专题：新形势下的中国国际战略

中美网络空间危机管理

许蔓舒　鲁传颖

内容提要：随着以互联网为代表的现代信息技术的迅猛发展，网络空间成为国家安全和国际竞争的新领域。网络空间冲突引发国家关系紧张、甚至走向全面对抗的危险不断上升。网络安全问题给中美关系带来了巨大的风险和隐患。回顾过去，中美网络空间的危机管理有成功的案例，也有失败的教训。当下，中美面临着战略意图误读、科技竞争意识形态化、缺乏战略默契的挑战。未来，中美两国需要共同努力，寻求达成网络空间危机管理基本原则的共识，充分发挥学术交流机制的作用，采取措施建立信任，为双方在网络空间危机管理中达成合作奠定基础。

关键词：中美关系　网络空间安全　危机管理

一、前言：理解网络空间危机管理

从20世纪90年代至今，以互联网为代表的现代信息技术在全球迅猛拓展，塑造并形成了人类活动的第二空间。在虚拟的网络空间中，国家间的较量此起彼伏，并日益走向常态化。不过，发生在网络空间的国家间对抗并不直接造成人员伤亡和损害，所呈现的冲突强度较低，远未达到战争迫在眉睫的危机程度。因此，即使是网络空间的军事行动也只是被划入战争门槛以下的冲突范围中。尽管总体处于低烈度有限对抗水平，但网络空间的对抗仍可能加剧国家间的紧张关系，甚至推动冲突双方走向全面对抗、甚至战争。

许蔓舒　上海国际问题研究院网络空间国际治理研究中心特聘研究员；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、研究员。

首先，低烈度、高频度的网络恶意行动会加剧国家间的猜忌、不信任和安全困境。一方面，随着信息通信技术的快速发展和应用，网络空间与国家经济、社会治理、国家安全密切相联，网络空间安全对国家安全具有“牵一发而动全身”的作用。另一方面，通过网络空间，国家和非国家行为体具备了直接或者间接损害他国繁荣、安全和重要价值的能力。加之在网络空间采取行动的成本低、技术扩散迅速、非国家行为体数量庞大，难以确定源自一国的网络攻击的发动主体是谁及发动原因，因而也无法基于国际法向有关责任方进行追责。其次，低强度的网络恶意行动可以达成损害他国利益的战略目的，容易导致国家间关系陡然紧张。例如，网络信息可以影响一国选举结果；网络攻击可以破坏核设施的运行；通过破坏敌国的经济、通信、交通等关键基础设施的信息系统，网络攻击甚至能够提供比导弹更加致命的破坏能力。最后，网络空间的军事行动增加了触发现实世界战争的危险性。从军事上看，网络空间行动的最大优势在于，“无需在他国领土建立物理存在就可以实现火力投送”。[1] 跟传统的军事斗争方式相比，网络空间军事斗争的方式更加多样、隐蔽、灵活，更容易通过欺骗、重定向、系统设置等方式远程操控对手的网络空间目标，这些不仅增加了战争迷雾，而且降低了动用国家军事力量的门槛。

总之，网络空间的出现给国家间对抗提供了新的角力场。网络情报收集、关键基础设施攻击、信息影响行动、网络空间作战，成为网络空间国家对抗的主要行动样式。伴随着攻击与报复的循环往复，网络空间对抗的升级、外溢、失控的后果可能超出政治家的控制。在此背景下，网络空间危机管理也被“整合到一般意义下的危机管理架构、政策和计划中”。[2] 在国际问题研究中，危机管理的对象通常指的是国际危机，即“指两国或多国的对抗，通常会包括参与方所感受到的爆发战争的可能性急剧增加的一小段时期”；[3] 危机管理的任务是“在危机中采取减少战争风险的克制措施”。[4] 换言之，在国际政治的语境下，危机管理是综合运用外交、军事、经济等方式，对危机进行控制和处理的行为，其目的是为了避免危机失控或者引发战争，确保危机能在国家重大利益不受损害的前提下得到和平解决。依照此思路，网络空间的危机管理可理解为：对可能导致国家间关系紧张、武装冲突、甚至战争的网络行动或事件进行控制和处理，目的是防止发

1 U.S. Joint Chiefs of Staff, “Joint Publication 3-12: Cyberspace Operations,” p. XII, https://fas.org/irp/doddir/dod/jp3_12.pdf, 2021-06-02.

2 Panagiotis Trimintzios, Roger Holfeldt, Mats Koraeus, Baris Uckan, Razvan Gavrila, and Georgios Makrodimitris, “Report on Cyber Crisis Cooperation and Management: Comparative Study on the Cyber Crisis Management and the General Crisis Management,” European Union Agency for Network and Information Security, November 2014, p.10, https://www.enisa.europa.eu/publications/ccc-study, 2021-05-09.

3 Phil Williams, *Crisis Management: Confrontation and Diplomacy in the Nuclear Age*, Martin Robertson & Co. Ltd., 1976, p.25.

4 Gilbert R. Winham, ed., *New Issues in International Crisis Management*, Westview Press, 1988, p.15.

生在网络空间的国家间对抗发生升级和外溢，避免引发现实世界的战争。

国际社会对网络空间危机管理的理解继承了传统国际危机管理的有关概念；但网络空间的虚拟性、匿名性和军民两用性，以及网络冲突的低烈度、高频度等特征，使得网络空间危机管理有着自己的特殊性。

网络空间危机管理是国际危机管理的新发展。国际社会对网络空间危机管理的理解继承了传统国际危机管理的有关概念，包括目标与手段；遵循危机预防、危机控制和危机降级等阶段的划分；试图通过危机预防、建立信任、军备控制、谈判和国际调停，以及危机处理、恢复重建等方面的工作，加强对国家在网络空间激烈对抗的事前、事中和事后管理。但是，网络空间的虚拟性、匿名性和军民两用性，以及网络冲突的低烈度、高频度等特征，使得网络空间危机管理有着自己的特殊性，其“任务的拓展、时间线的延长、行为体的增加使得危机管理工具的有效协调成为紧急的优先事项”。[1]

在实践中，网络空间危机管理已经成为国际军控领域的新议程，得到了一些国际组织和学术研究机构的关注。例如，联合国裁军研究所（United Nations Institute for Disarmament Research, UNIDIR）建立了“网络稳定”项目，并组织召开年度性会议探讨加强网络空间危机管理。人道主义对话中心（Center for Humanitarian Dialogue）自2019年关注网络安全威胁对国际安全的影响，希望通过对话找到信任建立措施及其操作指南，帮助减少网络大国之间的紧张关系和不信任。美国麻省理工大学计算机科学和人工智能实验室于2016年发起了“网络军事稳定圆桌会议”，旨在通过召开“1.5轨道”的研讨会，汇集美国、中国、俄罗斯等国的学者、智库和政府官员，共同探讨如何减少网络风险，促进国际和平与安全。

本文将中美网络空间危机管理定义为：对可能导致中美两国关系紧张、武装冲突甚至战争的网络事件进行控制和处理，目的是管控中美两国网络空间分歧，降低可能引发中美两国关系恶化甚至走向全面对抗的网络风险。通过分析中美网络空间危机管理的实践和面临的主要挑战，笔者希望找到可行的途径，减少中美在网络空间中的不信任，促进两国建立更为稳定的网络安全关系。

二、中美网络空间对抗与危机管理的历史回顾

中美两国经历了多次网络空间冲突，网络安全问题给中美关系带来了巨大的风险和隐患。中美网络空间危机管理有成功的案例，也有失败的教训。通过回顾

1 Christian Mölling, “Comprehensive Approaches to International Crisis Management,” *CSS Analyses in Security Policy*, Center for Security Studies (CSS), ETH Zurich, p. 1, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-42.pdf, 2021-05-09.

历史，本文旨在找出中美网络空间危机管理可以吸取的经验和教训。

（一）克林顿和小布什执政时期

20世纪90年代，美国总统克林顿在国内开启“信息高速公路”计划，同时推动互联网在全球扩张和拓展。小布什执政时期，美国在网络空间的战略重心旨在加强关键基础设施保护，侧重于从国内安全角度审视网络安全。中国于1994年正式接入国际互联网，信息化起步虽晚但发展迅速，到2008年中国网民数首次超过美国，居世界第一。[1] 从总体实力看，彼时美国的信息技术及产业规模在全球遥遥领先，中美两国的网络实力对比差距明显。同时，在克林顿和小布什执政期间，中美涉及网络的交集较小，因而两国的网络安全矛盾并不突出。

（二）奥巴马执政时期

奥巴马执政时期，中美之间涉网议题逐渐增多，争议集中在网络安全审查、网络窃密等网络空间上，即具体的网络管理措施或网络空间活动。其间围绕网络间谍问题，中美发生了激烈的较量。所幸在高层的直接努力下，两国成功地对这一网络空间危机进行了有效管理，建立了网络安全对话机制，稳定了双边关系。

奥巴马政府强调“互联网自由”，借信息自由流动之名，反对其他国家的互联网公共政策，“要求其他国家向美国企业开放市场 ，把美国的互联网企业推向全球”。[2] 中国在2010—2020年进入移动互联网时代。当网络作为交流平台的社会价值不断显现、互联网的规模效应足以影响国家安全时，中国采取了必要手段对国内出现的互联网问题进行监管。但在美国看来，互联网是自由贸易、言论自由、信息和经济交流的平台，中国的网络安全审查政策与美国的价值观相冲突。脸书（Facebook）、推特（Twitter）被限制，谷歌（Google）退出中国等事件也反映了中美在网络治理上的观念差异。尔后，伴随着美国对华为等中国高科技企业的安全审查和打压，美国政府、企业、媒体、学界大肆渲染和指责中国针对美国的网络窃密行动，中美的网络间谍争端开始升级，一度上升到国家间的激烈较量。

此次争端源起于2013年2月美国曼迪昂特公司（Mandiant）发布的一份报告，该报告指责中国军方直接参与针对美国企业、政府及重要基础设施的网络入侵活动。[3] 这是有史以来首份直接点名中国“网络间谍”问题的研究报告。同年6月，

1 中国互联网络信息中心 (CNNIC):《中国网民数量首次超过美国》,《北京日报》，2008年7月25日，https://it.sohu.com/20080725/n258380068.shtml，2021年5月19日登录。

2 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，第57页。

3 Jim Finkle, “Mandiant Goes Viral after China Hacking Report,” Reuters, February 23, 2013, https://www.reuters.com/article/net-us-hackers-virus-china-mandiant-idUSBRE91M02P20130223, 2021-05-09.

“棱镜门”事件[1]曝光美国情报机构对中国实施了长期的、大范围的网络监听活动。基于构建新型大国关系的共识，[2] 2013年6月8日，中美两国元首首次就网络安全问题开展对话，网络议题由此纳入中美战略与经济对话中。尤其值得一提的是，在该对话机制下，双方于2013年7月成立中美网络安全工作组并举行了第一次会议，而且双方都认可该工作组是两国网络安全问题双边对话的主平台。[3]

2014年，中美网络间谍争端开始升级。2014年5月，美国司法部以网络窃密为由起诉5名中国军官。对此，中国外交部迅速做出回应，表示强烈愤慨和坚决反对，要求美方撤诉，并随后中止了中美网络安全工作组对话。至此，中美网络安全关系跌至冰点。随后，双方围绕网络间谍问题的争端进入僵持阶段。2014年9月，中国银监会等部门联合发布《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》；同年12月，中国银监会与工信部联合发布《银行业应用安全可控信息技术推进指南（2014—2015年度）》，要求中国金融机构提高信息系统的自主可控率，以加强行业安全可控信息技术以及网络安全的建设；2015年3月，中国拟议《反恐怖主义法（草案）》（以下简称《反恐法》），要求企业为有关部门依法防范调查恐怖活动提供技术接口和协助。对此，美国一些官员及西方商业团体认为中国的《反恐法》，包括新出台的上述银行业监管规定，对外资企业构成了不公平的监管压力。[4]

2015年，中美网络间谍争端继续恶化。5月16日，天津大学张浩教授在洛杉矶入关时被捕，被当地法院以涉嫌经济间谍罪起诉。[5] 6月底，美国联邦人事管理局称其计算机网络遭到攻击，包括2100多万美国人的社保号码和其他个人信息被盗取。美方将上述网络攻击事件跟中国联系起来，认为是中国对美国采取的

1 2013年6月，前美国中央情报局（CIA）职员爱德华·斯诺登（Edward Snowden）将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》。6月5日，英国《卫报》披露美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森通信公司必须每天上交数百万用户的通话记录。6月6日，美国《华盛顿邮报》披露称，过去6年间，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果、雅虎等9大网络巨头的服务器，可以对即时通信和既存资料进行深度监听。

2 Caitlin Campbell and Craig Murray, “China Seeks a ‘New Type of Major-Country Relationship’ with the United States,” U.S.-China Economic and Security Review Commission Backgrounder, June 25, 2013, p. 4, https://www.uscc.gov/sites/default/files/Research/China%20Seeks%20New%20Type%20of%20Major-Country%20Relationship%20with%20United%20States_Staff%20Research%20Backgrounder.pdf, 2021-05-19.

3 参加中美网络安全工作组的中方官员来自中国外交部、国防部、公安部、工业和信息化部、商务部、国务院新闻办公室等部门；美方官员来自美国国务院、国防部、国土安全部、司法部、财政部、商务部、联邦调查局及总统国家安全事务委员会等部门。Office of the Spokesperson of the U.S., “U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track,” July 12, 2013, https://2009-2017.state.gov/r/pa/prs/ps/2013/07/211861.htm, 2021-05-19.

4 Ben Blanchard, “China Passes Controversial Counter-terrorism Law,” Reuters, December 28, 2015, https://www.reuters.com/article/us-china-security-idUSKBN0UA07220151228, 2021-05-19.

5 Lindsay Dunsmuir, “U.S. Charges Six Chinese Nationals with Economic Espionage,” Reuters, May 20, 2015, https://www.reuters.com/article/us-usa-china-theft-idUSKBN0O41PP20150520, 2021-05-19.

报复行为。时任美国国家情报局局长克拉珀（James Clapper）在国会听证会上称，中国是袭击的“主要嫌疑犯”，并补充说，鉴于“入侵”的困难，“必须向中国人致敬，因为如果我们有这样的机会，我们也不会犹豫的”。[1] 2015年习近平主席访美前夕，美国媒体释放消息称“美国酝酿制裁因网络窃密而受益的中国实体和个人”，[2] 而且美国国内出现了中止中美元首会晤的声音。[3] 至此，中美网络安全关系已经剑拔弩张。

在中美两国元首的直接指示下，两国特使围绕网络安全问题进行了互动。2015年8月30日，时任美国总统国家安全事务助理赖斯（Susan Rice）访华，与中方谈到了包括网络安全在内的一系列敏感问题，但是，两国官员在记者面前并没有提及任何在网络攻击方面的分歧。[4] 9月9日，习近平主席特使、中共中央政治局委员、中央政法委书记孟建柱访美。9月11日，中美双方对外宣布就网络安全的突出问题达成重要共识；[5] 同日，美国总统奥巴马到米德堡军事基地发表讲话，称中国针对美国的“网络攻击”“无法接受”，“我们可以选择在这一领域展开竞争——我保证，只要我们想赢，就一定能赢。”不过，“还有另外一种选择，我们可以达成某种共识，确认网络战无益于任何一方，然后建立某些基本的行为准则。”[6] 9月22日，习近平主席访美。在四天行程中，习近平在四个不同场合

1 Kristin Finklea, Eric A. Fischer, Susan V. Lawrence, and Catherine A. Theohary, “Cyber Intrusion into U.S. Office of Personnel Management: In Brief,” Congressional Research Service, July 17, 2015, p. 2, https://digital.library.unt.edu/ark:/67531/metadc743551/m1/1/high_res_d/R44111_2015Jul17.pdf, 2021-05-19.

2 Ellen Nakashima, “U.S. Developing Sanctions against China over Cyberthefts,” *The Washington Post*, August 30 2015, https://www. washingtonpost.com/world/national-security/administrationdeveloping-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html, 2021-05-09.

3 Nick Gass, “Susan Rice Headed to China Later This Week,”Polling Center, August 25, 2015, https://www.politico.com/story/2015/08/susan-rice-to-china-121714, 2021-05-19.

4 Edward Wong, “National Security Adviser Meets With Chinese President Before His U.S. Visit,” *The New York Times,* August 28, 2015, https://www.nytimes.com/2015/08/29/world/asia/susan-rice-xi-jinping-china.html, 2021-05-09.

5 2015年9月9日至12日，习近平主席特使、中共中央政治局委员、中央政法委书记孟建柱，率公安、安全、司法、网信等部门有关负责人访问美国，同美国国务卿克里、国土安全部部长约翰逊、总统国家安全事务助理赖斯等举行会谈，就共同打击网络犯罪等执法安全领域的突出问题深入交换意见，达成重要共识。“U.S., Chinese Officials Meet on Cyber Security Issues: White House,” Reuters, September 13, 2015, https://www.reuters.com/article/idUSKCN0RC0S420150913, 2021-05-09;《孟建柱访美就共同打击网络犯罪开展执法合作》，新华网华盛顿2015年9月12日电，http://www.xinhuanet.com//world/2015-09/12/c_1116543523.htm，2021年5月19日登录。

6 “Obama: China Cyber Attacks ‘Unacceptable’,” BBC News, September 12, 2015, https://www.bbc.com/news/world-us-canada-34229439, 2021-05-09.

谈论了互联网问题，包括《华尔街日报》书面采访[1]、西雅图欢迎晚宴[2]、中美互联网论坛[3]以及两国元首会晤[4]。访美期间，习近平反复强调，中美之间要合作，不要对抗。9月25日，中美双方就网络安全问题达成重要共识，[5]标志着一度白热化的中美网络对抗缓和下来。双方达成了标志性的协定，两国政府[6]承诺均不得从事或者在知情情况下支持网络窃取知识产权，承诺不将关于外资的国家安全审查范围泛化。除此之外，双方决定在网络安全信息共享、网络犯罪调查、网络空间国家行为规范等领域开展合作。

奥巴马执政时期，中美网络间谍争端的解决被广泛认为是一个成功的网络空间危机管理案例。此次危机的化解直接得益于中美双方首脑的直接努力，而根源在于中美在战略上互有需求。

奥巴马执政时期，中美网络间谍争端的解决被广泛认为是一个成功的网络空间危机管理案例。此次危机的降级和平息直接得益于中美双方领导人的直接努力，而危机管理成功的根源在于中美在战略上互有需求。双方需要在经济增长、地区稳定和气候变化等议题上持续合作。中美两国的决策者并不希望网络问题脱离中美关系的正常轨道，或干扰中美在其他广受关注的问题上的合作。[7]

此次危机缓和之后，中美加强了两方面的合作，使得中美网络争端在奥巴马执政后期，基本处于可控状态。一是建立了中美打击网络犯罪及相关问题的高级别联合对话机制。[8] 在2015年到2017年的三次对话中，第三次联合对

1《习近平接受〈华尔街日报〉采访》，新华网，2015年09月22日，http://www.xinhuanet.com/world/2015-09/22/c_1116642032.htm，2021年5月19日登录。

2《习近平出席西雅图参加欢迎宴会并发表演讲》，央广网，2015年9月23日，http://china.cnr.cn/NewsFeeds/20150923/t20150923_519951619.shtml，2021年5月19日登录。

3《习近平出席中美互联网论坛：中国倡导建设和平、安全、开放、合作的网络空间》，央广网，2015年9月24日，http://china.cnr.cn/gdgg/20150924/t20150924_519955675.shtml，2021年5月19日登录。

4《习近平：增强中美战略互信，推动中美新型大国关系不断向前发展》，新华社，2015年9月25日，http://www.gov.cn/xinwen/2015-09/25/content_2938968.htm，2021年5月19日登录。

5《习近平主席对美国进行国事访问中方成果清单》，新华社，2015年9月26日，http://www.gov.cn/xinwen/2015-09/26/content_2939210.htm，2021年5月19日登录。

6 Elizabeth Thomas, "US-China Relations in Cyberspace: The Benefits and Limits of a Realist Analysis," *E-International Relations*, August 28, 2016, p.3, https://www.e-ir.info/2016/08/28/us-china-relations-in-cyberspace-the-benefits-and-limits-of-a-realist-analysis/, 2021-05-09.

7 Tang Lan, and Adam Segal, "Reducing and Managing U.S.-China Conflict in Cyberspace," *NBR Special Report* no. 57, April 15, 2016, p.45, https://www.nbr.org/wp-content/uploads/pdfs/publications/special_report_57_us-china_april2016.pdf, 2021-05-09.

8 在中美打击网络犯罪及相关问题的高级别联合对话机制中，中方代表来自中央政法委、公安部、外交部、工业和信息化部、国家安全部、司法部和国家互联网信息办公室；美方代表来自司法部、国土安全部、国务院、国家安全委员会和美国情报机构。U.S. Department of Justice, "First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes," December 2, 2015, https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0, 2021-05-09.

话被认为是一个里程碑，[1] 双方同意建立网络安全高级专家组讨论网络空间国际规范，[2] 并启动了打击网络犯罪的中美热线。[3] 这一机制使得中美在网络领域建立起了工作层级的沟通渠道。二是中美互联网企业签约了大量的合作项目，包括微软和中国电子科技集团公司共同开发中国政府版 Windows 10操作系统，微软和百度共同开发 Windows 10搜索引擎，思科和浪潮共同开发云服务，易安信（EMC）和联想在数据存储项目上的合作，以及甲骨文和腾讯在数据库项目上的合作。双方互联网企业的深度合作对中美网络空间关系起到了压舱石的作用。

（三）特朗普执政时期

特朗普执政时期，中美网络争端扩展到信息和通信技术产业（Information and Communications Technology, ICT 产业），包括相关的技术、产品和服务。 在这一时期，中国进入产业互联网时代。中国政府提出“以信息化驱动现代化，建设网络强国”，[4] 致力于“推动互联网、大数据、人工智能和实体经济深度融合”。[5] 特朗普上台后将中国界定为“战略竞争者”，确定了“全政府”对华竞争策略，对华发动贸易竞争，同时综合利用经济、法律、外交、安全等政策工具加大在科技领域对中国的打压，推动在科技、产业方面与华“脱钩”，限制中国高科技产业的发展。在此背景下，两国在信息和通信技术领域爆发了激烈的斗争。

2018年8月，美国商务部以损害国家安全为由，对参与军民融合的中国科技企业采取出口管制、限制进口、扩大投资审查、撤销运营牌照、强制出售等经济制裁措施，严重影响了企业的正常运营；11月，美国司法部发布“中国行动计划”，对中国所谓“商业间谍行为”展开重点执法及调查活动，同时调查美国高科技产业受到中国对其进行投资并购的威胁、美国高科技企业供应链安全受到的威胁和出现“非法代理人”的情况。2020年，美国政府在“清洁5G”倡议的基

1 U.S. Department of Justice, “Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues,” December 8, 2016, https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues, 2021-05-09.

2 U.S. Department of Justice, “Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue, ” June 14, 2016, https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue, 2021-05-09.

3 U.S. Department of Justice, “Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues,” December 8, 2016, https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues, 2021-05-09.

4 中共中央办公厅、国务院办公厅：《国家信息化发展战略纲要》，http://www.gov.cn/gongbao/content/2016/content_5100032.htm，2021年5月19日登录。

5 习近平：《决胜全面建成小康社会 夺取新时代中国特色社会主义伟大胜利——在中国共产党第十九次全国代表大会上的报告》，www.xinhuanet.com//politics/19cpcnc/2017-10/27/c_1121867529.htm，2021年5月19日登录。

础上追加“清洁互联网”计划，限制中国互联网企业开展海外业务。对此，中国外交部和商务部采取了相应反制措施；同时，中国强调依靠科技自立自强来确保产业链、供应链安全，强调建立“双循环”新发展格局。中美围绕信息和通信技术供应链安全争端的背后，实际是两国产业和技术上的竞争。

随着美国在信息和通信技术领域持续打压中国企业，双方在网络空间中冲突升级的风险不断增加。美国大幅调整国防部网络安全战略，提出了极具进攻性的“持续交手”(persistent engagement) 和“前置防御”（defense forward）政策，[1] 并且通过《2019财年国防授权法案》及2018年8月特朗普签署的关于“美国网络行动政策”的第13号国家安全总统备忘录，简化了国防部发起进攻性网络行动的审批程序。这不仅增加了中美军事部门间的敌意，也提高了双方在网络领域动用国家力量的可能性。

特朗普执政时期，中美在信息和通信技术领域的冲突是一个失败的危机管理案例。从危机管理的角度看，中美在信息和通信技术领域冲突不断恶化的原因有四点：一是美应对中方的战略定位具有强烈的对抗性。美国将大国竞争列为国家安全战略的首要关切，2017年12月的美国《国家安全战略报告》和2018年的美国《国防战略报告》都明确聚焦与中俄的大国战略竞争。[2] 中国被视为挑战美国实力、影响力和利益，试图损害美国安全和繁荣的长期战略竞争对手。在此大背景下，美国担心中国的军事现代化，认为中国是美国在网络领域最主要的安全挑战者。[3]

二是网络安全问题的泛化。特朗普政府将网络安全问题与经济、贸易、科技、甚至意识形态捆绑在一起，使网络安全问题出现了前所未有的泛化和政治化。[4] 当网络问题演变成政治问题，其解决必然需要政治意愿和议程。在美国将中国看作首要对手并对华采取极限施压策略的背景下，网络安全被特朗普用作与中国开展贸易战和科技战的抓手。在此情形下，美方难以产生控制中美在信息和通信技术领域冲突升级的意愿。

三是沟通渠道几乎全部中断。特朗普就任美国总统后，中美于2017年10月4日举行了首轮执法与网络安全对话。新机制延续了原有的打击网络犯罪相关事

1 U.S. Cyber Command, “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command, ” March 23, 2018, https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf, 2021-05-09.

2 U.S. Congressional Research Service, “Renewed Great Power Competition: Implications for Defense—Issues for Congress,” Updated March 4, 2021, https://crsreports.congress.gov/product/pdf/R/R43838, 2021-05-09.

3 Lyu Jinghua, “Keeping China–U.S. Cyber Conflict off the Cards,” January 11, 2019, Carnegie Endowment for International Peace，https://carnegieendowment.org/2019/01/11/keeping-china-u.s.-cyber-conflict-off-cards-pub-78124, 2021-05-09.

4 唐岚：《从政策演进轨迹分析拜登政府的“网络安全观”》，《中国信息安全》，2021年第2期，第77—80页。

项的高级别对话，但美方认为该机制无法将网络空间规范、信息和通信技术贸易等问题纳入其中。随着中美关系的恶化，中美之间的四个高级别对话机制，包括外交与安全对话、全面经济对话、执法与网络安全对话、社会与人文对话，都遭到特朗普政府单方面中断。中美之间的90多个政府间交流机制均处于休眠状态，[1] 这也加剧了双边误判和冲突升级的风险。

四是源于信息通信技术本身的特殊性。信息通信技术是构建网络空间的物质基础，当网络空间与现实世界加速融合时，信息通信技术客观上已经成为“地缘政治力量的来源”[2]。这种新的力量可以作用于经济、民用关键基础设施、民意（舆论），也可以影响军事系统。正如学者拉什·多希（Rush Doshi）和凯文·麦吉尼斯（Kevin McGuiness）认为，“对全球电信网络的控制是一种政治权力”，“争夺电信技术标准主导权决定了国家的网络领导权”。[3] 同时，以信息通信技术为代表的战略新兴技术将继续开辟人类生产生活的新方式，赋予经济发展以新动力，这方面的技术优势将转化为一国长期的经济优势和军事优势。美国国家人工智能安全委员会（NSCAI）向国会提交的2021年度最终建议报告指出：“巨大的技术机会与战略脆弱性时刻保持一致。中国是一个拥有实力、人才和雄心的竞争对手，可以挑战美国的技术领先地位、军事优势和更广泛的世界地位。”[4] 当美国认为中国“处于人工智能、5G和量子计算等信息技术的前沿”[5] 时，遏制中国相关技术及产业发展，成为美国保持自身科技优势的必然选择。正因如此，中美在信息和通信技术领域的冲突不可能被成功管理。

1 The White House, “Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting,” June 8, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-, 2021-05-09.

2 Thomas F. Lynch III, ed., *Strategic Assessment 2020: Into a New Era of Great Power Competition*, National Defense University Press, 2020, p.139, https://ndupress.ndu.edu/Portals/68/Documents/Books/SA2020/Strategic-Assessment-2020.pdf?ver=-NTckVdG56-CfFYJ73PTgg%3d%3d, 2021-05-09.

3 Rush Doshi, and Kevin Mcguiness, “Huawei Meets History: Great Powers and Telecommunications Risk, 1840-2021,” Brookings Institution, March 2021, pp.2-5, https://www.brookings.edu/wp-content/uploads/2021/03/Huawei-meets-history-v4.pdf, 2021-05-09.

4 National Security Commission on Artificial Intelligence, *Final Report: National Security Commission on Artificial Intelligence*, p.19, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf, 2021-05-09.

5 Martijin Rasser, and Megan Lamberth, “Taking the Helm: A National Technology Strategy to Meet the China Challenge,” Center for a New America Security, January 2021, p.10, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Taking-the-Helm_FINAL-compressed.pdf?mtime=20210113105310&focal=none, 2021-05-09.

三、中美网络空间危机管理未来面临的主要挑战

如何处理对华关系是拜登政府面临的重要议题。由于美国两党对“中国威胁”有着高度共识，拜登政府在“回归”正常外交时，仍然会继承特朗普政府对华政策的一些要素。当美国认为“中国对美国的每一个重大的国家利益都产生了深刻的影响”[1] 时，网络空间可能演变为“大国竞争的另一个决定性的维度”[2]，无疑将成为中美竞争的一个主战场。

在奥巴马执政时期，美国对华挑起网络间谍争端，反映了美国政府“基于对中国网络能力增长和网络安全战略选择的应对，特别是对中国提出的网络强国战略可能对美形成全面挑战的防范”。[3] 在特朗普任内，中美网络关系受到贸易战、科技战和新冠肺炎疫情等诸多因素的挑战，呈现出高度竞争甚至是对抗的态势。由于网络安全与国家安全高度关联，拜登政府不会对特朗普政府的网络安全问题做出剧烈的调整，中美网络空间竞争的主基调不会发生本质变化。[4]

未来，中美网络空间博弈将继续围绕网络情报斗争、关键基础设施攻防、信息干预、网络力量对抗及国际规则制定展开，并更多体现为围绕供应链安全、知识产权保护、技术标准制定、信息和通信技术产业发展等方面的科技竞争。

总体而言，中美网络空间博弈将继续围绕网络情报斗争、关键基础设施攻防、信息干预、网络力量对抗及国际规则制定展开。同时，由于以信息通信技术为代表的新兴技术竞争成为中美战略竞争的重要组成部分，中美网络空间博弈将更多体现为围绕供应链安全、知识产权保护、技术标准制定、信息和通信技术产业发展等方面的科技竞争。从危机管理的视角来看，要防止中美网络空间竞争引发两国关系恶化、甚至走向全面对抗，中美两国还需要着力解决战略误解、争议政治化、沟通失灵等问题。中美网络空间危机管理未来面临的主要挑战包括：

首先，如何解读对方网络战略意图。网络安全是中美关系中的一项新议程。中美“在网络空间的相互不信任不断增加，并对彼此长期战略意图产生深深的负

1 Washington International Trade Association, “The Longer Telegram: Toward a New American China Policy,” January 28, 2021, p.6, https://www.wita.org/atp-research/new-american-china-strategy/, 2021-05-09.

2 John Thornhill, “China is Setting itself up to Win Cold War 2.0,” *Financial Times,* June15, 2020, https://www.ft.com/content/b6c5558e-ba0e-4381-b2b4-1acceb2ab484, 2021-05-19.

3 汪晓风：《中美经济网络间谍争端的冲突根源与调适路径》，《美国研究》，2016年第5期，第102页。

4 陈东晓、鲁传颖：《竞争但不失控：共建中美网络安全新议程》，上海国际问题研究院，2021年2月，第1页，http://www.siis.org.cn/Research/Info/5258，2021年5月9日登录。

面理解”。[1] 网络安全本身的复杂性及其所带来的深刻影响，使得传统的知识结构和认知模式都难以简单地应用到对对方网络战略的判断中。[2] 中国将信息和通信技术及其应用看作是经济发展的新引擎，希望以新兴技术促进经济发展，提高经济增长的质量。但美国对此有不同的理解，认为中国“要寻求在技术上超越美国，从而取代美国成为世界经济强国”[3]；中国将“利用新兴技术实现其国家优势，使其他国家处于劣势”[4]。

中美在网络安全和军事安全的政策上存在差异。中国坚决反对将网络空间军事化，反对一切形式的网络战备，强调国防建设中的网络防御。[5] 但美国认为，中国网络力量发展“不透明”，故意掩盖网络军事力量发展，意在利用网络空间的不对称优势给美国制造战略突袭；担心中国具有利用网络手段破坏美国太空资产、核武器系统的能力，与美构建类似核领域的相互威慑。对于美国公开承认拥有“世界上最成熟、最先进的网络军事能力”，[6] 中方则认为，美国网络军事上的“透明”是一种展示实力的威慑手段。对于美军网络司令部提出的“前置防御”和“持续交手”战略概念，中国学者认为，其核心思想是美军网络作战力量要在网络空间与对手保持持续的对抗，采取持续的竞争性网络行动获得持续的战略优势。[7]

所有这些分歧和战略认知上的差距都会影响双方对彼此战略意图的判断，也决定了双方究竟有多大动力避免冲突的升级。

其次，如何避免科技竞争意识形态化。美方把网络黑客攻击、数据安全、新兴科技发展等问题与意识形态问题联系在一起，甚至认为中美在网络治理上的差异反映了两国意识形态和发展模式的不同，把这种差异夸大为“道路之争”。例如，2021年美国国土安全部发布的“应对中国威胁的战略行动计划”，称中国采用灰色区域战略开辟新战场，从而对美国造成五个方面的不利影响，其中包括

1 Kenneth Lieberthal and Peter W. Singer, “Cybersecurity and U.S.-China Relations,” Brookings Institution, February 2012, p. IV. https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf, 2021-05-09.

2 鲁传颖：《中美关系中的网络安全困境及其影响》，《现代国际关系》，2019年第12期，第20—21页。

3 Washington International Trade Association, “The Longer Telegram: Toward a New American China Policy,” p.6.

4 Samuel J. Brannen, Christian S. Haig, Katherine Schmidt, and Kathleen H. Hicks, “Twin Pillars: Upholding National Security and National Innovation in Emerging Technologies Governance,” Center for Strategic & International Studies, January 23, 2020, p.3, https://www.csis.org/analysis/twin-pillars-upholding-national-security-and-national-innovation-emerging-technologies, 2020-05-09.

5《新时代的中国国防》，中华人民共和国国防部，2019年7月24日。http://www.mod.gov.cn/regulatory/2019-07/24/content_4846424_3.htm，2021年5月19日登录。

6 Cyberspace Solarium Commission, “Transition Book for the Incoming Biden Administration,” January 19, 2021, p.10, https://www.solarium.gov/#h.jlr70j8saqnt, 2021-05-09.

7 鲁传颖：《保守主义思想回归与特朗普政府的网络安全战略调整》，《世界经济与政治》，2020年第1期，第67—68页。

“中国利用信息收集威胁美国公民隐私以及信息安全”[1]。而给中国的数字技术发展和治理贴上意识形态的标签[2]也很可能成为拜登政府继续压制中国科技公司的政策借口。

理论上，在危机中追求有限目标和使用有限手段是危机管理的两个政治要件，[3]而美方过度关注网络意识形态问题则与这两个政治要件背道而驰。一方面，意识形态化容易让对手感到其根本利益受到威胁，导致危机中双方突破原有的战略目标，推动冲突快速升级。另一方面，意识形态化容易导致己方在危机互动中反应过度，减少对网络行动的限制，扩大网络行动的范围，通过增加网络行动的频率来获得自身在网络安全领域的安全感。

最后，如何在网络空间竞争中达成战略默契（tacit agreement）。在参与制定“持续交手”战略的美国学者费舍尔凯勒（Michael P. Fischerkeller）看来，网络空间是一个特殊的战略竞争空间，介于作战的限制条件和低于战争门槛的作战行动之间。通过默许的竞争（tacitly agreed competition），竞争方可以找到不明说的可接受 / 不可接受的网络空间竞争行为，从而在达成不明说的君子协定的同时，小心地避免与武装攻击相当的行动。[4] 但现实并未如美国政策制定者所愿。2019年6月，美国在俄罗斯电网系统里放置进攻性恶意软件，以防止俄罗斯在2020年美国大选时在美国的关键州实施选择性停电。[5] 不过，按照美国的说法，2020年底俄罗斯黑客通过太阳风（Solarwinds）供应链网络攻击已经建立了打击美国电力、能源、水利、通信等关键基础设施的能力。[6] 而且根据火眼公司 CEO 凯文·曼迪亚2021年2月国会听证会上的证词，“攻击者疑似在2019年10月进行了一次‘预演’来进行技术测试，然后在2020年3月至6月之间开始实际攻击”。[7] 此轮美俄

1 U.S. Department of Homeland Security, “DHS Strategic Action Plan to Counter the Threat Posed by the People’s Republic of China,” January 12, 2020, p.7, https://www.dhs.gov/sites/default/files/publications/21_0112_plcy_dhs-china-sap.pdf, 2021-05-09.

2 Erol Yayboke and Sam Brannen, “Promote and Build a Strategic Approach to Digital Authoritarianism,” Center for Strategic & International Studies, October 15, 2020, p.1, https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism, 2021-05-09.

3 Alexander L. George, ed., *Avoiding War: Problems of Crisis Management,* Westview Press, 1991, p. 24.

4 Michael P. Fischerkeller and Richard J. Harknett, “Through Persistent Engagement, the U.S. Can Influence ‘Agreed Competition’,” *Lawfare*, April 15, 2019, https://www.lawfareblog.com/through-persistent-engagement-us-can-influence-agreed-competition, 2021-05-09.

5 David E. Sanger and Nicole Perlroth , “U.S. Escalates Online Attacks on Russia’s Power Grid”, the New York Times, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html, 2021-05-09.

6 U.S. the Cybersecurity and Infrastructure Security Agency, “Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)”, January 05, 2021, https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure, 2021-05-09.

7 Scott Ferguson, House SolarWinds Hearing Focuses on Updating Cyber Laws, February 26, 2021, https://www.databreachtoday.com/house-solarwinds-hearing-focuses-on-updating-cyber-laws-a-16078, 2021-05-09.

之间的网络较量说明，“持续交手”战略不仅无法促成网络空间竞争中达成战略默契，反而促使竞争方做“最坏情况”的打算。

如果在同中方互动过程中，美方继续采取一系列点名羞辱（naming and shaming）、极限施压等方式，那么，中美之间将很难达成战略默契，也难以就军事等高政治领域的问题达成有效的制度安排。

四、促进中美网络空间危机管理的建议

中美是全球网络空间中最重要的两个大国，双方都前所未有地依赖网络空间，并给予网络空间极大的重视。2011年美国颁布的《网络空间国际战略》提出打造一个“和平、可靠的网络空间”。[1] 中国在《网络空间国际合作战略》中指出，致力于“共同构建和平、安全、开放、合作、有序的网络空间”。[2] 通过加强网络空间危机管理，共同构建一个和平与可信赖的网络空间符合中美共同的利益。

第一，建立关于危机管理基本原则的共识。尽管中美在网络领域的冲突越来越多，涉及的领域越来越广泛，但双方还缺乏危机管理的基本共识。这背后折射出双方在网络战略意图和网络军事安全政策方面存在深层差异，以及双方在沟通机制等方面的不足。危机管理基本共识的缺乏阻碍了双方在网络空间危机管理领域进行合作。

网络空间危机管理要想获得成功，需要遵循危机管理的基本规律。考虑到网络空间的特殊性，为有效控制网络冲突，网络空间危机管理需要把握以下四个一般性原则：（1）双方需要从外交层面高度重视危机管理的最基本要求，包括正确理解对方在网络空间中的利益诉求，准确判断对方网络政策的意图；（2）在提出相关政策时要给对方留出体面妥协的退路，避免使用点名羞辱、极限施压等方式，以免导致矛盾积累、激化，最终与解决问题的目标背道而驰；（3）避免以武力来处理危机和急于发出最后通牒，要给对方留有足够的时间来修正政策，这就意味着双方需要正确地认识到，网络安全是一个跨领域的议题，其决策过程往往涉及跨部门的协调，这在客观上大幅增加了决策难度，很难在短期内对对方的诉求做出回应；（4）避免以零和博弈的原则处理危机。[3]

此外，由于网络安全涉及多个议题领域，中美网络空间危机管理还需要特别

1 The White House, “International Strategy for Cyberspace,” May 1, 2011, p.3, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 2021-05-09.

2 中国外交部、国家互联网信息办公室：《网络空间国际合作战略》，新华网，2017年3月1日，www.xinhuanet.com/2017-03/01/c_1120552767.htm，2021年5月19日登录。

3 丁邦泉主编：《国际危机管理》，北京：国防大学出版社，2004年版，第32—35页；Alastair Iain Johnston, “The Evolution of Interstate Security Crisis-Management Theory and Practice in China,” *Naval War College Review*, Vol. 69, No. 1, p. 5, https://digital-commons.usnwc.edu/nwcreview/vol69/iss1/, 2021-05-15.

防止危机向其他领域外溢。这正是议题控制的意义所在，就事论事，防止议题的政治化，尽可能低政治化处理。同时，网络安全的专业性比较强，在开展危机管理时，需要实行专业部门的归口管理。但是，受到危机直接冲击的部门，或者利益受损部门最好能退出危机处理的领导地位，从而避免意气用事，影响大局。

第二，发挥学术交流机制在危机管理中的作用。在危机管理中，危机当事国为了显示某种决心，通常会采取抗议、谴责、召回大使、制裁等具有对抗性的行动。而这些行动无疑阻碍了正式的直接沟通渠道发挥作用。因而，国家间要尽可能建立多元化的沟通机制，保证在正常的沟通渠道阻断时，还能有畅通的民间渠道。

在民间层面，中美之间有两个机制对稳定中美网络空间关系作出了巨大贡献。一个是中美互联网论坛，另一个是中美网络安全“二轨对话”。前者由中国互联网协会同美国微软公司于2007年创建，旨在促进中美两国互联网业界的交流与合作，2015年后未再举办；后者由中国现代国际关系研究院与美国战略与国际问题研究中心于2009年共同创办，现已成为两国学界、战略研究界交换彼此关切的重要平台。

中美两国的学界如能以分歧点为牵引，开展深入交流和联合研究，不仅有利于深入了解双方的矛盾、关切和共识，寻找在政策层面双方可以接受的解决方案，更重要的是可以促进双方决策层的良性互动，为双边合作进行危机管理奠定基础。[1] 中美在网络空间有分歧和矛盾，也有共识和共同利益，双方需要也能够找到在网络空间实现竞争性共存的路径。中美能否实现网络空间良性互动，能否以联合国负责任国家行为框架为基础，寻找双方愿意合作的事项，制定降低冲突风险的措施，这些都需要中美学界共同研究并挥作用。

第三，采取措施建立信任。中美之间可以通过信任建立措施增加互信、减弱双边对抗强度。信任建立措施可以是军事的，也可以是非军事的；可以是单边的，也可以是双边的、多边的。例如，美国网络空间日光浴委员会（Cyberspace Solarium Commission）建议拜登政府，重新评估美军网络空间行动的授权，保持对军事行动的政治控制，[2] 这就是一项非常积极的、能有效避免网络行动导致危机快速升级的单边信任建立措施。

对于网络军事信任建立措施，双方可以就“可接受的行为规范、使用武力的门槛和作战条令的透明度等内容展开正式讨论”[3]。比如，中美双方可在2014年两军签署的《关于建立重大军事行动相互通报信任措施的谅解备忘录》和《关于

1 许蔓舒:《促进中美网络空间稳定的思考》,《信息安全与通信保密》，2018年第6期，第25—28页。

2 Cyberspace Solarium Commission, “Transition Book for the Incoming Biden Administration,” p.11.

3 Adam Segal, “Stabilizing Cybersecurity in the U.S.-China Relationship,” *The National Bureau of Asian Research (NBR) Report*, September 4, 2015, p.3, https://www.nbr.org/publication/stabilizing-cybersecurity-in-the-u-s-china-relationship/, 2021-04-06.

海空相遇安全行为准则的谅解备忘录》的基础上，研究增加“网络安全危机通报”和“网络空间安全行为准则”的附件。[1] 考虑到网络信息技术给核领域带来的风险，中美两国可以在多边框架下讨论并共同推动关于禁止对核武器使用网络攻击的国际协定。[2]

对于网络非军事领域的信任措施，由于维护网络空间的开放、和平与安全是中美的共同利益，双方可以在全球经济高度依赖的国际关键基础设施保护方面加强合作。例如，在全球进入万物互联的时代，网络漏洞已经成为影响一个国家经济发展和国计民生的重要网络安全风险，也是国际社会共同面临的网络空间治理难题。针对这种网络安全本源性的难题，中美两国可以共同推动国际社会构建一个互利的、稳定运行的漏洞管理国际机制，以漏洞管理为突破口落实负责任的网络空间行为规范，并以此作为构成网络空间国家间信任的基点，消除信息通信技术和依赖这些技术的基础设施所面临的潜在威胁。

1 陈东晓、鲁传颖：《竞争但不失控：共建中美网络安全新议程》，第6页。

2 阿里·莱维特等：《关于中美建立网络—核指挥控制与通信系统稳定性的报告》，上海国际问题研究院与卡内基国际和平研究院联合报告，2021年4月，第25—28页，http://www.siis.org.cn/Research/Info/5321，2021年5月19日登录。