网络空间国际秩序的形成机制*

郎　平

【内容提要】　网络空间与现实空间深度融合，因而兼具虚拟与现实的双重属性。随着网络空间内涵和外延的不断扩大，不同类型的行为体先后介入网络空间的国际治理，成为国际规范制定的主体；依托各自不同的利益诉求，各行为体在不同层面上展开了力量博弈，建立了相应的国际制度安排，以应对不同层次的冲突和挑战。对于网络空间而言，建立国际秩序就是不同行为体通过确立相应的制度安排制定国际规范，从而解决不同层次的问题和冲突的过程。未来网络空间国际秩序的形成主要表现为价值观、制度平台的选择以及规则制定的博弈，而秩序形成背后的演进机制则取决于国家之间以及国家与非国家行为体之间的力量博弈。中美之间的合作与竞争态势将成为影响网络空间国际秩序建立的重要参照。

【关键词】　网络空间　国际秩序　形成机制　中美关系

【作者简介】　郎平，中国社会科学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。

电子信箱：langping@cass.org.cn

互联网是冷战时代的产物。1969年11月，为了帮助美国抵御核袭击而提供通信系统，美国国防部启动了一个名为“阿帕网”（ARPAnet）的军研项目。此后，在诸多科学家的努力下，互联网得以率先在美国和欧洲形成。冷战结束之后，国际环境缓和，互联网随之进入商业化运营，并且开始在全球迅速普及。一般来说，互联网可以分为三个层面：一是物理实体的基础设施

*　感谢清华大学国际关系学院主办的“世界秩序的变革与中国应对”研讨会与会者给予作者的启迪，特别致谢阎学通、李彬、孙学峰、漆海霞、徐进以及匿名评审专家对于本文提出的宝贵建议和意见。

层,包括海底光缆、服务器、个人计算机、移动设备等互联网硬件设施;二是由域名、IP 地址等唯一识别符和技术标准所构成的逻辑层;三是各种网站、服务、应用、数据构成的内容层。互联网用户的活动以网络为媒介向政治、经济和社会领域扩展,由此构成了更加立体、多维度的网络空间。

对于究竟什么是"网络空间",目前并没有统一的界定,视角不同,定义的内容也各有侧重。但无论定义有何不同,网络空间所具有的虚拟属性和社会属性为其赋予了与海、陆、空等其他空间域完全不同的特征。首先,互联网是分布式的网络,它的技术特点决定了没有哪个个人、机构或国家能够单独控制互联网,传统的政府控制权被分散,网络空间治理只能依靠各利益相关方之间的协商和合作才得以实现;其次,网络空间的内容可以无视地理因素跨越国家的传统边界,通信规模和种类急剧攀升,网络信息传播具有极强的隐蔽性,传播范围之广、速度之快,很难被彻底切断或遏制;最后,和传统的军事攻击相比,发动网络攻击的门槛很低,而打击目标则更广,一个国家的政治、军事、经济、社会以及个人的安全都会受到不同程度的威胁,由于网络空间安全问题的模糊性、隐蔽性和不对称性,传统维护国家安全的手段很难有效应对。

目前,学界对于网络空间的研究主要集中于治理的模式选择和路径,探讨应采用何种方式对这个新兴的领域进行治理。由于互联网的技术属性,大部分学者是技术领域的学科背景,他们对网络空间治理的思路更多偏向于"去政府化"的跨国治理,其代表人物是美国学者弥尔顿·穆勒(Milton Mueller),他从政治、公共政策和国际关系等方面集中探讨了互联网被民族国家管制而出现的"碎片化",提出了从国家主权(national sovereignty)转向大众主权(popular sovereignty)的网络空间框架。[①] 随着网络空间逐渐成为国际关系和外交层面的核心议题,研究者开始将目光聚焦信息技术和网络空间对国际关系的影响。约瑟夫·奈(Joseph S. Nye)便是其中之一,他特别论述了信息技术发展所导致的传统权力的分散化;结合对全球网络治理活

① 弥尔顿·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;Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Cambridge, UK: Polity Press, 2017).

动的观察，提出了一个由深度、宽度、组合体和履约度四个维度构成的规范性分析框架——机制复合体理论。[①]美国外交关系委员会史国力（Adam Segal）是为数不多的从世界秩序的视角来关注网络空间治理的学者，他认为，在数字时代，传统上国家主导的世界秩序已然发生了改变，而网络空间的世界秩序已然被黑客掌控[②]，其观点在很大程度上体现出其捍卫开放、全球、安全、弹性互联网的价值观。

诚然，技术的确可以左右天下大势。以互联网为代表的信息技术逐渐渗透到国家政治、经济、社会活动的方方面面，它不仅改变了人们的生活方式，更引领了社会生产方式的变革。随着网络空间与现实空间的深度融合，网络空间不仅面临着现实空间针对虚拟空间的各种威胁，而且必须应对虚拟空间对现实空间原有国际秩序的冲击。建立网络空间的国际秩序已经成为当务之急，而其目标应包含两个层面：一是确保互联网本身的安全、有效运行，实现全球网络空间的互联互通；二是制定国际规范来抑制与网络有关的冲突升级，维持现实空间的和平与稳定。

一、网络空间国际秩序的界定

在现实空间，国际秩序是“国际体系中的国家依据国家规范、采取非暴力方式处理冲突的状态”，它包含了三个构成要素：价值观、制度安排和国际规范。[③]作为一个新生事物，网络空间尚没有形成以国际规范为核心要素的国际秩序。对于网络空间而言，建立国际秩序其实就是不同行为体通过确立相应的制度安排制定国际规范、解决不同层次的问题和冲突的过程，从而避免冲突升级为不可控的状态。

---

① 2017年3月，约瑟夫·奈在《国际安全》上发表了《网络空间威慑与劝阻》的论文，探讨了网络威慑的概念、手段及实现策略，并提出了网络空间威慑的四种途径。Joseph S. Nye, *The Future of Power* (New York: Public Affairs, 2011); *Is the American Century Over?* (Cambridge, UK: Polity Press, 2015); “Deterrence and Dissuasion in Cyberspace,” *International Security*, Vol. 41, No. 3, 2017.

② Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016).

③ 阎学通：《无序体系中的国际秩序》，《国际政治科学》2016年第1期，第13页。

一般来说,网络空间的冲突可以分为两类:一类是自然性的冲突,这类冲突的发生通常是源于非恶意的动机,例如治理体系的不完善或者缺失、管理机构的人事变动抑或某些不可控因素等;另一类冲突则更具暴力性,例如以人身、财产为侵害目标,通过非法手段,对被害人的身心健康、生命财产安全造成极大损害的行为,而国与国之间的武力冲突或战争则是最高级别的暴力冲突。特别是随着国家对互联网的依赖程度日渐增加,网络空间的脆弱性愈发凸显,安全威胁也更加复杂和多元化,它不仅包含了互联网技术和社会公共政策层面的挑战,也涉及经济层面的数字规则、安全层面的网络犯罪以及网络恐怖主义和网络战、社会层面的个人信息和隐私保护等。

由于冲突的性质不同,冲突的解决方式也有所差别。最为严峻和棘手的网络问题是网络空间对国家安全的威胁。2007 年的爱沙尼亚危机、2008 年的格鲁吉亚战争以及 2010 年伊朗核设施遭受蠕虫病毒攻击,使得国家安全的最高决策者们开始真正关注网络空间的安全问题。许多战略家们相信,网络空间的先发制人已经出现,网络战的潘多拉盒子已经开启。[①]约瑟夫·奈认为,与国家行为体相比,非国家行为体更有可能发动网络攻击,现在是各个国家坐下来探讨如何防范网络威胁、维持世界和平的时候了。[②]在网络空间,如何通过非暴力手段抑制冲突的升级,才是建立网络空间秩序的意义所在。

然而,国际社会对于网络空间的认识正处于一个学习的阶段,围绕网络空间治理什么、由谁治理以及在哪里治理这些基本问题,政府、私营机构、公民社会等不同行为体之间展开了激烈的交锋。2012 年,国际电信联盟召开国际电信世界大会讨论《国际电信规则》的修改,国际社会第一次出现了明显的分裂。俄罗斯和阿拉伯国家在提案中建议修改规则,使国际电信联盟能够在网络空间发挥更大的作用,但遭到美国及欧洲国家的强烈反对,认为这将改变互联网"无国界"的性质,赋予政府干预网络空间的权力,西方国家的私营部门以及非政府组织更是强烈抗议将互联网纳入联合国的管理之

① Myriam Dunn Cavelty, "Unraveling the Stuxnet Effect: Of Much Persistence and Little Change in the Cyber Threats Debate," *Military and Strategic Affairs*, Vol. 3, No. 3, 2011.

② Joseph S. Nye, "Cyber War and Peace," *Today's Zaman*, April 10, 2012.

下。大会按照多数原则，以政府表决方式通过了这份具有约束力的全球性条约。修订后的《国际电信规则》给予所有国家平等接触国际电信业务的权利及拦截垃圾邮件的能力，得到了 89 个成员国的签署，但是以美国、欧洲国家为首的 55 个成员国以“威胁互联网的开放性”为由拒绝签字。随着新规则在 2015 年 1 月 1 日生效，未签署的国家将仍然沿用原有规则①，这无疑使得新规则通过的意义大打折扣。

据此，有学者将 2012 年看作网络空间国际秩序之争的“元年”。② 在这一年，美国政府承认参与开发了蠕虫病毒等网络武器，参与了针对伊朗核设施的“奥运行动”(Olympic Games Operation)；美国政府大肆诬蔑中国和俄罗斯利用网络间谍进行不正当商业竞争，并且起诉了 5 名中国军官，中美、俄美关系一度步入低谷。即使一些跨国主义者再不乐见，网络空间还是成了大国博弈的新“战场”。在过去数百年中，民族国家是国际秩序的缔造者，凭借自身的军事和经济实力以及外交手段来影响国际规范和制度安排。然而，在网络空间，安全威胁可能来自国家行为体，更可能源自难以追踪的非国家行为体，抑或是国家与非国家行为体的结合；网络空间的关键基础设施大多掌控在私营部门特别是某些互联网巨头手中，政府的权力在很大程度上被分散。

在这种背景下，网络空间的无序状态持续下去，很可能会导致难以估量的后果，网络空间国际秩序的建立已经迫在眉睫。在网络空间国际秩序的形成过程中，就国际规范而言，一方面，在技术层面已经建立了较为成熟的

---

① “原有规则”是指 1988 年版的《国际电信规则》，由于互联网尚未普及，信息和通信技术并未包含在内。2012 年版的新规则为确保全球信息自由流通设定了通用原则，并特别纳入了增加国际移动漫游资费和竞争的透明度、支持发展中国家电信发展、为残疾人获取电信服务提供便利、提高电信网络能源效率、处理电子废弃物等多项新内容，为在全球普及信息和通信技术、实现信息的自由流通奠定了基础。由于在国际电信联盟是否应支持政府对互联网的监管、《国际电信规则》是否应涉及网络安全和允许对垃圾邮件进行监控等条款上存在不同意见，美国、英国等国拒绝接受修订后的规则，部分欧洲国家则持保留意见。中国网：《国际电信大会修订〈国际电信规则〉遭美英等抑制》，2012 年 12 月 15 日，http://news.163.com/12/1215/11/8IOVIBNC00014JB6.html，引用日期：2017 年 10 月 8 日。

② Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs, 2016).

国际标准;另一方面,传统现实空间的国际规范和原则可以同样适用于网络空间,例如《联合国宪章》的基本原则,但是还有更多的新问题需要制定新的规范来加以约束。就制度安排来看,新机制和旧机制如何在纷繁复杂的治理体系中和谐共存,各自的适用范围如何划分,都是面临的重要挑战。

二、网络空间的治理体系:行为体与机制

网络空间治理体系的形成,特别是达成的一系列制度安排,是构建网络空间国际秩序的前提和基础。随着网络空间的不断发展和扩大,不同类型的行为体先后介入网络空间的国际治理,成为国际规范制定的主体;依托各自不同的利益诉求,各行为体在不同层面上展开了力量博弈,建立了相应的国际制度安排,以应对不同层次的冲突和挑战。回顾网络空间治理体系的发展进程,可以观察到不同行为体之间的互动以及国际制度特征。

(一)20 世纪 80 年代中期至 90 年代中期:技术社群主导

这一时期以互联网技术和产业社群等私营部门为主导,互联网工程任务组(IETF)、区域互联网地址注册机构(RIR)等一系列互联网治理机制相继成立。这些机制成立的目的主要集中于技术层面,例如互联网技术标准的研发和制定,其目标是确保互联网在全球范围内的有效、安全运行。

20 世纪 80 年代中期,互联网开始商业化并进入一个快速发展的阶段,随之而来的技术问题也日趋复杂。1985 年,IETF 成立,这是一个由网络设计师、运营者、服务提供商等参与的非营利性、开放的民间行业机构,主要负责与互联网运转相关的标准和控制协议的制定。1992 年,互联网协会(ISOC)成立,其目标是为全球互联网的发展创造有益、开放的条件,并就互联网技术制定相应的标准、发布信息、进行培训等,并负责 IETF、互联网结构委员会(IAB)等组织的组织与协调工作;1994 年,万维网联盟(W3C)成立,作为互联网企业的业界同盟,它主要负责网页标准的制定与管理,也是网页标准制定方面最具权威和影响力的标准制定机构。

上述机制有一个共同的特征,那就是该机制是松散的、自律的、自愿的、全球性的、开放性的、非营利性的非政府机构,任何人都可以注册参与机制

的活动，通过讨论形成共识，制定技术标准和相关政策。这种将政府权威排除在外、没有集中规划、也没有总体设计的自下而上、协商一致的治理模式，在很大程度上体现了早期互联网先驱们所崇尚的自由主义精神和文化，也为后期互联网治理“多利益相关方”模式的发展奠定了基础。

（二）20 世纪 90 年代后期至 21 世纪初：技术社群与美国政府的博弈

这一时期的主要特征是美国政府由幕后走向台前，与技术社群之间就互联网域名和地址分配的控制权展开了激烈博弈。斗争的结果是民间非营利公司 ICANN（互联网名称与数字地址分配机构）的建立，但也就此拉开了政府在互联网治理中应扮演何种角色的争论序幕。

IP 地址分配和域名管理的实际工作开始于 1972 年，一直由阿帕网的发明者之一、协议发明大师乔恩·波斯托（Jon Postel）教授及其同事以民间身份负责。然而，随着互联网日渐全球化，域名和地址分配系统的重要性日渐突出，美国政府不甘心将该领域的控制权让于“国际特设委员会”，1997 年 7 月，美国商务部公开发表《关于互联网域名注册和管理的征求意见》，以实际行动宣示其对互联网域名和地址分配的实际控制权。[①] 1998 年 1 月，波斯托发动了互联网空间的第一次反美“政变”，他致信非美国政府根服务器的运营商，要求他们使用 IANA（互联网数字分配机构）的服务器获取权威根区信息，以实际行动向美国政府宣示：“美国无法从在过去 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。”[②]然而，此次“实验”仅维持了一周的时间就在美国政府的压力下停止。尽管波斯托将其称作一次“技术实验”，但却从事实上证明可以有效地摆脱美国政府对域名系统的根区控制权，直接推动了美国政府对互联网域名系统管理进行改革的决心。

1998 年 2 月，美国商务部公布了互联网域名和地址管理“绿皮书”，决定改善互联网域名和地址系统的技术管理，以“一种负责任的态度”终止美国

---

① Joel Snyder et al.，“The History of IANA：An Extended Timeline with Citations and Commentary，” *Internet Society*，January 17，2017.

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

政府对互联网数字地址与域名分配的控制权。经过广泛调研,1998 年 6 月,美国商务部国家电信和信息管理局(NTIA)重新发布了互联网“白皮书”,决定成立由全球网络界商业、技术及学术各领域专家组成的 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任务,NTIA 通过与 IANA 签订合同,对其行使监管权。至此,互联网域名与地址分配的主导权之争尘埃落定,ICANN 的成立将其他国家的政府排除在决策圈之外,但是由于历史原因,美国政府仍然保持了幕后监管的特殊权力和地位。

由此,IETF、ISOC、RIR 以及 ICANN 构成了掌控全球互联网关键资源的一个有机的机构集群。它们伴随着互联网的成长而发展壮大,以私营部门行为体为主导,制定了从标准到域名、IP 地址的分配这些使全球互联网得以有效运转的国际规范。更重要的是,它们实现了一次重大的权力转换,代表了政策和治理在方法与实质上的一次重要变革。① 与此同时,一些传统的政府间国际组织也开始触及互联网相关的议题,但只是零星的尝试,例如世界知识产权组织从 1996 年开始制定一些涉及互联网的著作权、网络域名和商标问题的条例;国际电信联盟也尝试参与到网络域名的治理中,但没有成功。值得一提的是,虽然这一时期互联网国际规范的制定权归属于这些非政府的私营机构,但美国政府仍然是一个独特的存在。这一方面是因为互联网的诞生固然离不开美国政府的支持,域名等关键资源的管理仍然处于美国商务部的监管之下;而另一方面,由于注册地在美国,这些机构仍须接受美国的司法管辖。

(三)21 世纪初至今:网络空间国际治理体系的形成

这一时期,互联网在全球层面迅速普及,并且融入国家政治、经济和社会生活的方方面面,网络空间治理的内容开始从技术层面向经济、社会层面的公共政策和安全领域扩展,逐渐形成了多层次、多元化、全方位的治理体系。WSIS(信息社会世界峰会)、IGF(互联网治理论坛)等全球性的互联网治理机构相继成立,与此同时,一些原有的国际组织和机构也将网络空间相

① 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 260 页。

关的议题纳入议程，勾勒出一幅貌似混杂无序的网络空间国际治理的制度蓝图。

2003 年由联合国大会决议召开的 WSIS 是网络空间治理进程中的一个标志性事件。此次会议虽然没有能够就信息社会和发展问题展开深入讨论，但却对互联网治理的机制发展产生了深远的影响，它主要体现在：(1)明确了互联网治理的内容以及建立 IGF 这一探讨全球互联网治理的重要机制；(2)明确了“行为体的不同角色与责任”，确认了主权国家政府在互联网公共政策制定领域的权力，而技术管理与日常运营则归属于私营部门和公民社会；(3)正式拉开了基于主权国家间的“多边主义”与基于私营部门的“多利益相关方”两种治理模式之争的序幕，凸显了美国、欧盟、发展中国家和公民社会这四种群体之间的利益博弈；(4)明确了 WSIS 的治理内容将聚焦互联网发展问题，并且与国际电信联盟、经济合作与发展组织、联合国贸易和发展会议、世界银行、欧盟统计局、联合国经济和社会理事会建立伙伴关系，形成了“WSIS＋10”的治理机制。

另一个突出的进展是网络安全治理机制的建立，网络安全治理的内容逐渐从技术层面的狭义“互联网安全”提升至国家战略层面的全方位的“网络安全”。早在 1998 年 9 月，俄罗斯就在联合国大会第一委员会提交了一份名为“从国家安全角度看信息和电信领域的发展”的决议草案，呼吁缔结一项网络军备控制的协定，但并没有得到其他国家的响应。直到 2004 年，联合国大会成立了 UNGGE(信息安全政府专家小组)，授权其对该决议草案的内容进行研究；2005 年至 2009 年的 5 年间，该决议草案的发起国迅速增加到 30 个，而美国则坚持反对将其纳入联合国大会议程；2010 年之后，美国的立场发生转变，首次成为网络安全决议草案的共同提议国。自此，包括中、美、俄在内的主要大国都同意就网络安全问题进行研讨和对话，联合国大会及 UNGGE 成为当前全球层次上网络安全治理的重要机制和平台。

与上一个阶段相比，当前的网络空间治理实现了两个维度的跨越：一是治理内容开始从技术层面向经济、政治和安全层面扩展；二是治理机制也由技术专家主导的非政府机构向传统的政府间国际组织和平台渗透，G20、金砖国家等重要的地区治理机制都将网络相关的议题纳入进来。此外，在网络空间治理机制向外扩展的同时，网络空间治理机制本身的改革也在不断

深化,最突出的事例就是 2016 年 10 月 1 日,美国商务部与 ICANN 间的 IANA 职能合同如期失效,美国商务部正式放弃对互联网根域名服务器的监管权,将其移交给 ICANN 管理。

至此,网络空间已经形成了由私营部门、政府、公民社会和个人用户等多种行为体构成的互动体系。从行为体互动的角度观察,私营部门在技术层面的博弈中取得了主导权;政府行为体之间的博弈则主要体现在经济和安全等政治性相对较高的领域;在社会公共政策领域,政府行为体、私营部门以及公民社会等多个行为体的博弈正陷入一片混战。从制度安排来看,不仅包含了以技术社群为治理主体的非政府机制,也包含了 ICANN 这样异质多元治理主体的机制,并且囊括了国家行为体和非国家行为体共同参与的机制(IGF)以及政府间的国际机制(联合国、北约)。

国际体系所体现的是行为体之间互动的客观存在,行为体、国际格局和国际规范是国际体系构成的核心要素。就网络空间的现状而言,上述多种利益相关方均已参与到全球治理的体系中来,多种行为体之间的互动已经形成了基本的力量格局,对于国际规范的探讨也正处于博弈进程中。但是,国际体系的形成并不意味着一定存在国际秩序,还需要经过行为体的博弈产生出主导的价值观,建立某种制度安排来实现包括规则制定权在内的权力分配,从而决定以什么样的方式来解决冲突,避免出现冲突不可控的失序状态。从这个意义上说,网络空间的国际秩序仍然处于早期的形成过程中。

三、网络空间的国际秩序:冲突与解决

随着互联网在各领域的无限渗透,网络空间的内涵和外延仍然在不断扩大,涉及的议题跨越技术、社会、经济和安全等各个层次,由此产生的冲突也在各个层次上表现出不同的态势和解决路径。如果国际社会能够确立有效解决冲突的制度安排,那么我们认为,冲突的解决正在向着有秩序的方向发展;如果能够在制度安排框架下达成相应的国际规范,那么我们认为,网络空间的国际秩序已经具备了基本的构成要件。当然,网络空间是否有秩序还要取决于国际规范是否能够有效发挥约束力。

（一）技术层面

目前，网络空间存在的安全威胁正在不断增多，根据国际电信联盟最新的统计报告，“对计算机网络构成的威胁正在从相对来说危害不大的垃圾邮件向具有恶意的威胁方向转化。”[①]因而，在技术层面，网络空间国际秩序建立的目标是实现相关社群在技术治理层面的权力分配，有效应对威胁互联网运行安全的隐患，确保全球互联网的互联互通。

技术层面的冲突主要有两类：第一类属于自然性冲突，主要源于互联网运行机制自身的安全风险。例如，互联网运行的管理缺陷会造成互联网访问不能正常运行，典型的案例如域名管理人员被捕入狱，伊拉克国家顶级域名“.iq”在2003年伊拉克战争期间一度无法申请和进行解析；2004年4月，由于负责利比亚顶级域名管理的公司陷入人事纠纷，该域名的主服务器停止工作，所有以“.ly”域名结尾的网站均无法访问，影响到大约1.25万个域名。[②]第二类则是更为常见的暴力性冲突，主要源于非国家行为体的恶意安全威胁。这些非国家行为体可能是有组织的黑客集团，也有可能是某些个人，他们利用软件的漏洞或者攻击工具，对目标发动攻击，致使互联网无法正常运转并造成较大的经济损失，其中最常见的是分布式拒绝服务（DDoS）攻击[③]和木马病毒。2017年5月，勒索病毒WannaCry利用Eternal Blue（“永恒之蓝”）的漏洞以及木马软件，以其惊人的破坏力在全球肆虐，影响到150多个国家、1万多个组织机构的计算机系统，造成全球80亿美元的损失，甚至危及一些国家的关键信息基础设施，这不能不说是目前网络安全模式的失败。[④]

---

① *Global Cybersecurity Index* 2017, ITU, July 6, 2017, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx, 访问时间：2017年5月10日。

② ICANN北京：《利比亚国家顶级域名（.LY）中止服务始末》，2017年5月30日，http://mp.weixin.qq.com/s/OOHLVjVSUL_hw5VD65Mp4g，访问时间：2017年6月10日。

③ 分布式拒绝服务（DDoS）攻击是指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击。

④ E安全：《早在WannaCry之前，至少存在三个组织利用永恒之蓝发起攻击》，2017年5月25日，http://mp.weixin.qq.com/s/AWUQAG0TNCPYi5BoYqtg4g，访问时间：2017年6月10日。

目前,针对第一类安全风险的制度安排已经相对成熟,国际社会建立了不同的机构来维护技术社群、用户以及政府之间的正常秩序。这些制度安排的特征是以私营机构为主导、以“多利益相关方”为治理模式的一系列国际机制(统称为 I*)。根据 ISOC 的界定,“多利益相关方”并不是一种单一的模式,也不是一种唯一的解决方案,而是一系列基本原则,例如包容和透明、共同承担责任、有效的决策和执行、分布式和可互操作的治理合作。①作为一种制度路径,“多利益相关方”在实践中具有相当的灵活性,以该框架为指导的治理机制呈现出不同的类型和特征。

一种类型以 IETF 为代表,I* 等技术性领域的治理机制大多属于此类。这些机制的治理主体是互联网领域的相关技术专家,奉行的是将政府权威完全排除在外、以共识为决策基础的治理模式。从治理内容上看,它的任务是就关键资源的管理、网页标准和传输标准制定共同的国际标准;但从目标上看,它实现了全球不同国家技术社群之间的协调一致,避免不同地区的技术社群因规则制定权力的争夺而陷入混乱。

ICANN 是另一种类型。同样是奉行“多利益相关方”的治理模式,ICANN 的权力主体由“同质”的技术专家向“异质”的多元化主体扩展,从域名注册商等中小企业到普通的互联网用户,从技术人员、政府、学术界到民间机构,各相关方都能够参与其中,表达自身的利益诉求。从这个意义上说,ICANN 的作用与其说是互联网关键资源的管理,不如说是维持了不同行为体之间在规则制定权和话语权方面的一种“均势”。

遗憾的是,针对第二类的安全风险,目前并不存在一个全球性的国际协调和应对机制。很多国家都成立了本国的 CERT(“互联网应急事件响应组”),专门处理计算机网络安全问题,例如漏洞威胁、恶意安全代码、数据泄露等;也出现了一些地区性的国际合作机制,例如,2013 年以来,中国、日本和韩国之间的国家互联网应急中心每年召开一次年会,建立了三方 7 * 24 小时的热线机制,就网络安全事件的应对进行密切协作,成功处置多起涉及中

① “Internet Governance: Why the Multistakeholder Approach Works,” *Internet Society*, 26 April, 2016, https://www.internetsociety.org/doc/internet-governance-why-multistakeholder-approach-works,访问时间:2016 年 5 月 20 日。

日韩的黑客攻击事件及其他重大网络安全事件，遏制了危机的蔓延；其他一些国家（如美国和俄罗斯之间）也在积极开展 CERT 组织之间的合作活动。[①] 但就如勒索病毒这样全球性的安全威胁而言，各个国家或地区 CERT 之间的国际合作机制仍然十分有限。

（二）社会公共政策层面

网络空间社会公共政策的核心内容是如何保障网络空间中互联网用户的人权。中国《国家网络空间安全战略》在提到建设有序网络空间的战略目标时表示："公众在网络空间的知情权、参与权、表达权、监督权等合法权益得到充分保障，网络空间个人隐私获得有效保护，人权受到充分尊重。"[②] 具体而言，网络空间社会公共政策应遵循三项重要原则：一是自由原则，即网络空间信息的自由流动、公民自由接入互联网以及互联网用户的言论自由；二是开放原则，即网络空间应保持开放的属性和开放的政策；三是保护原则，即网络空间的个人信息和隐私同样受到法律的保护。

围绕上述原则和目标，主要存在两类冲突：一是以政府行为体为主导的国际社会与盗窃个人信息和隐私的不法组织或个人之间的博弈，二是互联网企业与政府之间的利益较量。政府作为政策的制定者，对维护网络空间的社会秩序以及国家安全负有主要责任；作为互联网产业向前发展的主导力量，企业的战略考量主要基于维护企业的利益和价值观；黑客组织或个人依凭网络空间所赋予的不对称性权力，试图谋取私利。目前，很多国家的政府都在制定和规范本国的个人信息保护和数据安全政策，以规范不同行为体的行为。到目前为止，这些政策和规范仍然只停留在国家和地区层面，并且面临着诸多的未解难题，特别是直接掌控互联网信息流动的互联网企业的权利与责任边界。

美国政府与苹果公司和微软公司两大互联网巨头之间的博弈凸显了互联网企业与政府之间的利益冲突。2016 年 2 月，FBI 对苹果公司施压，要求

---

① 国家互联网应急中心：《第四届中日韩互联网应急年会在中国召开》，2016 年 9 月 19 日，http://www.cert.org.cn/publish/main/12/2016/20160919162812091883339/20160919162812091883339_.html，访问时间：2016 年 11 月 8 日。

② 中国网信网：《国家网络空间安全战略》，2016 年 12 月 27 日，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm，访问时间：2017 年 10 月 5 日。

其执行联邦法院的法庭指令,专门为其开发一套“政府系统”,帮助其破解一名恐怖分子的苹果手机密码,但遭到了苹果公司的反对。苹果公司总裁库克声称,苹果公司必须要保护用户的信息,“我们是隐私权的坚定拥护者,我们之所以做这些事情,因为它们都是对的”①;脸书、谷歌、亚马逊、推特、微软等知名互联网公司纷纷表态支持苹果公司的做法。2013 年,美国纽约南区联邦地区法院助理法官詹姆斯·弗朗西斯(James C. Francis)签发搜查令,要求微软公司协助一起毒品案件的调查,将一名微软用户的电子邮件内容和其他账户信息提交给美国政府,但却遭到微软公司的拒绝。2016 年 6 月,美国联邦第二巡回上诉法院判决认定,法院的搜查令不具域外效力,要获取境外数据,应通过双边司法协助条约解决。②

从上述案例可以看出,如何在公民权益与国家安全中寻求平衡目前是一个无解的僵局,对一个国家如此,对国际社会更甚。在国际层面,就上述问题的讨论还刚刚展开,在很多国际机制中都设有相关的议题,其中较有影响力的当属联合国框架下的 WSIS 和 IGF。WSIS 和 IGF 均是在联合国的支持下成立的国际机制,前者是讨论互联网与社会发展问题的重要全球机制,后者则是探讨互联网治理社会公共政策问题的重要全球性平台。在联合国的背景下,同样是采取“多利益相关方”的组织模式,它们提升了政府主体的角色,认为政府主体、私营机构、公民社会等不同的行为体在治理实践中享有平等的地位;从另一个角度看,这也意味着政府不得不在这个论坛上放弃它们的特权与专有地位。

但是,随着治理主体的多元化和异质化,“多利益相关方”的制度框架也使得行为体之间的矛盾和冲突更加复杂,不仅存在不同类型行为体之间的矛盾,而且引入了国家之间的竞争和冲突。例如,以巴西为首的发展中国家

---

① Nancy Gibbs and Lev Grossman, “Apple CEO Tim Cook on FBI, Security, Privacy: Transcript,” *Time*, March 17, 2016, http://time.com/4261796/tim-cook-transcript, 访问时间:2016 年 4 月 10 日。

② Nick Wingfield and Cecilia Kang, “Microsoft Wins Appeal on Overseas Data Searches”, *The New York Times*, July 14, 2016, https://www.bostonglobe.com/business/2016/07/14/microsoft-wins-appeal-overseas-data-searches/q2MhwFgFeSVAu3bVkv5b1O/story.html, 访问时间:2016 年 10 月 10 日。

将 IGF 看作某种政府间框架协议的准备和发展过程，最终目标是建立网络空间“全球适用的公共政策原则”，将网络空间纳入传统的政府间组织框架；以美国为首的发达国家则认为 IGF 的使命是一个集中信息和各方观点并进行对话的“场所”，它不应该进入实质性的政策制定流程中去。围绕议程的设置、顾问组和秘书处的代表权问题以及治理的根本原则等问题，两大派系之间的政治斗争和博弈愈演愈烈，始终未能找到有效的解决途径。

由于议题的泛化以及主体的多元化，社会公共政策领域的“多利益相关方”制度安排仅仅停留在对话层面，很难达成解决冲突的具体行动。尽管如此，相比较“伦敦进程”等其他全球对话机制，考虑到联合国的成员数量以及工作程序，联合国机制可能是低效的，但无疑也最具合法性，它有助于在社会公共政策领域达成某些一致性的自愿原则。联合国第三个 UNGGE 的“成果文件”第 21 条也表示，各国在努力处理通信技术安全问题的同时，必须尊重《世界人权宣言》和其他国际文书所载的人权和基本自由。[①] 中国外交部在《网络空间国际合作战略》的“行动计划”中表示：“支持联合国大会及人权理事会有关隐私权保护问题的讨论，推动网络空间确立个人隐私保护原则。”[②]

（三）经济和国家安全层面

在经济和国家安全层面，与网络空间有关的冲突主要体现在网络议题对传统国际规则的冲击。在经贸领域，国际社会面临的挑战是如何实现数字经济的效益最大化，其中既涉及电子商务等传统的贸易议题，也涵盖了跨境数据流动、数字产品贸易、计算设施本地化等与网络空间治理直接相关的新议题。在安全领域，网络空间给国家安全带来了诸多新的挑战，这其中既关乎高级政治领域的领土安全和政权稳定，也涉及经济安全等非传统安全议题。之所以将这两个层面归于一类，是因为这些冲突都是要通过政府间谈判制定规则来解决的，这与技术和社会公共政策层面的冲突解决路径完全不同。

---

① 联合国大会：《从国际安全的角度来看信息和电信领域的发展》，A/68/98，2013 年 6 月 24 日。

② 中国外交部、中国国家互联网信息办公室：《网络空间国际合作战略》，2017 年 3 月 1 日，http://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t1442389.shtml，访问时间：2017 年 3 月 2 日。

数字经济已经被纳入许多国家的发展战略,与网络有关的国际经贸规则谈判或对话在双边、区域和全球等多层面的国际机制中展开。在双边层面,美欧《跨大西洋贸易与投资伙伴关系协定》(TTIP)正在讨论包括跨境数据流动在内的数字贸易相关议题。① 在区域层面,《跨太平洋伙伴关系协定》(TPP)虽然目前走向不明,但在美国主导下制定的一套系统性的与互联网相关的国际经贸规则主张②很可能成为未来数字经济规则制定的蓝本;由我国与东盟国家共同倡导的《区域全面经济伙伴关系协定》(RCEP)启动了电子商务的谈判,涉及跨境数据流动、禁止计算设施本地化、数字产品非歧视待遇、禁止强制披露源代码等重要议题。在全球层面,在 WTO(世界贸易组织)框架下,美国和欧盟在 2012 年联合 21 个 WTO 成员发起了《服务贸易协定》(TiSA)谈判③;2016 年 7 月,美国和欧盟分别向 WTO 总理事会提交了关于电子商务的非立场文件,希望在 2017 年底召开的第 11 届部长级会议上启动电子商务多边贸易规则的谈判。

围绕上述议题的国际经贸规则制定,主要存在 3 个层面的适应性困境:(1)网络空间治理与传统国际经贸规则制定逻辑之间的冲突。前者强调的是"多利益相关方"共同参与的治理模式,后者则是以政府为规则的谈判和义务主体通过政府间的"秘密"谈判来达成经贸协定。新议题与传统架构的融合使得数字经济规则的规范目标不仅是推动数字经济发展,同时仍需兼顾消费者权益以及国家利益与公共利益之间的均衡;(2)国家行为体之间围绕新、旧议题的利益冲突。欧美等发达国家主张在国际经贸规则的谈判中增加与传统货物贸易并无直接联系的新议题,以便填补规则空白;以中国为代表的新兴经济体则由于难以把握规则制定的主动权而更倾向于在传统贸易方面发挥自身的优势。就目前的走势来看,新议题进入国际经贸规则的

---

① The Executive Office of the United States and the European Commission, *US-EU Joint Report on TTIP Progress to Date*, 17 January, 2017.

② 包含了跨境数据流动、计算设施本地化、个人信息保护、网络商业窃密等多项网络空间治理的重要议题。

③ 2012 年中国未参加谈判。2013 年,中国加入《服务贸易协定》谈判。参见中国新闻网:《商务部:中国已加入服务贸易协定谈判》,2013 年 10 月 17 日,http://www.chinanews.com/cj/2013/10-17/5393017.shtml。

谈判恐难以回避;(3)政府与私营部门之间在规则制定透明度和参与权限方面的冲突。按照传统国际经贸规则的制定逻辑,以私营部门为代表的其他利益相关方获取信息和参与谈判的程度非常有限;互联网业界则认为,这与网络空间国际治理主张的"多利益相关方"治理模式存在严重脱节,是在"用20世纪的贸易协定谈判方式为21世纪制定高标准规则"①。

网络安全领域的冲突同样存在于国家与国家以及国家与非国家行为体之间,前者如日益加剧的军备竞赛和网络战,后者如黑客攻击、网络犯罪、网络恐怖主义等;而2017年5月席卷全球的勒索病毒事件既是非国家行为体对国家安全发起的攻击,也涉及国家行为体如何管控自身的网络武器以避免网络武器的扩散。在这个层面,国际合作的目标应是达成具有约束力或一致同意遵守的国际行为规范以及信任和安全建立措施,以缓解网络空间的安全困境,维护网络空间的战略稳定。

国际社会对网络空间国际安全架构的构建仍处于初步的探索阶段,有关网络安全问题的合作与对话在全球(联合国)、区域(北约、欧盟、上海合作组织)以及双边机制等多层次同时展开。由于与网络空间有关的军事安全议题直接关系到国家的军事安全,因而在不同的层次上表现出不同的博弈态势:在联合国这样的全球机制中直接表现为发达国家与发展中国家之间的利益碰撞,例如,2017年6月,UNGGE就网络空间安全行为规范的谈判因发达国家与发展中国家的立场难以协调而暂告失败;在北约、上海合作组织这样的区域组织中则表现为协调立场,实现共同防御和寻求集体安全;在双边层面上,对话机制的建立主要集中在彼此关切的领域,有较强的针对性和局限性,例如,2015年12月,中美建立了打击网络犯罪及相关事项高级别联合对话机制,达成《中美打击网络犯罪及相关事项指导原则》,并同意建立打击网络犯罪及相关事项的热线。

从规则制定的角度来看,目前最为重要的国际机制是联合国大会第一委员会,而最值得关注的机制则是北约。从2004年联合国大会成立第一个

① IGF, "IGF 2016-Day 3-Main Hall-Trade Agreements and the Internet," December 5, 2016, http://www.intgovforum.org/multilingual/content/igf-2016-day-3-main-hall-trade-agreements-and-the-internet, 访问时间:2017年5月8日。

UNGGE 开始,国际社会就在商讨缔结一项网络安全行为规范的国际条约的可能性;2015 年 7 月,联合国大会第四个 UNGGE 向大会提交报告,汇报了所取得的重大进展,提出了 11 项自愿的、非约束性国家负责任行为规范、规则或原则建议,建议各国以自愿的方式在政策技术、多边协商机制、区域合作、关键基础设施保护等四个层面采取进一步建立信任的措施。① 相比联合国政府间谈判的多重博弈,北约卓越合作网络防御中心邀请成员国 19 名学者编纂推出的《可适用于网络战的国际法的塔林手册》凸显了美欧等西方国家的利益诉求,实现了战争时期与和平时期网络空间国际规则的全覆盖。这份手册虽然不是北约的官方文件,但它却是世界上第一份公开出版的、系统化的有关网络战的规范指南,它对网络攻击、网络战的行为标准等关键概念进行了界定,明确了政府的义务和责任,被一些西方媒体誉为网络战领域的"国际法公约"。②

综合上述分析,可以看到网络空间的国际秩序在不同层次上的进展态势有较大的差异。在技术层面,已经形成了相对稳定的全球秩序,当前的制度安排能够有效管理和应对不同社群之间的利益纷争,基本形成了私营部门主导下的国际秩序,但在全球层面仍缺乏有效的应对暴力冲突的国际机制;在社会公共政策层面,演进的方向是达成由多方行为体共同主导的国际秩序,不过考虑到冲突的解决在很大程度上受到一国国内政治的限制,要形成统一的国际规范还有相当的难度,因而下一步的目标还是在现有的制度框架下达成一般性原则的国际规范;在经济和安全领域,依托传统的政府间国际机制,如何达成有效应对各种暴力冲突的国际规范目前仍在博弈之中,而其发展的趋势仍然是建立由政府主导的国际秩序。

四、网络空间国际秩序的要素分析

国际秩序可以分解为三个构成要素:首先是行为标准的国际规范,其次要有指导国际规范制定的主流价值观,第三是约束国家遵守国际规范的制

① 2017 年 6 月,第五个 UNGGE 未能如期提交报告,这也反映出一旦进入深水区,国家之间的利益冲突将会越发难以调和。

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

度安排。[①]网络空间是一个新兴的领域，目前正处于国际秩序建立的形成时期，在某些领域固然有一些适用的国际法规范，但就网络空间的整体安全和稳定而言，国际规范仍然是一片空白；制度安排已经基本就绪，但就选择哪一个机制作为规范制定的场所，仍然没有尘埃落定；唯有关于主导价值观的争论已基本达成了国际共识。据此，未来网络空间国际秩序的形成主要表现为价值观、制度平台的选择以及规则制定的博弈，而秩序形成背后的作用机制则取决于国家之间、特别是国家与非国家行为体之间的力量博弈。

（一）价值观的冲突

互联网的发展离不开欧美等发达国家技术专家的发明创造，他们在技术上贡献智慧的同时，也将西方文化中自由、开放、民主的价值观注入其中，在互联网全球普及的过程中，他们支持网络空间的全球化和自由化，呼吁实现网络空间的自治，反对政府的权力干预，认为公民社会将取代国家，人类社会将进入全新的网络社会。[②] 例如，IETF 作为早期的互联网治理机构，其奉行的信条是“我们反对总统、国王和投票；我们相信协商一致和运行的代码”；其他如 W3C、RIR、ISOC 等早期互联网技术治理机构无不遵循了由私营部门掌控规则制定权的“多利益相关方”路径。基于互联网早期发展相对独立于国家的现实，特别是人们对网络空间作为一个“无边界性”的全球空间的认知，1996 年，美国网络活动家约翰·巴洛发表了《网络空间独立宣言》，声称网络空间是一个与外空和公海相似的“全球公域”，将网络空间治理的“去主权化”观念推向高潮。[③]

然而，随着信息技术逐渐深入国家的政治、经济和社会生活的方方面面，网络空间逐渐与现实空间紧密融合，主权国家作为现实空间中国际社会的基本行为体，势必会进入网络空间并成为网络空间规则制定中不可或缺的角色。特别是网络空间是一个多领域、多层次的空间，不同领域之间的议

---

① 阎学通：《无序体系中的国际秩序》，《国际政治科学》2016 年第 1 期，第 14 页。

② David Johnson and David Post, “Law and Borders: The Rise of Law in Cyberspace,” *Stanford Law Review*, Vol. 48, No. 5, 1996, pp. 1368-1378.

③ Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), p. 13.

题相互交叉融合,即使是技术层面的规则制定,也很难完全将政府排除在利益相关方之外。集体主义与民族主义的价值观与全球性、自由化的价值观形成了激烈的碰撞,权力与自由的交锋突出表现为国家在网络空间治理中的角色。弥尔顿·穆勒认为,传统的左派与右派分野已经无法简单区分网络空间治理的政治派系,那么以国家—跨国为横轴,以网络化—科层制为纵轴,至少存在网络化国家主义、虚拟世界反动派、非国家化自由主义以及全球政府治理四种政治光谱。①

除了政府的角色之外,价值观的冲突还体现在治理模式的选择上,特别是围绕"多利益相关方"的争论。在网络空间治理进程中,"多利益相关方"的治理实践主要包含了如下核心要素:多方共同参与、由下至上、共识驱动。作为一种治理路径,"多利益相关方"的核心价值观是不同行为体在平等的基础上共同参与治理,这与传统意义上政府主导、存在中央权威、由上至下的"多边主义"模式形成了鲜明的对比。"多边主义"更突出政府行为体在各利益相关方中的主导地位,它虽然不排斥其他利益相关方的参与,但是其前提仍然是在政府主导之下的"多利益相关方"的共同参与,因此在决策中更多表现的是政府自上而下的权威等级式管理,政府作为各利益方的代表发布相关政令、制定相关政策;"多利益相关方"则更强调私营部门、政府、国际组织、公民社会、学术机构等不同利益相关方之间的平等协作,是一种自下而上的、包容性的、网络化的组织和决策模式,与互联网本身的网络化特征相契合。

其实,所谓的模式之争并没有意义,因为在普遍意义上,"多利益相关方"是一种路径或方法(approach),而"多边主义"则是一种具体的实践模式,两者之间并没有可比性。在实践中,不同实践模式各有优劣,选择哪一种治理模式,关键在于针对特定的议题,哪一种治理模式更为有效。正如劳拉·德纳迪斯(Laura DeNardis)所说:"一个诸如'谁应该控制互联网,联合国或者什么其他的组织'的问题没多大意义;合适的问题应该触及在每个特定的背景下,什么是最有效的治理方式。"② 2015 年 12 月,联合国在"信息社会世

① 弥尔顿·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。

② Laura Denardis, *Global War on Internet Governance* (New Haven and London: Yale University Press, 2014), p. 226.

界峰会成果落实十年审查进程高级别会议”的官方文件中承认了两种模式的共存价值，指出：“我们再度重申坚持 WSIS 自启动以来所坚持的‘多利益相关方’合作与参与的原则和价值观……我们认同政府在与国家安全有关的网络安全事务中的主导作用，同时我们进一步确认所有利益相关方在各自不同的角色以及责任中所发挥的重要作用和贡献。”①

基于网络空间的虚拟和现实双重属性，价值观的碰撞必然会实现新旧两种模式在某种程度上的融合，而不是“东风压倒西风”的局面。一方面，我们需要互联网在全球层面的开放和互联互通，至少在基础设施和关键资源领域，这是互联网得以在全球有效运转的基本保障；另一方面，在网络内容监管、网络安全等政策制定层面，国家的权威仍然不可或缺。但是，考虑到“安全”概念内涵和外延的扩大趋势，非传统安全的重要性日益上升，再加上各国的国情不同，对于安全利益的优先排序也有较大的差异，不同政府对于应发挥主权权威的网络安全情景也必然有不同的界定。因此，两种价值观的碰撞还会持续，它一方面具有对立性，表现为有关网络主权的行使边界和行使方式的争论；但更重要的是它所具有的统一性，价值观的融合终将推动一种不同于传统国际秩序的新秩序的建立。

（二）制度平台的选择

从表面上看，网络空间治理的国际机制呈现出一种松散无序的状态，如约瑟夫·奈所说：“机制复合体就是由若干机制松散配对而成的，从正式机制化的光谱来看，一个机制复合体的一端是单一的法律工具，而另一端则是碎片化的各种安排；它混合了规范、机制和程序，其中有的很大，有的则相对较小，有的相当正式，有的则非常不正式。”②但是，如果对网络空间国际治理机制进行分层考察，就可以发现网络空间国际治理机制同样有其内在的逻辑。

---

① The UN General Assembly, *Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of WSIS Outcomes*, A/70/L.33, December 13, 2015.

② 约瑟夫·奈：《机制复合体与全球网络活动治理》，《网络空间研究》2016 年第 4 期，第 87—96 页。

网络空间的国际治理是由技术层面发端,随后逐渐向公共政策、经济和安全领域扩展的,由议题的性质所决定,制度安排在相同层次上具有共性,而在不同层次之间则存在明显的继承关系。在技术层面,以 IETF、ICANN 为代表的国际机制均属于技术社群主导的非政府机构,这种机制的特点是:一方面,由于确定了私营部门的主导地位,在技术层面更利于快速作出决策,避免了政府间博弈带来的冲突和低效率;但另一方面,由于排除了政府的主导权,这也从客观上限定了这些机制的使命只能局限在某个技术领域,对其他公共政策领域的影响力将会非常有限。

在社会公共政策层面,以 IGF、WSIS 为代表的国际机制大多归属于论坛或者会议等机制化水平较低的形式,虽然采用了包括政府在内的"多利益相关方"治理模式,但是至今未能产生有约束力的集体行动。究其原因,这是由公共政策议题本身的性质所决定的。互联网领域的公共政策涉及技术、内容、网站管理、政治、人权、宗教等多个领域,其内涵和外延都具有无限延伸的属性,而由于国情不同,每个国家对于公共政策的制定必然有不同的立场和出发点,除了一般性的原则之外,很难在国际范围内达成一致的公共政策。此外,"多利益相关方"网络化的组织模式也决定了它很难在需要资源高度集中的领域产生高效的集体行动。

在经济和国家安全领域,传统的政府间治理机制如 WTO、联合国、G20 占据了主导地位,其治理目标仍然是通过政府间谈判和合作的方式达成共识或者具有约束力的国际规则。然而,作为新生事物,传统国际机制中网络议题的国际规则仍然处于规则制定的早期阶段,国家间的利益冲突和博弈意味着规则的制定将需要较长的时间。考虑到利益的复杂性,在这个传统机制仍然占主导的层面上,小多边区域机制和双边机制要比全球机制如联合国更易于达成集体行动。这一方面是因为区域成员由于地缘相邻和区域内经济合作机制共享更多的利益关切;另一方面也是因为成员数目较少,利益冲突更易于得到缓和,利益博弈的难度相对较低。

网络空间国际治理的最大特点也是对传统全球治理机制的最大冲击在于它催生了新的治理机构。如弥尔顿·穆勒所说,这些集中于技术和社会公共政策的治理机制——如 IETF、RIR、ICANN 和 IGF——将治理的决策权置于跨国的、非政府的相关行为体手中,"它们从民族国家的外部出现,提

供了新的制定有关互联网标准与关键资源的重要决策的权威场所；新兴的合作、讨论以及组织纷纷出现，使凭借新型的跨国政策网络以及凭借新型治理形式来解决互联网治理问题成为可能”。[①]更重要的是，这些新兴的治理机构凭借其特有的价值观和制度安排，正在逐渐对传统的治理机构带来冲击和挑战，促使传统的机构作出适当的调整和改变，以适应网络空间治理多元化、跨领域的复杂现实。

但是，从国际规范制定的角度来看，上述制度安排存在集体行动效率不一的问题。在技术层面，IETF 能够迅速高效地达成集体行动，拿出有效的技术解决方案，ICANN 也能够依靠自身政策制定流程，在域名和地址分配领域确保竞争与开放；在经济和国家安全层面，政府间的博弈常常导致联合国大会的谈判进程一波三折，但是其目标仍是达成具有约束力的规则；只有在社会公共政策领域，由于议题的复杂多元化，IGF 等论坛机制常常被诟病为“毫无意义的闲聊场所”。[②] 围绕议程的设置、顾问组和秘书处的代表权问题以及治理的根本原则等问题，IGF 始终未能找到有效的解决途径。2008 年 3 月，国际电信联盟秘书长在 ICANN 的一次会议中，明确表示 IGF 是“浪费时间”。[③]

然而，一个机制的重要与否并不能仅仅寄托于其能否达成集体行动。如果将规范产生的生命周期划分为规范出现（norm emergence）、规范梯级（norm cascade）和规范内化（norm internalization）三个阶段[④]，那么网络空间治理的进程仍然处于提出规范的第一阶段。网络空间规则的产生通常有赖于两个条件：一是规范推动者的宣传和劝说；二是规范推动者劝说行为的制度平台。从这个意义上说，作为一个以最具代表性的国际组织为依托的

---

① 弥尔顿·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 5—6 页。

② Jonathan Zittrain, *The Future of the Internet: And How to Stop It* (New Haven and London: Yale University Press, 2008), p. 43.

③ “China Threatens to Leave IGF,” *Internet Governance Project blog*, December 5, 2008, http://blog.internetgovernance.org/blog/_archives/2008/12/5/4008174.html, 访问时间：2017 年 6 月 8 日。

④ Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” *International* Organization, Vol. 52, No. 4, 1998, pp. 887-917.

专门机构,IGF 作为一个具有广泛代表性的全球平台,即使很难达成集体行动,但它也可以成为一个容纳广泛争论和利益冲突的宣传和劝说的重要平台,其存在的意义更多体现在对话而不是行动。

由此可见,在网络空间国际治理机制的复合体中,并非所有的制度安排都具有产生国际规范的能力。新兴的治理机构在制定全球技术标准方面发挥了绝对的主导作用;但在社会公共政策层面,它的扁平化结构无疑降低了产生集体行动的效率,因而在社会公共政策领域,新兴的制度安排可能更有助于实现"多利益相关方"之间的信息交流和沟通,但却很难成为国际规范制定和执行的场所。在经济和国家安全领域,传统的主权国家间的制度安排更有可能达成国际规范,但不同机制的效率也有不同,例如联合国机构固然更具代表性和合法性,但也同样降低了它的工作效率;相比之下,区域性的机制和双边的机制可能代表性不够,但达成国际规范的可能性却更大。当然,这并不是渲染传统的国际机制与新兴机制的对立,而是应根据议题的性质,寻求两种机制之间的平衡。

(三)行为体之间的力量博弈

无论是价值观的冲突还是制度安排的选择,其背后发挥作用的仍然是网络空间不同行为体之间的互动。网络空间中的行为体除了传统的国家行为体之外,还包括私营部门、非政府组织、个人用户等非国家行为体。与其他领域不同,网络空间多层次、多元化的冲突与风险的复杂特性决定了不同行为体都应在网络空间扮演好自身的角色,需要行为体之间的相互协作。然而,由于利益诉求的不同,网络空间国际秩序的建立不仅体现在国家之间的力量博弈,而且表现为国家与非国家行为体之间的权力争夺。在网络空间,非国家行为体的权力和力量相对上升,构成了对传统上由国家主导国际秩序的重要挑战,这是网络空间区别于现实空间国际秩序的最大特点。具体而言,它具有以下三点特征。

第一,私营部门对关键基础资源的掌控以及对国际规则制定的发言权上升。如前所述,全球互联网技术层面的标准和规范制定均有赖于私营部门主导的非营利性、非政府机构,这些机构在互联网关键基础资源领域牢牢掌控着国际规则的制定权,将政府排除在外。近两年来,随着网络空间向各

领域的逐渐延伸，这些私营机构并没有简单止步于技术领域的话语权，而是试图在国际规则层面发挥更大的作用。

2016 年 6 月，微软公司发布报告《从口头到行动：推动网络安全规范进程》，提出可依据间谍情报技术、攻击手法、攻击目标及专门知识来开展技术溯源，同时配合以信号情报、人力情报、测量与特征情报，甚至可以渗透攻击者系统寻找证据。2017 年 2 月，微软总裁布拉德·史密斯在美国召开的 RSA 网络安全大会上，呼吁制定全球“数字日内瓦公约”，保障网民和公司不受政府在网络空间中行动的伤害；其目标是希望政府在开展相关网络行动时，不要伤害互联网企业和普通用户的利益。[①] 2017 年 6 月 3 日，兰德公司发布报告《没有国家的溯源——走向网络空间的国际责任》，称“现在是时候建立一个国际性的溯源机构”，建议国际社会尽快建立一个独立、可信、权威和“去政府化”的 GCAC（全球网络溯源联盟）。[②]

微软公司的倡议在网络空间引发了诸多关注，这一方面凸显了网络空间安全风险的严峻以及国际社会相关防范机制的缺失，另一方面也反映出互联网企业对于维护网络空间的安全环境有着迫切的现实需要，这两点是很多知名互联网企业积极推动建立网络空间安全秩序的重要驱动力。之所以提出“去政府化”的倡议，固然是对私营企业主导的互联网“多利益相关方”实践的延续，更多的则是为了维护私营机构的利益，与政府保持相对的独立性。如果微软公司建立 GCAC 的“去政府化”倡议得以实现，那么私营机构在网络空间安全秩序的建立中将“再下一城”。

第二，互联网技术的低门槛、匿名性和攻击性赋予了黑客组织不对称性的权力，恶意网络攻击成为国家安全面临的重大威胁。恶意网络攻击对国家安全的威胁是全方位的，常常会造成重大的经济损失，破坏关键基础设施的正常运行，引发社会动荡，甚至会关系到政局的稳定。即便是拥有强大国家机器的政府，也必须正视恶意网络攻击所带来的威胁，与黑客组织的斗争刚刚开始。

---

① 鲁传颖：《“数字日内瓦公约”，球在美国手上》，《环球时报》2017 年 2 月 20 日。

② RAND Corporation, *Stateless Attribution: Toward International Accountability in Cyberspace*, June 2017.

近年来,全球恶意网络攻击持续增加,危害性也日渐增大,但是由于溯源的困难,国际社会对不知源于何处的"敌人"缺乏有效的应对;而由于战略意图传递受阻,信息的交流和互动缺乏明确的路径,传统的威慑机制在网络空间受到了很大的挑战。约瑟夫·奈认为,网络威慑主要有四种途径,即惩罚威胁(threat of punishment)、防御抑阻(denial by defense)、利益牵连(entanglement)以及规范禁忌(normative taboos),威慑的有效性则取决于实施过程中对威慑方式、威慑对象和具体行为三个关键因素的区分;在网络威慑的实施过程中,对于国家和非国家行为体、技术先进国家与落后国家、大国与小国的区分直接关系到网络威慑战略的手段和效果。① 2017 年 2 月,美国国防科学委员会发布题为《面向网络威慑的网络部队》的报告,详细研究了针对各种潜在网络攻击的威慑需求,提出了通过威慑、作战及升级控制应对网络"敌人"所需要的关键(网络及非网络)能力。②

值得一提的是,在政府与黑客组织的网络攻击攻防战中,非国家行为体的背后常常可以发现政府的影子。无论是 2008 年格鲁吉亚战争中的网络战还是 2010 年伊朗核设施遭受蠕虫病毒攻击,都被认为有政府力量的背后支持;2017 年 5 月在全球爆发的勒索病毒造成了数十亿美元的经济损失,危及一些国家关键基础设施的安全,但这些病毒武器的肆虐却与美国政府网络武器库管理不善直接相关。一般而言,能够针对一个国家发动网络攻击的能力,并不是某个私营机构或组织的技术能力和财力可以支撑的,而一旦实现了黑客组织和某些国家力量的"勾结",很可能会带来更大的安全威胁。

第三,国家行为体之间的博弈仍然是网络空间建立国际秩序的主要推动力,但与其他领域相比,其利益的博弈更加多元和复杂化。在网络空间,特别是随着议题由技术向经济、安全领域的逐层扩展,政府的主导权逐渐增强,国家间的博弈与冲突也愈发突出。

在早期的互联网治理进程中,国际社会常被划分为"两大阵营":一方是

---

① Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3, 2017, pp. 44-71.

② Defense Science Board of Department of Defense, *Task Force on Cyber Deterrence*, February 2017.

以欧美国家为代表的发达国家，它们坚持“多利益相关方”的治理模式，主张由非营利机构如 ICANN 来管理互联网；另一方是中国、俄罗斯、巴西等新兴国家，它们提倡政府主导的治理模式和“网络边界”“网络主权”的概念。这种阵营的划分是基于国家间信息技术发展水平的差距和治理理念的不同，前者作为既得利益者希望维护现有的治理模式，而后者则希望打破发达国家的垄断，争取更大的话语权。

但事实上，对于一个涵盖内容极为广泛的新兴议题而言，阵营的划分不可能是铁板一块。随着网络空间成为大国利益争夺的新领域，在利益的冲撞之下，各阵营内部均出现了离心倾向：美国和欧洲就隐私和数据保护问题各持己见；新兴经济体中巴西和印度都明确表示支持西方主导的“多利益相关方”模式，与中、俄立场有明显的不同；此外还有一些处于中间地带的国家，例如韩国、新加坡等，它们一方面支持“网络主权”的概念，另一方面也更加重视公民社会等非国家行为体。不过，传统的阵营划分也并不是完全的分崩离析，在涉及军事领域网络安全的国际谈判中，发达国家与发展中国家的对立仍然可见。2017 年 6 月，联合国框架下的 UNGGE 宣布谈判破裂，在国际法适用于网络空间等关键问题上，美欧等发达国家与中、俄、印等新兴经济体立场相左，无法调和，导致这一届工作组未能如期向联合国大会秘书长提交报告。

可以判断，国家之间的阵营今后将更多地基于议题(issue-based)而不是传统意义上的意识形态。从理性的角度分析，国家间博弈的依据是各自的国家利益，而由于国情的不同以及网络空间议题的多元化，不同的利益聚合点自然会带来不同的“阵营组合”，其目标是实现国家在综合国力竞争中的优势；但同时，网络空间中私营部门与政府之间在一定程度上的相互独立甚至是利益的对立，也提示了一种新的趋势：传统思维中的国家行为体博弈可能会更多汇聚于一个广义的网络安全领域。

五、中美关系与对策建议

当今世界仍然处于信息技术革命的浪潮之中，互联网、大数据、人工智能、云技术甚至很多我们至今未曾想象到的新技术将会不断涌现，越来越多

的人和越来越广泛的政治经济生活都将被裹挟其中,网络空间的内涵和外延不断扩大,网络空间面临的安全风险和冲突也必然层出不穷。网络空间的国际治理是从技术领域起步的,随后不断向其他领域延伸;网络空间国际秩序的形成也会基本遵循这一先后顺序,依据不同层次议题的特性,逐渐由技术层向高级政治领域递进。可以预见,在未来较长的一段时期内,网络空间国际秩序的形成将会呈现一种动态的演进过程,新的行为体、国际制度和国际规范将会不断出现,或在某些领域形成新的秩序,或促使已有的国际秩序根据变化的环境作出适应性的调整和改变。

从传统的国家视角来看,国际秩序主要是由大国建立的,网络空间国际秩序的建立也同样如此,特别是中、美两个大国之间的力量博弈。中、美作为当今世界最大的两个经济体,网络议题近几年在双边关系中占据了重要的位置,其合作与竞争并存的态势与两国的整体关系保持了一致。互联网的性质决定了网络空间是一个分布式的网络,没有任何一个国家或者行为体能够控制所有的网络节点和信息,这就意味着跨越国家的网络空间议题必须要通过不同国家和行为体之间的协作才能实现,垃圾邮件、网络犯罪、网络战皆是如此。但是,网络空间不可能脱离现实空间存在,它仍然处于无政府状态的国际背景之下,国家之间的竞争必然会延续至网络空间中来,其核心内容就是网络空间国际规则的制定和国际权力的再分配。

2012 年同样是中美网络关系的一个重要节点,经历了谷歌退出中国和美国诬蔑并起诉 5 名中国军官的跌宕起伏之后,网络冲突在中美关系中的重要性日趋显现,逐渐上升至首脑外交的战略层面。在主导意识形态方面,美国政府近年来大力倡导“多利益相关方”的治理模式,认为互联网治理应由私营部门主导,而政府不应参与其中;中国则认为网络空间治理需要多方的共同合作,每一个行为体都应发挥各自的作用,政府不应被排除在外。在制度安排的选择上,美国更倾向于让私营机构以及双边和区域政府间机制发挥作用,中国则更强调发挥联合国的作用。在国际规范的制定方面,美国强调应确保互联网的自由、民主和开放,“一个世界、一个互联网”;中国则强调建立“网络空间命运共同体”,建立互联互通也应确保政府在境内管辖的相关网络设施和事务的主权。在数字经济领域,美国提出了以跨境数据自由流动为核心的经贸规则;中国则更加重视维护本国的数据安全,近期更是发

布了《个人信息和重要数据出境安全评估办法(征求意见稿)》。在网络安全领域,美国提出原有的相关国际法如"武装冲突法"应适用于网络空间,中国则强调《联合国宪章》的基本原则同样适用于网络空间的国家行为体规范。

从近两年的走势来看,中美在全球网络空间规则制定中的合作还是取得了一定的进展。2015 年 6 月 UNGGE 的最终框架达成,一方面,报告强调国际法、《联合国宪章》和主权原则的重要性,指出各国拥有采取与国际法相符并得到《联合国宪章》承认措施的固有权利;另一方面,报告提到既定的国际法原则,包括人道主义原则、必要性原则、相称原则和区分原则,回应了美国等发达国家的关切。[①] 2015 年 12 月,WSIS 的十年审查高级别会议成果文件也同时承认了"多利益相关方"和"多边主义"两者的适用条件,承认了两种模式的合法性。这两项重要的谈判成果可以被看作中美两国在网络关系极度恶化之后达成的历史性多边合作成果,为网络空间行为准则的制定奠定了一定的基础。

就双边关系而言,中美两国已经展开了多轮网络安全对话,并且建立了执法与网络安全高级别对话机制,这是合作的一面;但竞争的一面更不能忽视,2017 年 6 月 UNGGE 谈判破裂就充分说明中美之间的博弈还将在很长时间内持续。国际制度具有"非中性"的特征,即对具有不同优势和实力的国家而言,它所能带来的效果和影响是不同的。美国是互联网的缔造者,由于客观历史因素,美国(包括私营企业和非政府机构)的治理主体在各个国际治理机制中都占有明显的优势,这种优势更是凭借其当前领先的信息技术水平和大量的优秀人才而得到进一步强化,并最终转化为塑造国际规则的强大能力。中国这样在互联网发展中属于后来居上者的新兴国家,与美国相比还是有相当明显的实力差距,这也意味着中美两国在网络空间的一些核心议题上具有完全不同的利益诉求,很难在现阶段达成一致的立场。

然而,在网络空间国际秩序亟待建立的形势下,作为世界第二大经济体和在国际社会中日益发挥重要作用的大国,中国仍然面临着难得的历史机遇。近两年来,中国的网络外交表现得相当积极进取,不仅提出了缔造"网

① 联合国大会:《关于从国际安全的角度看信息和电信领域的发展政府专家组的报告》,A/70/174,2015 年 7 月 22 日。

络空间命运共同体”等一系列理念、主张和原则,更是主办和积极参加了世界互联网大会、UNGGE、ICANN 大会等重要的国际会议,并积极推动“一带一路”、G20、金砖国家等多边合作框架中有关网络议题的国际对话与合作。中国积极参与国际互联网治理进程,意味着我们一方面要接受现有的治理体系,另一方面又要谋求改善和应对现有体系中于己不利的部分。

为了推动建立公正、合理的网络空间国际秩序,中国可以从以下三个方面着手:首先,在价值观层面,以实际行动配合外交理念的推广,将习近平主席提出的“尊重网络主权、维护和平安全、促进开放合作、构建良好秩序”的基本理念落到实处。结合整体外交战略,中国近几年在全球治理中积极倡导“命运共同体”的理念,在网络空间也提出了建立“网络空间命运共同体”的愿景。但对于国际社会而言,外交理念需要实际行动相配合才更具说服力,例如,我国不妨针对当前国际社会面临的威胁,如勒索病毒的肆虐,倡议建立相应的国际应对机制。

其次,在制度安排层面,中国应保持开放、包容的心态,针对不同的国际制度平台进行理性、客观的评估并制定相应的对策,尽可能实现利益和效率的最大化。例如,对 I* 等技术层面的机制,中国应积极鼓励政府和私营企业相关技术部门的深度融入,在技术创新和管理上下功夫;对 IGF 和 WSIS 等“闲谈”机制,政府部门可以保持适度介入,采取切实举措大力支持私营部门、学术界等其他利益相关方的参与,在其背后掌控大局;对传统治理机制下的网络议题,政府应加强与相关私营部门等其他相关方的信息共享、咨询和沟通,建立以政府为中心的辐射式支持模式。

最后,建立网络空间良好的国际秩序,应在积极参加网络空间国际规则制定的同时,重视国内网络空间秩序的建立,实现内外兼修。外交是内政的延伸,中国参与网络空间国际规范的制定必然会受到国内政策和理念的影响,而网络空间国际治理的趋势和理念也会对中国国内政策产生倒逼效应,从而带动和影响国内秩序的建立。如此,中国应从自身着眼,加强能力建设,理顺部门关系,加强跨学科、跨领域的信息共享机制的建立和全方面人才培养,而内外统筹的根本目的是服务于中国的国家利益,早日实现网络强国和“两个一百年”的奋斗目标以及中华民族伟大复兴的中国梦。