全球网络空间规则制定的合作与博弈

郎　平

【内容提要】随着互联网在国家政治经济生活中的作用逐渐加强，国家对高度依赖网络的不安全感也日趋增加，由此引发的国家间冲突使制定全球网络空间规则显得非常必要且迫切。在应对网络有组织犯罪和网络恐怖主义中，以国家间合作为主流，而一般性网络冲突和网络战则体现出国家间利益的博弈。网络空间规则的制定主要围绕技术、军事安全和对策三个层面展开博弈。国家间的博弈主要表现为美国与欧洲对互联网主导权的争夺以及美欧与中俄在治理理念和模式上的对立。目前，网络空间规则的制定仍然处于“规范兴起”的起始阶段，要达成一项全球网络空间协定还面临诸多困难和挑战，但是，明晰彼此底线并努力寻求共识应该成为推动网络空间规则制定的首要目标和任务。中国作为一个新兴大国，要实现向网络强国迈进的目标，应当积极关注和参与不同国际平台上有关网络规则的讨论，开展国际合作的同时勇于承担更多的国际责任，在确保国家安全的前提下，推动互联网的可持续发展。

【关键词】网络规则　网络治理　网络安全　联合国

【作者简介】郎平，中国社科院世界经济与政治研究所国际政治理论研究室副主任、副研究员

【中图分类号】D815/G20

【文献标识码】A

【文章编号】1006-1568-(2014)06-0138-15

随着网络安全问题逐渐进入国家安全的视野，国际关系中源于网络安全问题的冲突和摩擦日益增加。军事领域网络攻防能力的竞争和网络间谍活动都不同程度上导致国家间关系的紧张。2014 年 5 月，美国司法部以网络盗窃为由对五名中国军官提起诉讼，更凸显了网络安全在大国关系中的重要性。然而，当前网络空间的无序状态如同众多车辆在四通八达的道路上快速行驶，却没有统一的交通规则，任何一起交通事故都可能引发严重的后果。目前，国际社会围绕网络空间规则制定的合作与博弈正在全球展开。

一、网络空间安全问题及治理现状

网络空间进入国际关系的视野是在 1991 年海湾战争之后。在军事战略家们看来，强大的军事力量已不再是战场获胜的唯一法宝，赢得信息战和确保信息主导权的能力日益重要。1993 年，美国兰德公司的两位研究员约翰·阿尔奎拉（John Arquilla）和戴维·龙费尔特（David Ronfeldt）发表了一份研究报告称“网络战即将到来”。[①] 一时间，有关计算机、国家安全和网络空间的争论甚嚣尘上，网络战成了最热门的流行语。但由于网络战似乎还仅仅是一种“臆想”，因而很快沉寂下去。直到 2007 年爱沙尼亚危机、2008 年格鲁吉亚战争和 2010 年伊朗核设施受到“震网”病毒攻击并且遭受重大损失，网络安全威胁才开始鲜活起来，真正进入国家安全的议程。

网络空间具有跨国性、隐蔽性、军用和民用设施混淆、网络攻击门槛低等特点。根据网络空间对国家安全的威胁程度可大致划分为：（1）有组织的网络犯罪，如洗钱、贩毒、贩卖人口、走私、金融诈骗等传统犯罪活动的虚拟化；（2）网络恐怖主义，既包括针对信息及计算机系统、程序和数据发起的恐怖袭击，也包括恐怖组织借助网络空间进行传统恐怖主义活动的宣传和动员等；（3）一般性的网络冲突，这类冲突烈度较低，还不至于引发国家间的军事对抗，但是却上升到了政府间的外交层面，如中美之间的网络间谍案、欧美之间因网络监听引发的冲突等；（4）网络战，即至少有一方是国家行为体参与的网络空间的军事对抗，由于上升到战争行为，网络战对国家安全威

[①] John Arquilla and David F. Ronfeldt, “Cyberwar is Coming!” *Comparative Strategy*, Vol. 12, No. 2, 1993, pp. 141-165.

胁的程度最高，它既可以独立存在，也可以是当代战争中的一部分。

从国家间互动的角度来看，网络犯罪和网络恐怖主义是各国普遍面临的安全威胁，国家之间的合作大于冲突；网络战和网络冲突则更多体现为国家间的利益冲突，是竞争性的关系，因而国家间博弈主要在这两个层面上展开。权力与财富、冲突与合作是国际政治的永恒主题。虽然网络空间是一个虚拟的数字化世界，但同样充斥着来自各种利益集团和各类行为体的利益争夺，而国家行为体的介入也令“网络空间”这个原本技术色彩浓厚的领域增添了政治学的色彩。有学者指出，“我们如今再也不能对网络空间的政治特性漠然视之，网络空间正在成为一个由政府、军方、私人企业和公民网络等各种行为体参与的，高度竞争、殖民化和重塑的领域。”①

进入21世纪后，互联网不仅在全球经济和商业往来中发挥越来越重要的作用，对确保国家经济发展、社会稳定和国家安全也日益重要。国家对互联网的依赖程度越深，维护网络安全的需求也就越迫切，“网络主权”或“网络边界”的概念应运而生。如美国学者罗伯特·阿克塞尔罗德（Robert Axelrod）所言，“尽管网络空间并不存在真正的物理边界，但对一国政府而言，网络的每一个节点、每一个路由器、甚至每一次转换均发生在民主国家的主权边界之内，因而它必须遵守该国的法律；网络运行的海底电缆或者卫星连接也同样由某个实体公司所控制，该公司的活动也应遵守所在国家的法律。”② 从这个角度来看，网络空间不可能真正脱离国家政府的约束，国家以行使主权的手段介入网络空间治理也成为必然。无论是维基解密事件还是斯诺登泄密事件，都可以看到政府的干预和介入。正因为如此，网络空间治理从一个技术问题演变为国际关系中一个重要的安全议题，并走上大国外交的舞台。

日益突出的网络安全问题，严重威胁着主权国家的安全，但却没有一套专门适用于网络空间安全的全球行为规范和准则；③ “当前的网络空间就如

① Nazli Choucri, *Cyberpolitics in International Relations*, Cambridge, MA: The MIT Press, 2012, p. 8.

② See P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, New York: Oxford University Press, 2014, p. 182.

③ 2001年11月由欧洲理事会26个欧盟成员国以及美国、加拿大、日本和南非等30个国家的政府官员在布达佩斯共同签署的《网络犯罪公约》，是全世界第一部、也是迄今为止唯一一部针对网络犯罪行为所制定的国际公约。但是，由于它的管辖范围主要针对网络犯罪方面国家间法律与合作的协调，因而也不足以应对网络空间的诸多威胁和挑战。

同 19 世纪初蛮荒的美国西部。”[①] 北约盟军欧洲最高司令、美国海军上将詹姆斯·斯塔夫里迪斯（James G. Stavridis）曾表示：“我们的经济被卷入了互联网的汪洋之中，但这个海洋却不受法律的保护，没有任何行为规范。现在，我们必须开展全球对话来应对这一挑战。”[②] 虽然国际社会在确立全球网络空间规则方面有共识，但对如何制定及制定何种规则却存在严重分歧。

国际社会在现阶段面临的形势与电报发明之后的情形颇为相似。1839 年，首条电报运营线路在英国投入使用，随后在世界范围内扩散，将远隔千里的人们以一种前所未有的方式联系在一起。随着信息通过电报跨越国家边界的传输，问题也产生了：不同的国家收取不同数额的关税，使用不同类型的设备，甚至使用不同的电报码。为解决这种混乱局面，欧洲国家（英国由于其电报网络私营而被排除在外）于 1865 年达成一项要求所有国家必须遵守的统一规范，如国际电报统一关税、所有信息的隐私权保护以及统一使用德国版莫尔斯电码，由此成立了一个新的国家间组织——国际电报联盟（ITU），负责协定管理和监督。作为国家间组织，国际电报联盟在保证全球通信的同时，也保留了国家政府干预的权力。1934 年，国际电报联盟更名为“国际电信联盟”，将电话与无线电纳入管辖范围，并提出“致力于联通世界”的口号。

如今，将世界各地的人们更紧密地联系在一起的互联网出现了。全世界已经有超过 30 个国家制定了有关网络空间或互联网使用的政策。在国际层面，北约、欧盟、上合组织等国际组织也就网络安全展开了不同程度的合作。国际社会尽快达成一项国家间的网络空间行动准则的重要性和迫切性日益凸显，而国家间利益博弈也随之展开。

二、网络空间规则制定的国家间博弈

目前，全球网络空间规则的制定仍然处于初始阶段。费丽莫（Martha

[①] Scott Beidleman, *Defining and Deterring Cyber War*, Strategy Research Project, US Army War College, 2009, p. 21.

[②] House and Senate Armed Services Committees, Testimony of: Admiral James Stavridis, United States Navy Commander, United States European Command before the 113th Congress, March 19, 2013, pp. 28-29, http://www.armed-services.senate.gov/imo/media/doc/Stavridis%2003-19-13.pdf.

Finnemore）和斯金克（Kathryn Sikkink）曾经在《国际规范动力学和政治变革》一文中将规范界定为“某个特定身份的行为体行为恰当的标准”，并将规范的生命周期划分为三个阶段：规范兴起（norm emergence）、规范普及（norm cascade）和规范内化（internalization）。作者认为，欲催生新的规范需要两个条件：一是规范倡导者的劝说；二是规范倡导者发挥影响力的制度平台。[①] 在网络空间，全球规则的倡导者主要是各国政府，制度平台包括联合国、北约、欧盟等国际和地区组织，其中联合国因其广泛代表性是全球规范谈判和讨价还价的最重要平台。从国家间互动的角度来看，网络空间规则制定过程中的博弈主要体现在三个层面：技术、军事安全和对策层面。

（一）技术层面

互联网起源于美国，20 世纪 90 年代之前，互联网一直是一个为科研和军事服务的网络，其治理权主要分为两部分：一是顶级域名和地址的分配；二是互联网标准的研发和制定。90 年代初，美国政府将互联网顶级域名系统的注册、协调与维护的职责交给了网络解决方案公司（NSI），而互联网地址资源分配权则交由互联网数字分配机构（IANA）来分配。互联网运行的另一项重要内容是标准的制定和管理。目前，承担互联网技术标准的研发和制定任务的是 1985 年底成立的互联网工程任务组（IETF），其两个监督和管理机构即互联网工程指导委员会（IESG）和互联网架构委员会（IAB）则共同归属于互联网协会（ISOC）管辖。总部位于美国弗吉尼亚的互联网协会成立于 1992 年，是一个独立的非政府、非营利性的行业性国际组织，它的建立标志着互联网开始真正向商用过渡。由此可见，互联网的控制权虽然归属于独立的非政府组织，但根本上仍是“美国制造”，很大程度上被美国政府所控制。

为了抗议美国政府对互联网的垄断，表明技术专家们在独立和平等的环境中分享互联网技术的愿望，IANA 创始人、协议发明大师乔恩·波斯托（Jon Postel）于 1998 年 1 月 28 日发动了互联网世界的第一次“政变”。他发送了一封机密邮件给掌管着世界上 12 台域名服务器中 8 台的操作员，要求他们重新配置服务器，认定其南加州大学的计算机为主机，而其余 4 台服务器仍然认定美国政府的电脑是主机。由于波斯托在互联网行业的巨大声望，这 8 位

[①] Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” *International Organization*, Vol. 52, No. 4, 1998, pp. 895-896.

操作员冒着被美国政府起诉的危险照做了。这一天，互联网世界一分为二，以实际行动向美国政府宣示，“美国无法从那些在过去 30 年里建立并维持互联网运转的专家们手中掠夺互联网的控制权”。[①] 然而，在美国政府的压力下，此次“试验”仅持续了一周。

1998 年 1 月 30 日，美国商务部公布互联网域名和地址管理“绿皮书”，宣称美国政府享有互联网的直接管理权，遭到几乎所有国家及机构的反对。此时，互联网开始在全球范围内迅速普及，美国政府意识到垄断互联网的局面难以继续。1998 年 6 月，经广泛调研，美国重新发布了互联网“白皮书”，决定成立一个由全球网络商业界、技术及学术各领域专家组成的民间非盈利公司——互联网名称与数字地址分配机构（ICANN），负责接管包括管理域名和 IP 地址分配等与互联网相关的业务。虽然美国商务部不再直接参与机构的管理，但仍然牢牢掌握着 ICANN 的控制权和管理权。[②] 2014 年 3 月 14 日，美国商务部下属的国家电信和信息管理局（NTIA）宣布将放弃对 ICANN 的控制权，但明确拒绝由联合国或其他政府间组织接管，只同意由 ICANN 管理层与全球“多利益攸关方”（Multi-stakeholder）讨论接管问题。[③]

国际电信联盟是联合国机构中唯一涉及网络问题的条约组织，在制定技术标准方面发挥着重要作用。它由不同领域的技术人员管理，每个季度向联合国秘书长提交一份威胁评估报告。国际电信联盟在联合国网络安全领域相当重要，它不仅是一个成员国的组织平台，而且是一个自主的规范倡导者，其主要任务是推进其成员国制定的议程并提出具体倡议。2012 年 12 月，国际电信联盟大会在迪拜举行，俄罗斯、中国以及其他发展中国家倡议将互联网纳入国际电信联盟的管辖范围，允许政府对互联网的运行进行管理，但遭到美国及欧洲国家的强烈反对，它们认为这将改变互联网治理的“无国界”性质，赋予政府干预网络空间的权力。在美欧国家缺席的情况下，国际电信联盟打破传统的一致通过原则，以多数通过方式通过了新协议，但该协议最终

① Singer and Friedman, *Cybersecurity and Cyberwar*, 2014.

② 2014 年 3 月，美国政府发表公开声明，同意放弃对 ICANN 的管理权，但是只允许将管理权转交给某个独立的非政府机构，目前仍未落实。

③ The NTIA,“NTIA Announces Intent to Transition Key Internet Domain Name Functions,” March 14, 2014, http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

能否得到各成员国批准进而生效还面临着很大的不确定性。

在2014年4月于巴西圣保罗召开的全球互联网治理大会上，西方国家与以中俄为首的发展中国家继续展开激辩。虽然美国在 3 月份表示愿意让渡ICANN的管理权，但发展中国家仍希望推进互联网改革，打破美国在互联网标准制定方面的垄断。与此同时，美国和欧盟之间也面临着争夺互联网霸主地位的冲突。2014年2月，德国总理默克尔与法国总统奥朗德在巴黎会晤时专门提出要建设独立的欧洲互联网，取代当前由美国主导的互联网基础设施。美国希望继续掌握互联网的游戏规则制定权，把互联网看作尽可能不对数据跨境传输进行限制的电子商务平台；但欧洲却希望建设独立的欧洲互联网，夺回一些IT主权并减少对外国供应商的依赖。[①]

（二）军事安全层面

军事安全层面的规则制定博弈主要发生在联大第一委员会。[②] 第一阶段的标志性事件是1998年9月23日，俄罗斯在第一委员会提交了一份名为“从国际安全角度看信息和电信领域的发展”的决议草案，[③] 呼吁缔结一项网络军备控制的协定。该决议未经表决就被联合国大会通过，自此被列入联合国大会的议程。但直到2004年，该草案始终没有得到其他国家的响应。

这一时期，俄罗斯与美国的不同立场充分折射出两国在网络空间技术的地位差异。俄罗斯担心美国在互联网空间的优势地位会直接转化为军事上的优势，因此希望通过缔结一项国际协定来限制网络军备竞赛。美国自然不希望缔结一项协定来约束自身的优势，认为这样的条约一旦通过，在增加信息和电信安全的幌子下，会被用来限制信息的自由。美国智库哈德森研究所（Hudson Institute）研究员克里斯托弗·福特（Christopher A. Ford）认为，俄

① 王芳、郑红：《法德探讨建立欧洲独立互联网》，载《人民日报》2014年2月21日，第21版。

② 在联合国框架下，多个部门、附属和专门机构都涉及网络安全的问题，例如大会、安理会、经社理事会、打击跨国有组织犯罪公约缔约方大会等。这些机构对网络安全问题的讨论主要集中在两个层面：一是政治军事层面，例如网络战、网络攻击、网络恐怖主义；二是经济层面，例如有组织的网络犯罪，如毒品、传统的商业犯罪行为。联合国负责网络战规则制定的政府间机构是联合国大会第一委员会，组织平台包括国际电信联盟、联合国裁军研究所和联合国反恐执行工作队。

③ Christopher Ford, “The Trouble with Cyber Arms Control,” *The New Atlantis–A Journal of Technology & Society*, Fall 2010, p. 65.

罗斯对信息战和网络空间的治理模式过于强调控制大众媒体的内容，意图影响国外和国内的看法。[①] 这一时期由于俄罗斯势单力孤，美国对这项议题并不重视，默认了这项议题的存在，是国家间利益冲突的蛰伏期。

第二阶段的标志性事件是 2005 年 10 月 28 日，俄罗斯的决议草案首次被美国否决。从次年开始，决议草案的发起国不再只是俄罗斯，中国、亚美尼亚、白俄罗斯等 14 个国家相继加入。从 2005 年到 2009 年的五年间，俄罗斯决议草案的共同发起国迅速增加到 30 个，而美国则始终保持对立立场。

2004 年，联合国大会成立第一个政府专家小组。[②] 该小组在 2004 年和 2005 年先后召开三次会议，但由于中俄与美国之间严重的利益分歧，未就网络空间的潜在威胁和合作达成最后共识。这一时期，由于互联网迅猛发展，包括中国在内的越来越多的发展中国家意识到网络空间对于国家安全的重要性，希望通过缔结一项网络战的协定来消减美国的网络优势，确保国家安全。而美国当时正处于小布什的第二任期，先发制人战略与对多边主义的厌恶使得美国与联合国的关系处于低谷。双方的冲突焦点集中在国际人道主义法和国际法是否足以防范通信技术被恶意用于政治军事目的，美国认为没有必要重新缔结一项网络战的新协定，现有国际法足以胜任网络空间的行为规范。

第三阶段开始于 2010 年，其标志是美国立场发生转变并首次成为网络安全决议草案的共同提议国，由此提议国扩大至包括俄罗斯、中国、美国在内的 36 个国家。美国立场转变有两个原因：一是奥巴马政府上台后外交战略思路的变化，重视多边主义；二是格鲁吉亚战争使美国看到，缔结新的协定虽然会约束其能力，但也是对类似俄罗斯的国家的有力约束。约瑟夫·奈描述了美俄两国在网络安全问题上的对立和立场变化：“十多年来，俄罗斯一直寻求缔结一个互联网监管的国际条约，禁止使用可以在战争中激活的恶意软件或电子元件，但美国认为禁止网络攻击能力的措施会破坏国家的网络防御能力，并且反对国家互联网审查制度的合法化。尽管如此，美国开始与俄罗斯展开正式对话，甚至倡导缔结一个类似于《日内瓦公约》的国际条约。”[③]

[①] Ibid., p. 59.

[②] 该专家小组成员包括 15 个国家，分别为：美国、英国、德国、俄罗斯、中国、印度、南非、巴西、白俄罗斯、法国、约旦、马来西亚、马里、墨西哥、韩国。

[③] Joseph Nye, *Cyberpower*, Cambridge, MA: Harvard Belfer Center for Science and International Affairs, May 2010, p. 18.

但是，分歧依然存在。2012 年，中国、俄罗斯、塔吉克斯坦和乌兹别克斯坦向联合国提交了一份名为“信息安全国际行为准则”的草案，遭到以美国为首的西方国家的强烈抵制。该文件认为，与互联网有关的公共政策问题的决策权属于各国主权范畴，应尊重各国在网络空间的主权。在治理方式上，中俄主张政府是网络空间治理的最主要行为体，在网络空间履行国家职能，负责信息基础设施的安全和运营，管理网络空间的信息，并依法打击网络犯罪行为。但美国认为，网络空间是由人类创造出来的虚拟空间，具有“全球公域”属性，应将其纳入美国的全球公域战略。网络空间既包括国家行为体，也包括公司、非政府组织、学术团体以及个人，网络空间的治理主体应该是“多利益攸关方”，政府应将同等重要的责任和权利分享给其他行为体。[①]

在此背景下，政府专家小组的工作也开始取得进展。第二个政府专家小组[②]最终在 2010 年提交了报告，就“信息安全领域现存和潜在的威胁是 21 世纪最严峻的挑战”达成一致。报告兼顾各方共同愿景，承认网络空间指证问题的存在及网络空间的两面性，互联网本身是中性的，取决于使用者的意图。2013 年 6 月，第三个政府专家组提交的报告进一步强调恶意使用通信技术的威胁，并且提出加强稳定和安全的合作措施，包括规范、增加透明度的自愿措施、各国信心和信任以及能力建设措施。2013 年 12 月，联合国大会通过第 68/243 号决议，决定成立由 20 名专家组成的第四个政府专家小组，其主要任务是讨论现有国际法能否适用于网络空间，美欧赞成将联合国武装冲突法适用于网络空间，但中俄反对，认为这将导致网络空间的军事化。

（三）对策层面

对于国家间的一般性网络冲突，其解决方式更多是依靠冲突双方的外交磋商，如果不能达成一致，则可能诉诸其他多边途径。中国和美国之间因网络间谍案引发的冲突、美国与欧盟等国家因“棱镜门”监听事件导致的冲突都归为此类。由于这些冲突的起因和情况皆有不同，需要冲突国家之间根据具体情况制定相应的对策。这些冲突的解决办法经由反复的实践而最终沉淀为冲突各方遵守的国际惯例。

---

① 鲁传颖：《试析当前网络空间全球治理困境》，载《现代国际关系》2013 年第 11 期。
② 该工作组于 2009 年开始工作，新增加了爱沙尼亚和以色列等国家。

以中美之间的网络间谍案为例，2014 年 5 月 19 日，美国司法部以网络窃密为由对五名中国军官提出起诉，并在联邦调查局网站上发布了“通缉令”，作为对 2013 年 2 月 19 日美国麦迪安（Mandiant）网络公司报告的回应。尽管美国明知不可能抓捕这五名军官，但此举更多是通过威慑进一步明确美国的强硬立场：“无论在何地，任何个人都不能利用 21 世纪的网络工具使美国利益受损。”中国在第一时间提出抗议，敦促美方立即纠正错误，撤销所谓“起诉”。随后一周，中美交锋不断升级，中国政府宣布暂停中美网络安全小组的活动，政府采购计算机停用 Windows 8 系统，并且所有国外 IT 产品和服务都必须经过安全审查。2 月 26 日，中国互联网新闻研究中心发表了《美国全球监听行动纪录》报告，确认美国在中国进行了大范围的窃听。此外，该问题也很可能会波及在华的美国咨询公司，从而失去中国的国有企业客户。

中美网络间谍案既是网络间谍案件，也可以被看作是知识产权盗窃的经济纠纷，目前有两种可能的解决途径：第一，通过双边磋商，或者恢复中美网络工作组的工作，从而在该框架内解决。或通过更高级别双边会谈，就彼此的底线相互通报并达成一致。中美双方继续双边网络安全对话，即使不能就网络攻击的解决达成一致，也可以就一些攻击行为或非正式的原则达成共识。美国中央情报局前局长迈克尔·海登（Michael Hayden）指出，正如冷战期间美苏两国情报部门在不使冷战升级为“热战”达成共识一样，中美两国虽然对对方网络盗窃商业机密非常不满，但彼此应达成一种共识，明确双方能够容忍的底线，避免形势失控。[①] 非正式的原则固然短期内不能杜绝网络盗窃行为的出现，但却可以作为一种设定的准则，随着时间的推移逐渐加深影响，最终培养一种负责任的意识。

第二，如果双边途径无法达成一致，就很可能要通过其他多边框架加以解决，如援引世贸组织相关知识产权的条款。美国一些学者认为，中美之间如果不能通过双边对话达成一致的话，可以在世贸组织框架内对中国以“盗窃知识产权”提起诉讼。中国在 2001 年加入世贸组织之后受益匪浅，对世贸组织的身份和形象极为重视，如果在《与贸易有关的知识产权协议》框架下对中国盗窃或者违反知识产权规定提起诉讼，一旦胜诉，就会导致中国数十

[①] Singer and Friedman, *Cybersecurity and Cyberwar*, 2014.

亿美元的损失。在美国学者看来，只有在中国很看重的框架内提起诉讼才能使中国无法回避网络间谍案问题，同时，也给中国政府提供一个“指证”美国政府对中国发动网络攻击的机会，两国可以直接正面交锋，对中国政府来说也不是坏事。[①]

中美网络间谍案是全球网络空间规则制定过程中国家间利益博弈的一个缩影。作为当今世界两个极具影响力的大国，中美在网络空间治理的理念和模式上有着截然不同的立场，这在很大程度上影响到相关对策的制定。斯诺登事件之后，美国的国际形象大为受损，受到多方指责，与欧洲盟友的关系也因网络监听而陷入低谷，美俄关系也因俄罗斯向斯诺登提供避难而雪上加霜。虽然美国在网络空间的主导权方面作出了一定的让步，但中、美、欧、俄等大国之间在网络空间的博弈将会持续。

三、未来走向和挑战

从当前的进程来看，主要大国在制定网络空间行为准则的必要性方面已经达成共识，但对于条约内涵仍存在较大分歧。由于不同的网络空间治理理念和不同的利益考虑，目前各国对达成“全球网络空间协定”的真实态度并不明朗。美国是当今互联网世界的霸主，虽然其政府官方声明希望就网络空间的行为准则达成一致，但实际上并不愿意放弃目前掌控的技术制高点，不希望在绑住自身手脚的同时，给其他国家赶超机会，甚至出现少数国家背弃协定的情况，因此美国更希望维持现状。此外，中俄与美国对协定的诉求也尖锐对立。2009 年，俄罗斯再度提出禁止国家使用任何类型的网络武器和开展网络空间的“军备控制”，但在美国看来，俄罗斯的建议虽然约束了国家行为体，但难以限制政府使用“爱国黑客”作为代理人发动网络攻击。美国则更希望通过协定约束网络间谍这种盗窃知识产权的行为和保护脆弱的民用关键基础设施，中国和俄罗斯则担心西方国家借此推销其价值观，侵蚀本国的网络主权。不同的利益诉求和网络空间作为新生事物的“万事开头难”特性，决定了全球协定的达成仍然是长路漫漫。

[①] Ibid.

由于网络空间的特殊性，国际社会很难达成类似 1967 年的《外太空协定》或 1923 年的《海牙航空战公约》的条约。在网络战层面，美国主张将《联合国人道主义法》[①] 适用于网络空间，但人道主义法对网络战的约束也有相当的局限性。例如，网络攻击何时和如何被看做是战争行为？网络空间的一个关键问题是如何区分军用和民用设施。与传统战争不同，网络空间中军用和民用设施的界限并不清晰，网络既可能是民用也可能是军用，如果将该国际法应用到网络空间恐难有效实施。中国和俄罗斯坚持反对将《人道主义法》适用于网络空间冲突，认为这将导致网络空间的军事化。

北约专门研究网络战的卓越协同网络防卫中心邀请了 20 名法律专家，历时三年，于 2013 年 3 月最终完成了《塔林手册：适用于网络战的国际法》。虽然这部手册并非北约官方文件或者政策，只是一个建议性指南，但它被认为是西方第一份公开出版的、系统化的网络战国际法，被誉为网络战领域的“日内瓦公约”。《塔林手册》对网络战一些关键且敏感的概念进行了界定，直指网络安全问题的核心。它规定一国政府不应在知晓的情形下允许在本国领土内或在政府控制下的网络设施被用来对其他国家发动有害的、不合法的攻击行为；国家对指向其来源并且违背其国际义务的网络攻击行动应负有国际法责任；明确了使用武力的若干标准，如当网络攻击行动的规模和效果与使用武力的非网络行动相当时，网络行动就被认为是使用武力，培训和装备持有恶意软件的游击队组织也被看作是使用武力，而政治和经济强制（coercion）不能等同于使用武力，资助黑客集团也不构成暴动的一部分。[②] 必须承认，在制定全球网络空间规则方面，北约走在了其他区域和国际组织的前面。这份规则的制定固然有着强烈的北约色彩，但客观来看，就其框架进行探讨可以在某种程度上推进联合国框架内的谈判。

从目前的形势判断，如果没有突发事件，达成一项各国均能接受的全球网络安全准则可能需要很长时间。但这并不意味着制定网络空间规则的进程将止步不前。按照通常的做法，制定规则首先应该从概念界定开始，但这恰

[①] 《人道主义法》是指出于人道原因而设法将武装冲突的影响限制在一定范围内的一系列规则的总称。它保护没有参与或不再参与敌对行动的人，并对作战的手段和方法加以限制，因此也被称作战争法或武装冲突法。

[②] Michael N Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press, 2013, pp. 29-30.

恰是现阶段网络空间规则制定的难点和障碍。鉴于当前网络安全问题的日益凸显和对国家间关系的消极影响，尽快推动网络空间规则的制定已经成为各国的共识。在这种情况下，网络规则的讨论应避开当前的障碍，从共识开始，率先就各方共同认可的原则、规则和程序初步达成一致。2013 年 10 月首尔网络空间会议通过了《首尔原则》，认为包括《联合国宪章》在内的国际法准则也应适用于国际网络空间，这无疑是一个进步。

联合国大会的报告和决议则采取了模糊和兼顾的做法。2010 年，第一委员会的决议草案不再要求首先对缔结网络军备条约进行概念界定，并且将“国际原则”的目标替换为“国际概念”和“可能的措施”。[①] 2013 年，政府专家组向大会秘书长提交报告，报告称各国政府必须牵头所有努力，但私营部门和民间社会的适当参与将促进合作的有效开展。报告并未就现行国际法是否适用给出明确结论，仅表明这对降低国际和平、安全与稳定的风险至关重要，但并不反对今后另行制定准则。专家组还认为，由国家主权产生的国际准则和原则适用于国家开展与信息和通信技术有关的活动，各国必须对此类国际不法行为承担国际义务。

尽管这种做法很大程度上是无奈而为之，但对于继续推动网络空间规则的制定仍十分必要。寻求共识并不难，如僵尸网络对所有国家都具有同等的威胁，可以首先认定建立僵尸网络系统为非法。即使不能就如何界定“网络攻击”达成一致，但仍可以从防范共同威胁开始，对各国共同承认的某一类型的攻击进行限制并制定行为规范。明确各国的底线在当前阶段尤为重要，即便不能明确何种行为是符合规范的，也应明确哪些行为是不可接受的。如果国家间能够就不对某些关键基础设施发动网络攻击达成一致，同样也是重大的进步。非正式规则的积极作用在于推动催生一种共同的责任概念。因此，即使协定不能达成，谈判和磋商也有助于制定某些行为准则，通过潜移默化的方式来影响和塑造未来的行为。

此外，还有一些新的动向值得关注。2013 年以来，美国学界和媒体对网络安全威胁的认识开始回归理性，使喧嚣的网络战降温。《外交事务》（Foreign

[①] Tim Maurer, *Cyber Norm Emergency at the United Nations*, Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project, Harvard Kennedy School, September 2011.

Affairs）杂志刊文称，“我们应该忘记网络战的叫嚣，黑客行为可以减少真实世界的冲突，并且有助于和平。”[①] 布鲁金斯学会学者彼得·辛格尔（Peter Singer）在 2014 年 3 月的一次访谈中表示，所谓“网络珍珠港”或者“网络 9·11”的景象虽然危险，但近期内真正发生的可能性并不大，美国网络司令部司令凯斯·亚历山大（Keith Alexander）关于“美国军队每天遭受数百万次网络攻击”的说辞过于夸大，因为这些攻击中的确有恶意的，但更多是恶作剧、政治抗议或间谍行为，完全没有达到网络战的程度，美国对网络安全问题的认知仍处于“无知”、“狂热”和“担忧”的混合状态。[②] 他认为，网络安全问题的确存在，它是个人、企业、社会、政府的共同责任，而不应成为美国政府借此夸大威胁、要求增加军费的理由。美国军方与学界的不同声音可能会在未来一段时间内对美国的网络安全政策带来微妙影响：一方面，网络武器的研发和攻防能力的建设还将持续，网络战能力势必成为国家间军力较量的一个重要阵地；但另一方面，如斯诺登事件和中美网络间谍案等一般性的网络冲突问题将更加现实和突出，亟须加以规范并找到恰当的解决途径。

结 束 语

全球网络空间规则的制定仍然处于“提出规则”的初始阶段，在网络恐怖主义与网络犯罪层面以国家间合作为主，而国家间博弈则将集中在一般性网络冲突和网络战两个方面。鉴于美国多年来在互联网技术层面的主导地位，当前国家间的博弈主要表现为美欧与中俄在治理理念和模式上的冲突以及美国与欧盟在互联网的主导权上的争夺。2014 年 2 月，中国中央网络安全和信息化领导小组成立，并且提出了从网络大国向网络强国迈进的目标。作为一个新兴大国，中国应当在现阶段采取积极的对策，参与全球网络规则的制定。

第一，目前在国际层面探讨网络空间规则制定的平台有很多，如联合国（包括大会以及附属机构）、世界贸易组织、世界银行、互联网名称与数字地址分配机构、伦敦议程、欧盟、上合组织等，中国应当积极关注和参与这

[①] Thomas Rid, “Cyberwar and Peace: Hacking can reduce Real-World Violence,” *Foreign Affairs*, November/December, 2013.
[②] Charles Hoskinson, “The Cyber Threat,” *Washington Examiner*, March 21, 2014.

些平台有关网络规则的讨论，尤其是全球层面的磋商。在打击网络恐怖主义和有组织网络犯罪方面开展国际合作，承担更多的国际责任。在网络战规则的制定以及双边的网络冲突中采取更加积极、灵活的态度，用全面、长远的眼光作好多方面的准备，在确保国家利益的前提下，推动全球网络空间规则的制定，避免网络空间“巴尔干化”的风险。

第二，对中美网络间谍案的可能走势作出全面的预判，着力改善所谓“黑客大国”的负面国际形象。中美网络间谍案是中美两国结构性矛盾在网络空间的缩影，对中美两国关系的影响不容忽视，尤其是很多美国民众已经将“黑客”当作中国的标签。中国应尽可能在中美两国的现有对话机制内继续就该问题进行对话，商讨具体的解决办法，争取明晰各自的底线以及双方应遵循的原则，同时也应作好在世贸组织框架下应对的预案，包括指定专门的人员，熟悉相关的条款和准则以及建立必要的各部门沟通机制。

第三，在全球网络规则的制定过程中，加强与美国、欧盟及发展中国家的交流与合作。既要学习借鉴美国、欧盟国家在网络安全治理、立法等方面的做法，也要增加与其在政府、企业、学界等多轨道的交流合作。尽管与美国、欧盟等国家存在治理理念和模式上的分歧，但这不应成为全球网络规则制定进程的“终结者”。发展中国家普遍面临着互联网设施和技术落后的不利处境，中国应呼吁在制定全球网络规则时充分照顾到这些国家的利益，敦促发达国家向发展中国家提供更多的资金、技术和人员支持。

最后，打铁还要自身硬，中国要想争取互联网的管理权，首先要强化自身的网络能力建设。一方面要加快互联网技术的研发和人才队伍培养，强化网络军事攻防能力建设，尽快缩小与美国等西方发达国家的差距；另一方面应统筹协调国内工信部、外交部等各相关部门之间的关系，把握好网络主权与互联网联通性的关系，在维护国家主权的同时，确保互联网行业的可持续、健康发展，使网络成为强国腾飞的一大助力。

[收稿日期：2014-07-14]
[修回日期：2014-09-19]
[责任编辑：樊文光]