strategic Studies Quarterly*, 2011, pp. 18 – 36.

中美网络关系等多个层面探索维护网络空间的战略稳定问题。① 总体来看，国内外现有的研究更多是在网络空间稳定和核稳定领域分析战略稳定的内涵，缺乏关于网络空间与国际体系战略稳定影响的分析，对全球战略稳定层面的研究关注不够。

在实践中，大国在网络空间中的冲突日趋激烈，网络空间军事化进一步加剧，成为影响全球战略稳定的重要不确定因素，这不仅使网络空间的秩序与和平面临严重威胁，也对各大国之间的国际安全、政治互信，以及全球贸易体系、科技创新体系和供应链完整造成严重破坏。② 因此，厘清网络空间大国关系的演进过程与内涵，分析其对战略稳定带来的深层次影响，在此基础上提出维护网络空间战略稳定机制，对于维护网络空间和全球战略稳定具有一定的现实意义。

一、网络空间大国关系的力量格局和行为模式

网络空间大国关系是国际体系中的主要国家行为体在网络空间中的互动关系，主要受到双重因素的影响，分别是国家在网络空间实力分布产生的力量格局，③以及基于网络空间特殊的安全、政治、经济逻辑所形成的国家在网络空间中的行为模式。④

1. 网络空间的力量格局

力量格局是国家在网络空间中的实力分布，它在一定程度上与现存国际体系中的力量格局关联密切，国家实力可以映射到网络空间当中。另一方面，网络空间自身所具备的特殊属性也对网络空间力量格局产生了很大影响，使得物理空间与网络空间的力量格局并非完全一致。可以根据网络空间的演进将网络空间中的力量格局的变化划分为三个阶段。

第一阶段是网络空间的无政府阶段。这一阶段的特点是“I* ”在互联网关键资源治理机制中主导地位的形成，民族国家在网络空间中的角色还处于被忽视的阶段。⑤ 无政府并不意味着混乱和秩序缺失，相反依靠代码治理和技术社群的主导作用，互联网得到了稳定、快速的发展。开放、透明、自下而上的多利益攸关方治理模式在网络空间秩序构建中发挥了重要作用。由于国家并没有过多地参与到这一进程中，很多人因此提出了所谓的“网络空间自治论”。⑥ 传统国际关系中以国家为主体的力量格局并未在这一阶段的网络空间中呈现。⑦ 这也反映了早期的互联网发展更多是基于技术和关键资源的分配，国家所关注的安全、政治、经济尚未出现在这一阶段的网络空间中。⑧

第二阶段是美国霸权阶段。随着人类社会的安全、政治和经济活动不断地映射到网络空间中，美国携技术上的先发优势成功

① 这方面的研究参见许蔓舒《促进网络空间战略稳定的思考》，《信息安全与通信保密》2019年第7期；石斌《大国构建战略稳定关系的基本历史经验》，《中国信息安全》2019年第8期；徐纬地：《战略稳定及其与核、外空和网络的关系》，《信息安全与通信保密》2018年第9期；沈逸《解析中美网络空间战略稳定的目标、方向与路径之争》，《信息安全与通信保密》2018年第9期。

② 周宏仁《网络空间的崛起与战略稳定》，《国际展望》2019年第3期，第29～31页。

③ 鲁传颖《网络空间治理的力量博弈、理念演变与中国战略》，《国际展望》2016年第1期，第118～119页。

④ 鲁传颖《网络空间安全困境及治理机制构建》，《现代国际关系》2018年第11期，第55～59页。

⑤ “I* ”是指一系列“I”开头的国际互联网组织，如ICANN、ISOC、IAB、IETF等，在互联网发展中扮演了核心角色。

⑥ David Johnson & David Post, “Law and Borders: The Rise of Law in Cyberspace”, *Stanford Law Review*, Vol 48, No. 5, 1996, pp. 1368 – 1378.

⑦ 〔美〕米尔顿·穆勒《网络与国家：互联网治理的全球政治学》，周程等译，上海交通大学出版社，2015年，第3～4页。

⑧ Miles Kahler (ed.), *Networked Politics: Agency, Power, and Governance*, NY: Cornell University Press, 2009, p. 34.

将自己在物理世界中的实力反映到网络空间中，成为网络空间中具有超强实力的国家。① 美国支持的 TCP/IP 协议，战胜了包括一些欧洲国家在内支持的 X. 25 协议，并以此为基础建立了全球互联网。② 互联网发展早期形成的技术社群如 ICANN、IETF、ISO、IAB 多位于美国境内。硅谷的崛起使得美国的互联网企业几乎垄断了网络领域硬件、操作系统、软件、应用等全生态系统。因此，美国成为网络空间中唯一的霸权国家，决定着网络空间中的商业、政治和安全秩序。其他国家实质上都是接入美国的互联网，也被动地接受了美国对于网络空间秩序的安排。③

第三阶段是巴尔干化阶段。“巴尔干化”是指原本美国主导的相对统一的网络空间出现分裂，各国政府开始加强对网络空间主权的维护，形成了网络空间国家化的趋势，原有的秩序开始出现巨大变革。④ 产生这种现象主要有三个原因。一是网络空间战略性意义不断上升，各国强化在网络空间中的主权，全球网络空间秩序与利益协调难度不断增加。⑤ 例如中国明确提出了网络主权战略。2018 年以来，欧盟也提出积极维护自身的“数字主板”和技术主权。二是美国作为霸权国家过度将在网络空间中的优势转化为实现国家战略的工具，抵消了美国在网络空间规则制定中的合法性，加速了美国霸权的衰落。在政治上，美国以所谓的“互联网自由”推动意识形态扩展，危害他国的政治安全。“阿拉伯之春”中美国政府要求脸书、推特等社交媒体平台拒绝接受埃及、伊朗等政府的指令，并为反对派的组织动员提供支持。在安全上，美国利用在网络空间中掌握的公共资源，追求自身在网络空间的绝对安全，对全球开展大规模网络监听，危害了包括盟友在内的世界各国国家安全。三是网络安全的非对称性进一步加剧了美国面临的网络安全挑战，使得美国不得不将更多的资源投向维护国内安全，加强网络军事力量建设。同时，美国对建立和维护全球网络空间秩序的态度发生转变，提出建立以“理念一致国家”(Like Minded States) 为基础的网络空间秩序。⑥ 作为这一政策的延续，特朗普政府还撤并了主要负责网络空间国际治理工作的国务院网络事务协调员办公室，取消了协调员这一关键职位。这表明美国政府对构建网络空间全球秩序的方向发生了变化。

2. 大国在网络空间的行为模式

影响网络空间大国关系的另一重要因素

① John B. Sheldon, “Geopolitics and Cyber Power: Why Geography Still Matters”, *American Foreign Policy Interests*, Vol. 36, No. 5, 2014, pp. 286 – 293.

② Jeremy Malcolm, *Multi-Stakeholder Governance and the Internet Governance Forum*, Wembley, Australia: Terminus Press, pp. 44 – 69.

③ Madeline Carr, “Power Plays in Global Internet Governance”, *Journal of International Studies*, Vol. 43, No. 2, 2015, pp. 640 – 659.

④ Camino Kavanagh, “The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century”, Geneva: United Nations Institute for Disarmament Research, 2017.

⑤ 在第五届信息安全政府专家组中，美国政府由于其提出的“反措施”“国家责任”原则未能获得一致支持，因而否决了整个专家组的报告，致使专家组旨在建立网络空间规范的进程受阻。参见 Michele G. Markoff, “Explanation of Position at the Conclusion of the 2016 – 2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security”, June 23, 2017, https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/。[2020-02-15]

⑥ Michael P. Fischerkeller & Richard J. Harknett, “Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation”, Alexandria: Institute for Defense Analysis, 2018.

是大国在网络空间中的行为模式，主要表现为网络技术对传统安全、政治和商业逻辑的颠覆，国家形成了更具进攻性的网络安全逻辑、相互不信任的网络政治逻辑和“技术国家化”的商业逻辑等三个层面。①

第一，国家的网络安全逻辑与传统安全逻辑存在很大差异，国际合作更加难以开展，各国普遍采取更具进攻性的网络政策。这背后反映了网络本身的不安全性（insecurity）、网络空间的不安全感和网络攻防的不对称性等网络技术对国际安全所带来的深刻影响。首先，网络具有不安全性，任何设备和系统都是由人设计的，因此理论上任何设备和系统中都存在着不同程度的错误。这种设备和代码产生错误的概率不仅很高，并很可能成为网络攻击的漏洞。因此，网络安全是泛在的，无法做到绝对安全。其次，网络空间给国家带来了很大“不安全感”，表现在国家难以对网络安全环境做出客观、准确的态势感知及威胁评估，网络空间的虚拟性、匿名性颠覆了物理世界对安全环境的认知。最后，网络攻防具有不对称性，网络攻击的对象不仅仅是军事目标，还包括大多数对国计民生具有重要价值的关键基础设施，这些关键基础设施数量大、分布广泛，并且主要由企业运行，存在极大的安全风险。从防御角度而言，要对如此众多具有潜在安全风险的关键基础设施进行保护，不仅收效甚微，成本也难以负担。这也使得国家无法单纯依靠防御来应对网络威胁。

第二，大国在网络空间政治互动中缺乏基本互信，导致政治安全无法得到保障、政治共识难以建立、政治承诺落实困难等新的逻辑。首先，政治安全对于任何大国而言，都是国家利益的核心领域，不容侵犯。在物理世界中，西方国家在意识形态领域的话语权要远远大于其他国家，也很难遇到政治安全问题。网络的匿名性和不对称性改变了这一格局，无论是俄罗斯黑客干预大选，还是剑桥分析事件，都表明西方国家民主政治的核心区域，在网络空间中面临极大的挑战。② 其次，大国在网络空间中的政治共识难以建立。由于网络议题的跨域性，不同群体在不同议题上具有不同的立场，使得大国之间很难就具体议题达成共识。如美国政府强调网络间谍的合法性，但是美国企业和民众却出于知识产权和隐私保护的目的反对政府的观点，这就极大增加了大国之间在网络间谍问题上达成共识的难度。③ 最后，由于网络具有抵赖性（deniability），影响了大国对政治承诺的落实。网络空间是匿名的，对网络攻击的溯源具有极大的技术难度，因此，对行为抵赖成为普遍的做法。无论是震网病毒、索尼影业还是“想哭”病毒等网络攻击事件都没有找出背后真正的始作俑者，很多溯源都是基于一些国家单方面的认定，缺乏合法性和权威性。

第三，网络空间也在对传统的商业逻辑产生影响，“技术国家化”（technology nationalism）导致供应链碎片化、产品本地化的趋势越来越明显，对传统基于效率优先、全球分工的商业模式带来了极大挑战。技术和产品封锁一直是国家间竞争的重要手段，如美国在国际上推动建立的《瓦森纳协议》和国内的《出口管制法》都是重要的体现。网络空间的不同点在于网信技术在民用领域的发展很大程度上领先于军事技术，致使这一领域的技术国家化将会对国际经济体系带来深刻和长远的负面影响。谷歌、微软、亚马逊这样的全球性企业所掌握的人才、技术和资源甚至超过了政府，对美国而言，如斯诺登所

① 鲁传颖《网络空间安全困境及治理机制构建》，2018年，第55～59页。

② Clint Watts，“How Russia Wins an Election”，*Politico Magazine*，December 13，2016.

③ Jack Moore，“Intelligence Chief：OPM Hack Was Not a ‘Cyberattack’”，September 10，2015，https://www.nextgov.com/cybersecurity/2015/09/intelligence-chief-clapper-opm-hack-was-not-cyberattack/120722/.［2020-02-15］

揭示的那样，这些企业成了政府实现战略目标高度依赖的资源。① 对另外一些国家而言，依赖这些外国企业则意味着自身的脆弱，因此鼓励发展基于本土的网络产品和服务。国家开始从战略竞争、国家安全的角度来看待网络空间的商业逻辑，客观上破坏了供应链完整性，从而颠覆了传统的商业逻辑。

二、网络空间大国关系对战略稳定性的影响

战略稳定是国际安全领域的重要概念，源于美苏在核领域的战略互动，很多人将战略稳定理解为大国在核武器领域的战略稳定关系。② 另一种战略稳定是指在国际体系层面的全球安全、政治、经济体系的稳定，中国与俄罗斯曾经发表过两份维护全球战略稳定的联合声明。③ 随着战略性地位不断提升，以及对现存国际体系的颠覆性影响越来越大，网络空间不仅成为国际体系中具有战略意义的新领域，也开始对物理世界的国际安全、政治和经济体系的稳定造成冲击。④ 因此，可以从两个层次来分析网络空间大国之间的互动关系对战略稳定的影响。一是大国在网络空间的互动加剧了网络空间的冲突和安全困境，从而影响了网络自身的稳定性；二是网络空间对全球战略稳定的影响。

1. 大国博弈加剧网络空间陷入脆弱稳定的状态

目前的网络空间大国关系主要特点是，战略博弈加剧导致了网络空间在安全上陷入困境，政治上相互不信任以及商业领域博弈加剧。从网络空间的大国关系来看，衡量网络空间是否处于稳定状态的因素主要包括，网络空间的总体安全环境，国家在网络空间中爆发冲突的可能性，以及是否存在可以维护稳定的制度体系。⑤ 当前，这种竞争性的大国关系，冲击了网络空间自身的稳定性，使其陷入一种脆弱稳定状态，并极有可能导致网络空间的战略不稳定。

首先，大国在网络空间的战略竞争，使得原本在全球网络安全领域扮演重要角色的网络安全技术协调机构之间的合作面临困境，阻碍了对维护网络安全具有重要价值的知识和信息工作的分享，加剧了网络空间的整体安全环境进一步恶化。计算机应急响应机构（CERT）和国际网络安全应急论坛（FIRST）是网络安全领域最重要的技术合作组织，前者以国家为单位开展合作，如中国计算机应急响应机构（CN-CERT），美国计算机应急响应机构（US-CERT）等。斯诺登事件之前，各国 CERT 之间有大量的技术合作，对于维护全球网络安全具有重要作用。受网络空间大国关系的影响，目前各国 CERT 之间的合作在越来越多的政治压力下大幅降低。FIRST 是全球性的网络安全技术社群，在网络安全有害信息共享和打击黑客领域具有举足轻重的作用，目前也面临与 CERT 同样的困境。由于受到美国政府的压力，FIRST 宣布暂停华为的会员资格，要求华为不得再参加 FIRST 的相关活动。类似政治干预技术安全的情况愈发严重，造成了网络空间安全环境的恶化。

其次，大国之间的网络冲突越来越严重，

① Dennis Broeders, Sergei Boeke & llina Georgieva, "Foreign Intelligence in the Digital Age Navigating a State of 'Unpeace'", The Hague Program for Cyber Norms Policy Brief, September 2019.

② Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era", *Journal of Information Warfare*, Vol. 15, No. 2, 2016, pp. 66 – 73.

③ 杨毅主编《全球战略稳定论》，国防大学出版社，2005 年，第 3 页。

④ James N. Miller & Richard Fontaine, "A New Era in U. S. -Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies are Reshaping Pathways to Crisis and Conflict", Washington DC: Center for New American Security, 2017.

⑤ Gary Hart, et al., "Report on a Framework for International Cyber Stability", Washington DC: International Security Advisory Board, U. S. Department of State, July 2, 2014.

单边主义和先发制人的思想盛行，网络空间安全秩序陷入集体行动困境。网络空间的集体行动困境主要表现在现有的国际安全架构无法适用于网络空间，大国在建立新的国际安全机制上缺乏共识。在震网病毒、棱镜门、索尼影业和黑客干预大选等全球重大的网络安全事件中，国际安全架构基本失灵，加剧了各国网络战略向自助和进攻性方向调整。美国国防部制定了前置防御（defense forward）和持续交手（persistent engagement）政策，主张要把网络安全的防线扩展到他国主权范围内，并且通过网络行动对其网络对手进行反击。① 美国先后宣布对伊朗、朝鲜和俄罗斯的关键基础设施实施了网络攻击，作为对两国危害美国网络安全行为的报复。② 美国认为自己的行为是出于防御的目的，但是国际社会以及伊朗、朝鲜和俄罗斯对此有完全不同的解读，各方之间的网络冲突将会进一步加剧和升级。

最后，大国之间在网络空间领域建立信任措施举步维艰，美俄、中美之间的对话渠道集体陷入困境。建立信任措施是国际安全领域预防冲突升级的重要举措，大国之间也试图将 CBMs 作为维护网络空间稳定的重要机制。美俄、中美之间都曾试图在网络空间建立 CBMs。斯诺登事件之前，美俄之间成立了网络安全工作组，并就 CBMs 达成共识，后因俄罗斯接纳了斯诺登的政治避难而被取消。③ 再后来，黑客干预大选事件不断升级，美国从对俄开展跨域威慑到直接入侵俄罗斯电网作为报复，美俄冲突不断加剧。中美之间也曾在 2013 年成立中美网络安全工作组，并尝试推动 CBMs，后因起诉军人事件，工作组被无限期中断。虽然后来中美之间建立了打击网络犯罪高级别对话机制和执法与网络安全对话机制，但由于缺乏两国军方的直接参与，在建立 CBMs 上效果并不明显，特别是在贸易冲突的干扰下，执法与网络安全对话陷入停滞状态，中美网络关系总体上也处于一种脆弱稳定状态。

2. 网络空间对全球战略稳定造成冲击

网络空间对全球战略稳定的影响体现在对核战略稳定，以及对国际安全、国际政治和国际经济体系稳定造成的冲击。

网络安全已成为核武器面临的重大风险来源，但大国之间对此却未能建立相应的维护稳定机制。核武器的指挥与控制系统和卫星通信系统存在巨大的网络安全风险，对核安全造成冲击，从而影响核领域的长期稳定。由于核武器所具有的特殊性，任何针对核武器的网络安全事故都会导致国家的警惕、焦虑、困惑，削弱国家对于核威慑力量的可靠性和完整性的信心，从而导致重大的危机升级和破坏性后果。相对于传统核领域大国之间在核威慑、危机管控、冲突升级/降级等方面具有的成熟经验，国家对于网络安全对核武器所造成的威胁不仅缺乏全面、准确的认知，对于危机管控和冲突降级的举措也缺乏共识。因此，网络安全已经构成对核稳定的重大挑战，需要尽快建立相应的稳定机制。

网络科技改变了传统军事形态和作战方式，给国际安全领域带来了新的风险和威胁。随着网络、人工智能在军事领域的实战化，战争的形态将被彻底改变。军人、战场和战争模式会发生颠覆性的变化。程序员将成为军人中的重要组成部分，他们手中的武器与动能武器截然不同，攻击的目标发生了巨大变化。一方面，网络技术会使得武器杀伤的精确性大幅提高，降低战争的暴力性，另一方面，也会使得很多民用关键基础设施成为被

① U. S. Department of Defense, "Summary of the Department of Defense Cyber Strategy", September 18, 2018.

② "U. S. Escalates Online Attacks on Russia's Power Grid", *The New York Times*, June 15, 2019.

③ "U. S. and Russia Sign Pact to Create Communication Link on Cyber Security", *The Washington Post*, June 17, 2013.

攻击的对象，从而造成更大范围的影响。① 现有的国际法，包括《联合国宪章》《国际人道法》如何在这一领域适用，大国之间存在很大的分歧。② 现有的国际安全架构，包括军控与裁军机制，也无法用来解决新的现象。网络武器扩散、人工智能武器的滥用，将有可能带来重大的危机和人道主义灾难，危及国际安全体系的稳定。

现有的国际政治体系总体上也越来越难以适应网络空间所带来的挑战。特别是联合国作为国际政治体系的中枢核心，如何在网络空间秩序构建上发挥领导作用，受到了部分西方国家政府和社会的质疑和抵制。联合国需要建立自身在网络空间治理中的合法性、代表性和有效性，来维护网络空间政治体制的运转。首先，联合国在传统国际政治领域的合法性不仅源于战后的制度安排，也源于成员国的授权。网络是一个新的空间，不同行为体、不同国家对于网络空间的基本属性在认识上存在极大的分歧，联合国在物理世界中的合法性能否延伸到网络空间中受到了很多西方国家的质疑。其次，联合国是主权国家组成的国际政府间组织，非国家行为体并不认可国家可以代表其加入联合国，并且由于联合国特殊的官僚体制，非国家行为体很难参与到决策体系中，加剧了网络空间治理中具有重要影响力的非国家行为体对联合国代表性的质疑。③ 最后，联合国的有效性在于是否能够在重大网络空间治理问题上促使各国达成共识并加以落实。以联合国信息安全政府专家组为例，在过去已经结束的五届专家组中，只有三次达成共识，不仅范围有限，而且其中一些关键共识未得到落实，从而加剧了国际社会对于联合国政治地位的质疑。④ 联合国在网络空间规则制定、秩序维护中作用的缺失使得国际政治体系在未来将会面临更多、更大的挑战。

网络经济的颠覆性及其背后的国家安全、隐私保护因素加剧了国际经济治理体系面临的挑战，给全球经济的未来带来了极大的不确定性。一是数字经济规则缺失，数据的本地化和数据流动之间的矛盾对于国际经济体系的撕裂正在加剧，越来越多的国家出于安全需要开始要求数据本地化存储。数据在全球的流动将会受到限制，从而对全球化造成新的冲击。二是大国博弈导致的供应链的碎片化趋势，将会进一步加剧数字地缘经济的博弈。⑤ 网络发达国家与网络新兴国家之间如果不能就维护信息通信技术的全球供应链体系和创新生态体系完整达成共识，将会有可能在网络空间出现不同的地缘经济集团。三是一些颠覆性的创新会挑战现有的国际经济治理机制，如区块链技术应用产生的虚拟货币成为洗钱、勒索、诈骗等网络犯罪的首选工具，现有的国际经济治理体系无法应对虚拟、去中心化所带来的挑战。

三、维护网络空间战略稳定的几点思考

大国互动关系影响了网络空间和全球战略稳定，危及网络空间的和平发展。维护战略稳定已经是网络空间全球治理领域最紧急和最基本的议程之一。根据物理学的定义，

① UNIDIR, "The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approaches", Geneva: United Nations Institute for Disarmament Research, 2017.

② Michael N. Schmitt, et al. (eds.), "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", Cambridge: Cambridge University Press, 2017.

③ Mueller Milton, *Networks and States*, Cambridge, MA: MIT Press, 2010.

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 李巍、赵莉《美国外资审查制度的变迁及其对中国的影响》，《国际展望》2019 年第 1 期，第 45～50 页。

稳定是指物体受到扰动后能够自动恢复到原来的状态。因此，维护网络空间战略稳定需要从主动和被动两个方面开展工作。主动是指国家需要建立网络空间战略稳定观，减少自身行为对稳定的破坏；被动是指建立一套在稳定被破坏后能够使其复原的机制，即网络空间安全架构。

1. 建立大国共识的网络空间战略稳定观

维护网络空间战略稳定需要大国之间在战略稳定观及其内涵上达成共识，这有助于大国更好地认识自身在网络空间的行为对战略稳定的影响。从大国关系角度来看，网络空间具有战略性、整体性、全局性、颠覆性等四个特点。战略性是指各国都开始从战略高度来看待网络空间的崛起，并制定相应的战略规划来获取相对于对手的战略竞争优势，因此，不会轻易妥协，或者放弃自己的战略利益。整体性是指所有接入到互联网中的设备在技术层面都是可以相互连通的，大到核武器，小到个人可穿戴设备，网络空间将数百亿的大大小小设备连接到一起。这些设备都是通过相同的协议、介质、编码而连接成一个整体，任何一个部分出现了问题，都有可能对整体秩序产生冲击。全局性是指网络空间中不同的议题往往会相互关联，并产生全局性影响。如国家维护网络安全的举措会影响技术和经济发展。网络技术具有颠覆性的影响，网络空间的演进逐步地颠覆了现有的国际秩序观念。如网络的实时传输，改变了基于传统地缘所建立的时空概念，过去建立在物理世界的军事、安全观念和能力都不足以应对网络空间的安全与军事需要。

根据网络空间战略性、整体性、全局性和颠覆性的特点，结合前文所述大国关系给战略稳定带来的挑战，可以构建出当前网络空间战略稳定的内涵。主要包括大国在网络空间的冲突不会导致全球互联网运行的中断；网络战略和政策不会导致互联网的“巴尔干化”；军事行动不会导致大规模的关键基础设施瘫痪；设定网络行动的禁区，不将核武器的指挥与控制系统作为网络军事目标。国家可以以此为目标，对自身的网络空间战略进行相应调整，减少对战略稳定的破坏。

一是确保战略博弈的可控性，国家在采取相应的行动时，应当保持一定的克制，以避免酿成危机或加剧冲突的升级，破坏网络空间的和平与发展。① 二是维护网络空间的整体性和连接性，国家在网络空间的行动不破坏网络空间的整体性。比如对于全球网络运营至关重要的互联网关键基础设施一旦出现问题，就会产生严重后果。因此，全球网络稳定委员会提出的保护互联网的“公共核心”(public core)就是对此的反应。三是政策制定时应充分考虑网络空间的全局性，在制定网络安全、数字经济、信息化等不同领域的政策时，应当兼顾相互之间的影响。一方面，国家具有维护网络安全的重要职责，但另一方面采取过度的安全化或者军事化的措施都会对网络空间产生全局性影响。如出于保护个人隐私和国家安全的目的，国家会采取一定的数据本地化措施，但是过度的本地化会对网络空间数据自由流动产生负面影响。四是在应对网络技术的颠覆性影响时，避免引起现有体制的失灵。特别是类似于网络武器、人工智能武器的发展和使用会给国际社会带来一系列的伦理、国际法、国际安全挑战。国际社会应当采取措施，将其对国际体系的冲击保持在可控的范围，不触碰底线，不触发旧体系的解体。

2. 构建网络空间国际安全架构

网络空间大国的竞争与冲突固然对战略稳定提出挑战，但缺乏能够复原的机制也是影响战略稳定的另一重要因素。国际社会曾参照传统国际安全领域做法，试图通过增加网络透明度、CBMs、危机管控来建立网络空

① Joseph S. Nye, “Deterrence and Dissuasion in Cyberspace”, *International Security*, Vol. 41, No. 3, Winter 2016/17.

间的稳定机制。① 这一努力并未取得成功，联合国信息安全政府专家组的工作陷入困境，美俄、中美之间建立的稳定机制基本都陷入停滞状态。因此，国际社会需要根据网络空间自身的属性和特点来采取稳定措施，将关注点集中在建立网络空间的国际安全架构上。网络空间的脆弱稳定状态与国际安全架构在应对网络冲突时几乎完全失灵，无法发挥网络冲突预防、危机应对、调停、冲突降级等作用。② 从现有网络冲突的特点来看，应在全球关键基础设施保护、集体溯源、漏洞分享机制和供应链安全等方面建立安全架构体系，形成真正有效的稳定机制。

第一，加强对各国共同依赖的全球关键基础设施的保护，不仅有助于维护全球网络空间稳定，也有利于国际社会探索在网络领域建立合作机制。关键基础设施保护是各国维护网络安全的重要任务，由于大国之间缺乏互信，使得相应的合作难以开展。美国国务院网络事务办公室副主任米希尔·马科夫(Michele G. Markoff)就曾在中美网络对话中指出，“我们不会告诉任何人我们关键基础设施的数量和分布”。公开信息当然会暴露自己的风险点，但完全不公开也会导致合作难以展开。对于全球关键基础设施保护，不仅具有敏感性，而且还有重要性和紧迫性。可以从全球能源、交通、金融正常运营所依赖的关键基础设施开展合作，明确全球关键基础设施的定义，建立相应的规范和措施，要求国家不应对全球关键基础设施进行攻击，并且建立相应的合作机制。

第二，开展集体溯源合作，为网络冲突的争端解决建立国际性的平台。溯源问题之所以关键，是因为它涉及责任归属问题。由于缺乏客观中立的国际组织来对相应的网络安全事件进行调查，绝大多数涉及国家的网络攻击最后都不了了之，这种现象会鼓励更多的网络攻击发生，扰乱国际网络安全秩序。有学者认为，应当在联合国层面建立相应的机构，专门就网络攻击的溯源问题开展工作，在网络攻击发生后开展相应的调查，一旦这样的国际机构成立，必将对攻击者产生极大的震慑作用，从而遏制网络攻击高发的态势。③ 要做到这一点还存在一定的难度，主要原因是少数大国垄断了溯源技术，既不愿意与其他国家进行分享，也不愿意协助联合国开展溯源能力的建设。对此，国际社会应当有明确的态度，克服少数国家的阻碍，支持联合国在溯源方面开展相应的工作。

第三，推动构建国际漏洞公平裁决机制(IVEP)。漏洞是指计算机存在的程序缺陷，这种缺陷往往被用来开发网络武器，开展网络攻击，从而对网络空间战略稳定构成重大的冲击。各国都将漏洞分享作为应对网络安全威胁的重要方法。在国内层面，漏洞公平裁决机制(VEP)是一个跨部门的过程，用于确定是否将以前未知的漏洞(零日漏词)通知软件供应商，或将该漏洞暂时用于合法的国家安全目的。④ 但是在国际层面，大国都在将发现和利用漏洞作为谋取战略竞争优势的手段，这加剧了网络空间整体的不稳定。从网络空间国际安全架构角度来看，推动各国在漏洞领域加强合作是重要的技术基础。国际社会应探索设立相应的国际机构，负责处理重大漏洞的信息共享机制和危机合作机制，主要包括漏洞信息共享，建立漏洞危机处理合作机制。

第四，加强供应链安全治理，有助于从技

① Daniel Stauffacher & Camino Kavanagh, “Confidence Building Measures and International Cyber Security”, Geneva: ICT Peace Foundation, 2013.

② Jeremy Rabkin & John Yoo, *Striking Power: How Cyber, Robots, and Space Weapons Change the Rules for War*, New York: Encounter Books, September, 2017.

③ Martin Libicki, *Cyber Deterrence and Cyberwar*, Santa Monica: RAND Corporation, 2009.

④ 朱莉欣《构建网络空间国际法共同范式——网络空间战略稳定的国际法思考》，《信息安全与通信保密》2019 年第 7 期，第 9 ~ 11 页。

术和商业两个层面避免网络空间的“巴尔干化”，维护网络空间战略稳定。网络空间所依赖的网络产品和服务是建立在复杂的全球供应链体系之上，也是全球科技和商业领域最复杂、最高效的领域之一。在缺乏国际治理机制保障的情况下，大国愈发表现出技术国家主义色彩，只信任本国生产的产品，以国家安全名义排除使用其他国家的产品；以保护国家安全为由阻碍来自其他国家正常的投资活动；利用垄断核心技术和产品的优势拒绝向他国出售相应的技术和产品。为了维护网络空间战略稳定的技术和商业基础，国际社会应当为网络设备和产品提供更加安全的标准体系，增加供应链体系的透明性、可靠性、可问责性。① 国家应当将重心放在网络安全和服务的审查上，而非以破坏贸易规则的形式来拒绝国外的产品和投资。各国政府应该达成共识，不在民用网络安全产品中植入后门与漏洞，破坏供应链体系的安全性。美国微软公司在“数字日内瓦公约”中就倡议政府“不以科技公司、私营部门或关键基础设施为攻击目标”。

四、结　语

战略稳定是网络空间全球治理领域中的一项新兴议程，对于从战略和体系层面思考维护网络空间和平与发展具有重要价值和意义。厘清网络空间大国关系与战略稳定之间的关系，对于各国政府更好地理解和制定网络空间战略目标和实施路径具有重要的参考价值。当前，概念在理论层面还处于不断发展和完善的进程中，需要有更多国内外的学者参与探讨。在实践层面，这一领域还需要联合国以及各国政府的支持和推动，将战略稳定作为构建网络空间秩序的基础。

（责任编辑：刘　仑）

① NIST, “Best Practices in Cyber Supply Chain Risk Management: Intel Corporation: Managing Risk End – to – End in Intel’s Supply Chain”, https://csrc.nist.gov/CSRC/media/Projects/Supply – Chain – Risk – Manag ement/documents/case_studies/USRP_NIST_Intel_100715.pdf. [2020 – 02 – 15]