大数据时代的网络安全治理：议题领域与权力博弈*

任　琳　吕　欣

摘　要：网络空间治理的核心问题包括由谁治理、治理什么、如何实现公平有效的治理等。网络安全治理的议题包括对网络基础设施、流动于其中的数据、网络内容与文化和网络行为等的治理。治理的目标包括通过治理确保国家安全、谨防网络军事化趋势、避免陷入网络战漩涡、维护社会稳定，反对网络恐怖主义，打击网络犯罪，确保基础设施安全、个人信息与人身安全。在治理过程中又需要注意提升国家参与网络空间治理的能力，具体包括技术性权力、解释性权力和制度性权力，进而努力实现公平、有序的治理。

关键词：大数据　网络安全　全球治理　权力博弈

中图分类号：D80　**文献标识码：**A　**文章编号：**1005-4812(2017)01-0130-143

对网络空间的安全进行治理，首先需要厘清治理的领域、对象、内容和方式。唯有了解问题之所在，方能对症下药。网络空间的物理载体、流动于其中的信息以及与该两者相关的行动，都是治理的对象。它们如同一把双刃剑，既带来了进步，也造成了前所未有的安全隐患。而应对这些问题的国际规范是否成熟呢？很遗憾，答案是否定的。作为一个新兴战略增长点和新的安全领域，网络尚处在治理规范相当不完善的初级阶段。国际上已经对网络治理做出了众多尝试性努力，如中美等主要大国积极谋求开展关于网络安全的双边对话与合作，欧盟等区域性的网络安全治理不断走向规范化，联合国等传统国际组织努力寻求在网络安全规范的制定中发挥作用。然而，不得不承认的是，网络安全治理仍然处于一个十分

*本文是国家社会科学基金重大项目“网络空间的国家安全战略”（项目编号：11&ZD061）的阶段性成果。

不完善的阶段，各项工作面临诸多难题，包括治理主客体不明确、基本概念不清晰、治理领域界限模糊、适用规范不明等。它们无不构成网络安全治理难以摆脱的法律困境。

一、网络空间治理的挑战和机遇

以既有的概念理解，网络空间治理包括两个方面：一是信息安全（数据安全和相关内容安全），二是网络安全。前者以网络空间中的流动数据为重点，后者强调的是作为物理介质的空间本身的安全，数据通过相关物理介质在网络空间里传输。而信息借助网络传输和储存，标志着大数据时代的到来。

以大数据为特征的网络时代，是如何推动人类社会进步的呢？首先，大数据为世界经济的发展提供动力。云计算、移动通讯、互联网和物联网的普及促进了商业的迅猛发展。互联网作为知识、信息和财富的新载体，逐步承担起推动经济增长新动力的重任。信息产业迅速扩展，以迅雷不及掩耳之势传递海量商业信息，促进经贸往来，配置全球资源，提高劳动生产率；其次，数据和信息在网络空间的自由流动，在一定程度上促进了全球文化的融合；再次，网络空间在国际关系领域的形成导致国际关系主体的骤然多元化。[①]个人、团体和组织等行为体借助这一渠道，迅速地了解和传递信息，大大增强了其参与全球事务的能力。最后，互联网技术和信息传输逐渐成为推动军事领域创新和发展的重要依托。

大数据在带来商业机遇、通信便利、国防能力增强及社会生活其他领域进步的同时，也带来了不少治理难题和挑战。

首先，某一国家一旦掌控网络空间的基础设施和流动于其中的数据，便有将之转化为实现霸权工具的可能。基础设施安全是数据安全得以保障的基础。物理层面的技术主导权具有决定性作用，国家在网络空间中的竞争地位可以由其确定。网络弱国往往缺乏对物理层面的主导权，进而难以确保数据安全。

其次，由于信息具有带来福祉或强化暴力的能力，网络空间中的“马太效应”能够迅速扩展至现实生活，并进一步强化其效果。因此，如何治理流动中的信息成为值得人们深思的重大问题：一方面，应合理界定数据产权，避免窃密或侵权；另一方面，确保必要的技术进步和信息扩散服务于人类发展。信息革命扩大了发达国家与发展中国家之间、发达地区与发展中地区之间的“数字鸿沟”，

① [美]曼纽尔喀斯特著，夏铸九，王志弘等译：《网络社会的崛起》，北京：社会科学文献出版社，2001年版，第91页。

导致不平等产生的几率和社会不稳定因素增加。

再次，互联网的普及虽然使相对弱势的文化获得平等传播的渠道，却无法避免强势文化的长驱直入，导致不公平竞争。西方发达国家占有网络空间中的传播优势，例如，英语作为世界语言而得以广泛普及，欧美国家借助其所主导的全球化进程在世界范围内大量建构和推广强势文明。

最后，网络空间行为亟需规范。例如，全球金融信息联动使部分掌控全球金融网络的国家或其他行为体可控制一方的经济命脉，可能导致该地区或更大范围内的经济波动、骚乱甚至经济崩盘。此外，从某种意义上说，具有隐蔽性的网络空间天生是恐怖主义隐身的“港湾”，恐怖势力通过向社交网络渗透或借助黑客传递信息、招募成员、筹集资金、扩张实力，以多种方式破坏社会稳定。[①]

大数据时代的网络安全治理内容庞杂、困难之大前所未有。在一些重要的国际论坛或国际组织平台上，中美等各主要国家多次就网络安全及其治理展开对话，以期通过共同商议，有针对性地解决这些难题，如 2015 年 G20 峰会公报对网络安全治理进行了论述。[②]公报认为网络安全治理系指对网络空间的物理介质及其中所流动的数据进行治理，而治理的目标是实现国家安全、社会稳定和经济繁荣。

二、网络安全治理的议题领域

结合国际上诸多官方讨论和学术研究，对网络空间安全治理进行梳理和总结，可大致将其分为以下几个领域：（1）网络空间“物理疆界”的治理，即网络基础设施的管理；（2）网络空间中大数据的治理；（3）网络文化空间及内容的治理；（4）网络空间行为的治理，主要涉及打击跨国网络犯罪、网络恐怖主义以及对通过网络空间实施的金融制裁加以规范等。诚然，由于彼此间存在着诸多交叉，很难对各领域的界限作出清晰的划分。

（一）网络基础设施安全的治理

网络基础设施的安全是网络安全的物质基础，因而网络基础设施的重要性受到世界各国的高度关注。例如，2014 年 1 月 10 日，俄罗斯出台了《俄罗斯联邦网络安全战略构想》。在某种意义上，没有网络基础设施的安全，就没有数据安全。因此，在论及网络空间治理规则之际，必须首先重视在该层面上制定合理的

① 李刚，朱文：“基地组织、ISIS 网络恐怖主义纪实解密暴恐‘双煞’的网络‘花招’”，载《中国信息安全》2014 年第 10 期，第 90-101 页。

② http://www.g20.org/hywj/lnG20gb/index.html

规范，确保其关键基础设施的安全。后者主要体现在 CPU、操作系统和网络三个技术层面。[①]实现这三个层面的技术自主，是确保物理层面国家网络安全的必由之路。通过“市场换技术”、合资和引进，一些电信企业已逐步实现了交换机等联网设备的自主研发。在自主研制 CPU 和操作系统的道路上，中国电科等大企业正奋力前行。

此外，实施网络基础设施的管理，离不开依照规范明确地界定网络的“物理疆域”。实现对其合法而有效的治理，必须在互联网之“根”的管理中获得治理的合法性，后者建立在共有和共治的基础上。然而，现实状态并非如此乐观。不少学者认为，导致物理疆界模糊的根本原因之一是根服务器的全球共同监管长期未能实现，即使 ICANN 的私有化也并非是将之移交联合国，而是交由“全球利益攸关者”管理。[②]这意味着对它的松散化治理和寡头垄断。其结果必然是具备技术和管理经验优势的国家或行为体将继续垄断 I CANN 的控制权。因此，从物理层面上看，网络基础设施的治理从根源上就存在严重的信息不对称。基础性的界定做不好，更难以制定治理规范，进而确保监管电力、交通、银行等关键基础设施的安全。

从规范层面上看，治理中也会相应地遇到一些争议和难点。网络空间的运行逻辑和现实世界不同。主权国家的地理疆界并不与信息流动的边界相重合，“越境”破坏电力、交通、银行等关键基础设施的行为很难得到有效监管。由于互联网已成为当今世界信息传播的主要渠道，国家很可能因对其依赖程度的愈益加深而损失巨大。如若众多核心领域的网络基础设施暴露于不安全的外部环境之中或受制于人，确保国家安全便几乎无从谈起。例如，一条光缆被破坏可能会造成交通瘫痪。又如，操控水电站的网络一旦瘫痪，成千上万人的生活就可能受到影响。因此，避免网络基础设施遭到破坏，成为当今时代国家的重要利益之所在。

然而，某些大国以此为借口，诉诸网络军事化的趋势依然十分明显。例如，2015 年 2 月 6 日，美国《国家安全战略》提出，美国国防司令部将加强网络能

[①] 苏金树：“网络空间基础设施核心要素的自主之路”，载《信息安全研究》2016 年第 5 期，第 462-466 页。

[②] 域名解析系统或曰 DNS（Domain Name System）是互联网运行和管理的中枢，用于将域名转化为网络有效识别的 IP 地址。三种主要的域名服务器包括本地域名服务器、根域名服务器和授权域名服务器。根域名向服务器回应与提供主机要求的查询，向互联网终端的用户提供域名解析服务。掌握了根域，可以将物理占有和技术优势转化为实际控制，也就意味着掌握了全球互联网管理的技术规则主导权。

力建设，以网络行动破坏敌方的指令和基础设施，销毁其武器。[①]为替其网络军事化造势，美国一方面继续倡导借助互联网打击恐怖主义；另一方面又不断设置假想敌，指摘其他国家。在一定程度上，对攻击方并不确定的黑客行为作政治化的解读，旨在为网络空间的军事化寻找说辞。通过无限夸大所谓来自中国黑客的攻击，将黑客的个人行为等同于国家行为，并认定这些攻击危害了美国的关键信息基础设施，如“电力网络的控制计算机、金融交易系统的中央服务器、航空调度系统的主控服务器等等”。[②]这一行为严重损害了双边关系。实现对网络空间的有效治理，必须避免恶意的政治化行为并谨防其军事化。网络军事化趋势一旦加剧，极有可能将网络空间推入军备竞赛的漩涡，同时也很难避免其“硝烟”蔓延至现实世界，造成严重损失。

综上所述，网络安全治理需要明确规定网络安全优先事项与保障范围，制定全面系统的保障措施。维护网络基础设施的安全并不意味着以此为借口扩军备战，而有赖于国际社会各成员的相互对话、合作及共同治理。从源头上寻求治理的合法性，明确界定和保护“网络空间的物理介质”，是规范网络空间行为、确保网络基础设施安全的基础。

（二）网络空间中流动数据的治理

信息泛指流通于网络空间之内的各类数据。就数据的“流动”而言，主要涉及跨国流动、数据开放、隐私和机密等。所谓信息或数据安全并不会给世人以陌生感，“棱镜门”事件无疑令人警觉。通过监控流动中的数据，美国对全球各地可谓一览无余。网络信息安全不仅仅涉及个人隐私，而且关乎国家命运，不能不为各国所高度重视。

一国的国防安全与数据安全息息相关。首先，从军事和国防安全的角度看，数据的疆界并不清晰，难以有效地治理流动于其中的数据。不确定性极高的网络战略互动很容易导致互信缺失，战略行为失范，甚至逐步走向网络空间的“军事化”，最终令系统陷入战略不稳定而难以自拔。其较为典型的案例是“棱镜计划”，它的前身是“9·11”事件后美国为打击恐怖分子所采取的监听计划。通过加以秘密的“政治化”和“军事化”，局部性的监听逐步演化为其对象遍及境内境外、无所不包的“棱镜计划”。据已披露信息，美国国安局已对中国、法国、德国、英国、西班牙以及墨西哥、巴西实行监控。“棱镜计划”给人们提了个醒，致使

① “Fact Sheet: The 2015 National Security Strategy”, https://www.whitehouse.gov/the-press-office/2015/02/06/fact-sheet-2015-national-security-strategy

② 沈逸：“数字空间的认知、竞争与合作”，载《外交评论》2010年第2期，第38-47页。

其不得不感叹数据隐私成为稀有物品，而各国也深感国家信息安全之门难以守护。“棱镜门”折射出美国将信息安全“军事化”的图谋。该事件被曝光后，美国非但未曾向受害国家道歉，反而进一步为“军事化”寻找借口，转移视线。例如，美国想方设法在网络空间视角下，极力渲染“中国威胁论”。美国对其遭受的黑客攻击作出具有明显“政治化”倾向的解读，常常混淆事实，从而以此为契机，加快网络军事能力建设的步伐，这难免会破坏双边或多边关系的健康发展。因此，有必要在全球范围内作好顶层设计，制定共识性规范，探讨对流动数据实行管辖的合理范围，尊重各国对国防和军事安全的维护，谨防部分国家行为的过度军事化。

其次，从个人隐私层面看，游走于网络空间中的个人，其个体的信息安全很难被保证。如 2016 年 2 月，推特（Twitter）的密码恢复系统发生故障，导致上万名网民信息的泄漏。如果没有相应的治理规范和应对措施，与之相类似的事件很难得到有效的处理，用户的信息安全无法得到足够的尊重和保障。又如，英国宽带服务提供商滔客（TalkTalk）因受到攻击，泄漏了约 400 多万用户的隐私数据，其中不仅仅有姓名、家庭或工作地址、电子邮箱和账号等常规数据，甚至包括他们的信用卡账号等信息。在多次遭到攻击之后，滔客即便采取了预警措施，给用户造成的损失依然严重。此外，美国医疗保险公司 ANTM(Anthem)受到网络攻击，大量用户的私人信息被曝光，后者包括用户的姓名、出生日期、身份证明、社保信息等。诸如此类的事件数不胜数。

再次，经济生活中的信息安全治理包含了颇为丰富的内容，如商业机密（知识产权）、电子商务和信息产业标准化等。这些领域内数据泄漏带来的损失往往难以弥补，对其网络安全的治理因而迫在眉睫。管控经济数据的流动需要关注信息产业的治理，包括完善行业标准、贸易投资规则等。在过去两年内，不少著名的全球 500 强企业都曾遭受黑客袭击，其中甚至不乏索尼和苹果等著名的电子品制造商，还包括一些金融巨头，如摩根大通。这些企业深受数据泄漏之苦，经济损失惨重，殃及范围极广。以 2014 年摩根大通银行所受攻击为例，其影响波及美国 1/4 的人口，7600 万家庭和 700 万小企业，包括银行信息在内的个人数据被全部窃走，妨害了正当的商业竞争。

在个人和企业为饱受信息泄露之害而烦恼之时，国际上却并无相应的准则、规范和法律对此加以治理。如果没有足够的安全意识，特别是完备的法律体系和国际规范，游走在网络空间中的个人和企业会几乎如“透明人”一般暴露于潜在

攻击者的面前。因此，治理流动中的信息，需要建立起相对成熟的信息安全评级体系与治理机制，一方面加强全球顶层设计，另一方面采取有针对性的措施，如此方能卓有成效地落实对数据安全的保护、问责及实施相关处罚。缺乏完备的治理规范必导致该领域“责任人”的缺位。随着信息通信手段被更广泛地运用于经济领域（如大量的电子商务），数据安全监管不力所造成的损失将难以估量。

最后，在发展层面上，通过数据流动造福人类，应防止地区间的不平衡，即“数字鸿沟”的出现。在互联网时代，保护知识产权当有合理的限度。在强调保护知识产权的同时，也需避免数据资源分配不均带来的各地区发展不均衡，借助合法的技术与商业数据促进经济增长。以美国为代表的发达国家凭借在高技术领域的优势地位，就知识产权保护提出苛刻的要求，为高技术产品贸易设置壁垒，从而不利于世界经济一体化和人类共同繁荣。先进技术和产品的推广受阻，在一定程度上限制了发展中国家及其民众共享科技进步成果的机会，阻碍了人类社会的整体进步。因此，治理规则的制定也应避免“数字鸿沟”的加深，确保世界各国的发展权均得到保障。

（三）网络文化空间及内容的治理

互联网时代在为各国文化的传播带来新机遇的同时，也使其面临挑战。各国日益视文化为国家发展的重要战略资源。强势文化对弱势文化的“蚕食”历史上比比皆是。互联网传播的速度更快，范围更广，致使上述二者间不对称竞争的烈度加剧。网络信息霸权和文化帝国主义[①]给国际社会造成的威胁前所未有，与之相应的文化安全问题由此产生。[②]面对强势文化的挑战，一方面，各国必须坚定不移地捍卫其“文化主权”，另一方面，应当以开放和自信的态度，通过文化的交流与传播增强本国的文化软实力。在不断拓展视野，从世界文明的丰富宝藏中汲取养分的过程中，还需发掘本民族文化的优秀资源，向世界传播自己的优秀文化。以中国文化的传播为例，通过讲好中国故事，使中国文化走出去，增强文化自信。

此外，许多争论围绕互联网内容的治理而展开。有人认为，网络空间中的内容应完全自由流动，不受任何限制；但一旦暴力、色情、谣言等内容以网络空间为介质大肆传播，便极有可能危及现实社会的安全与稳定。网络文化空间需要有颇具包容性的发展理念，也亟需有针对性的治理规范。确保文化创新、文化包容

① 蔡文之：《网络：21 世纪的权力与挑战》，上海：上海人民出版社，2007 年版，第 42 页。
② [德]哈拉尔德·米勒著，郦红，那滨译：《文化共存—对塞缪尔·亨廷顿‘文明冲突论’的批判》，北京：新华出版社，1998 年版，第 18 页。

和文化传播是网络文化空间保持其活力的重要途径，而消解恶性的网络舆情，维护社会稳定则系保障网络空间运作合法有序的必要之举。如若引导得当，对互联网言论的保护和规范可使网络文化空间在推动文化产业的发展中发挥不容小觑的作用，带来巨大的现实利好。网络空间还有助于建立政府与市民社会的良性对话机制，提高决策层治国理政的能力，促进对腐败等违法犯罪行为的有效打击等。在完善内容治理的规范之际，可以结合实际情况，从利益相关者呈多元化态势的角度出发，鼓励和引导相关互联网企业和网民参与其中，促使其在规约自身行为的同时，勇于承担更多的社会责任。

（四）网络行为的治理

谈及网络空间里的行为治理，便无法回避网络空间对行为互动与行为取向的特殊塑造作用。网络空间营造的特殊环境能够对个人与个人、个人与国家、国家与国家之间的传统交往及互动方式加以重塑。这主要表现在以下几个方面：一是网络空间不受地理意义上的地缘边界辖制，不为现实世界中力量投送的“射程”所限；二是网络空间中各行为体的实力不尽对称，即使是个人（如网络黑客、网络恐怖主义者），也有能力单枪匹马地发动针对国家等更大行为体的袭击；三是随着网络技术的突飞猛进，划分弱国、强国、中等国家的传统标准似乎已不再适用。此外，网络空间环境还具有开放性、交互性、虚拟性、分散性等特征。

在上述现象中，与虚拟性相伴而生的信息“不对称”成为对网络行为事先预警和事后治理的桎梏。信息的“不对称”所描述的是一种无法确认攻击源、无法预知攻击时间和攻击对象的状态。在计算机终端的后面可能坐着一个恐怖分子，其在网络紧身衣的保护下巧妙地隐藏身份，在无法预知的时间点，以无法预知的手段，突然发起网络攻击。这种新型恐怖主义的危害常常超过以往任何一种恐怖行为。[①]信息的“不对称性”增加了网络犯罪行为治理的难度。

网络行为治理问题主要涉及跨国网络犯罪、网络恐怖主义、借助网络空间实施的非适度的金融制裁等。对之进行打击、惩罚、规范或者治理，同样亟需制定成熟的国际准则和规范。如果对此类行为不予以有效惩治，不仅会造成网络空间内的混乱，还将殃及现实世界的稳定与发展。不少国家纷纷采取打击网络恐怖主义的行动，如美国在2001年“9·11”之后增加相关开支，加大对网络恐怖活动的打击力度。一些大国建立彼此间的信息（情报）共享机制，合作打击恐怖主义行为。上合组织在其框架内“规定了各方应依据其国内法原则，通过立法等措施，

[①] Walter Laqueur, “Postmodern Terrorism”, in *Foreign Affairs*, September/October, 1996, p.35.

监控金融交易，防范和打击恐怖主义融资活动”。[①]由于恐怖组织的人员招募和融资行为往往通过网络进行，信息共享及网络监管中的相互合作成为打击这些行为不可或缺的举措。

在网络空间行为的合作治理方面，不少国家和地区纷纷建立信息共享和预警机制。例如，2013年1月，欧盟成立了“欧洲网络犯罪中心”，旨在打击网络犯罪行为，保护企业和民众免受其侵害。2013年，《欧盟网络安全战略》建议通过立法巩固欧盟信息系统安全，规范网络空间行为，保障网络购物环境的安全，刺激经济增长。2014年，欧委会公布网络安全新战略，建立预防机制，防范网络安全风险，共享风险预警信息。

网络空间的特性导致治理和规范网络行为对大数据的全面收集和分析产生依赖。网络空间治理在仰赖大数据的同时，也不得不面对后者数据量庞大、时效性极强、内容异常复杂等问题。这无疑需要突破数据瓶颈，对复杂且看似毫无规律的大数据进行卓有成效的整理和分析，以超越原始CPU处理速度和非常规的数据处理方式有效地整合大数据，从庞杂无章中觅得“数据中的模式”，指导现实对策的制定。[②]诸如相关性分析等一些手段，可以被用于支持大数据分析。[③]最后，在强调对数据的分享、利用、共同治理的同时，还需要规范大数据的运用。这显然需要制定配套的法律规范，对大数据的收集和利用作出明确的界定，将其限制在合理、合法的范围内。

网络的连通性使一些现实的战略行动得以以更强的力度展开。虽然网络空间刚开始在战略领域“一展身手”，但其打击力度、杀伤性或破坏性极大，因此亟需采取有效手段加以监管。凭借金融制裁的巨大威力，对他国实行威慑或“惩罚”，进行战略施压即其中一例。2012年，迫于美国的压力，世界各国金融机构赖以开展金融交易的环球同业银行金融电讯协会(SWIFT)发出禁令，禁止伊朗利用其进行交易，以防止伊朗获取发展资金、技术和设备。之后，欧盟紧随美国，也向伊朗“关门”。在此情境下，遭受制裁的伊朗银行及实体行业全然无法通过SWIFT网络从事交易。石油生产与出口受阻，无疑将伊朗的经济拖入寒冬，其货币里亚尔大幅贬值。一时间，伊朗国内物价上涨，通货膨胀率居高不下，失业率急剧上

① http://legal.people.com.cn/n/2014/1230/c188502-26297011.html

② 参见[美]陈封能，[美]斯坦巴赫，[美]库玛尔著，范明，范宏建等译，《数据挖掘导论》，北京：人民邮电出版社，2006年版，第1，5章。

③ Kennetch Cukier, Viktor Mayer-Schoenberger, “The Rise of Big Data: How It’s Changing the Way We Think About the World”, in *Foreign Affairs*, Vol.92, No.3, 2013, pp.28-40.

升。由此产生的种种社会问题令其国内局势一度陷入动荡。由此可见，借助网络实施金融制裁的威力之大，超乎想象，但这也带来对合理性边界的认定问题。如果缺乏有效和公正的治理规范，这种制裁“武器”很可能被滥用。

三、网络安全治理能力与三种权力

网络空间是一个崭新的战略增长点和国家互动领域，尚缺乏健全的治理规范。一方面，作为非传统安全的典型领域，网络空间具有有别于现实空间的互动逻辑，对它的治理颇为复杂，具有极大的不确定性；另一方面，该领域进入人们的生活方为时不久，在国际和国内层面，均还未能形成成熟的法律和规范体系，难以应对各国面临的新挑战。在这一情形下，相关规则的不健全导致治理中存在大量的“灰色地带”。概念、权利和义务的主体与客体仍未厘清。此外，在治理规范的制定过程中占得先机，意味着在制度议程的设定和条款的解释中占据优势。换言之，某一国家或其他行为体若凭借其技术或其他客观优势，在网络空间治理规范的制定过程中抢占了先机，便赢得了议程设置之“先行者”的权力，可能将自身利益“嵌入”国际制度和规范中，这在很大程度上决定了网络空间权力结构的发展趋势。因此，新兴国家和发展中国家在对网络空间治理的参与中，亦需要注意提升本国的相关能力，具体包括技术性权力，解释性权力和制度性权力，进而致力于进行公平、有序的治理。上述三种权力相互联系，共同作用，对网络空间的真实博弈施加影响。

首先，技术性权力是一种基础性权力，起着助推剂的作用，占据技术上的领先地位便确保了在其他两种权力中的优势。其次，制度性权力一方面是技术领先的制度体现，另一方面又是奠定未来网络空间基本权力格局的基本规制性力量。最后，网络空间的运行秩序和规范并不定型，也非一成不变，而是留有解释的空间，这就是解释性权力。它是其他两种权力的“压仓石”。使解释话语保持中性，避免偏颇，能够奠定治理的合法性基础；解释话语被强权控制则会将整个治理秩序推向极端化的歧途。

没有网络基础设施的安全，就没有网络空间的整体安全。而网络基础设施的安全从根本上必须依靠技术领域的不断进步。正如俄罗斯已痛下“决战”信息化的决心，普京强调，“信息资源和信息基础设施已成为争夺全球制高点的舞台，未来的政治和经济状况均取决于信息资源”。技术型权力指的正是国家以网络技

术为支柱的权力，而网络技术的核心是信息与知识等“软性”的权力。[①]技术领域中往往存在“马太效应”，因而强者越强，弱者越弱。前者可以利用高技术门槛，将其他国家拒之门外，进一步扩大优势。其一方面继续保持技术领先；另一方面，又把这一领先拓展到更为广阔的领域。发达国家始终保有其在尖端互联网技术领域的领军者地位，如若关键性产品的源代码不开放，便难以对数据的运作实行监管。再者，软件的主要供应商基本来自美国（如微软），一旦软件自给未能实现，数据安全便难以确保，而目前无论是硬件抑或软件的自给之路皆愈加曲折。通过合资、引进和“市场换技术”，国内的技术研发正逐步走向自主。[②]然而，又当如何处理国内技术研发与国际合作的关系？是否可单纯地依赖企业和市场行为，承担起维护国家网络安全的重任？这些问题尚悬而未决。

技术上较为发达的国家，往往在对外交往及国际标准和规则的制定中占有强势地位。制度性权力就是这样一种建立在技术性权力基础上的权力的表现，虽然后者并不一定是前者的必然条件。这种制度性权力尤其是指在一个规范尚不健全、制度建设有欠完善的领域，国家或其他行为体由于种种客观原因，巧妙地把握这一“制度中空”的机会，依靠相对的权力优势，通过主导性话语权，积极谋求建立制度的“先行权”。通过掌管议程的设置，进一步引领治理规范的导向，进而将自身利益嵌入其中。之所以说制度性权力以主导议程的设置为其主要表现形式，个中的主要原因在于每一个国家和行为体都有自己心目中的轻重缓急，对不同议题的偏好各异。制度性权力由谁掌握，谁就能把自己的议题偏好高置于组织的议程之上，并以此作为制定行为规范的依据。是否能够将自己感兴趣的议题和于己有利的规范转化为组织的议程和规范，直接决定了国家或其他行为体参与治理的目标能否实现。在这个意义上，国际议程设置“是一个政治问题。议题本身的轻重缓急可能并不是决定其能否列入国际议程的主要指标；相反，国家间的权力博弈、是否拥有议程‘进入渠道’或靠近议程‘切入点’，将是决定国际议程设置最终结果的最重要要素”。[③]只有强化自身治理能力的建设，才能在国际制度的建设中增强竞争力。如在进行有关网络安全标准的全球对话方面，发达国家的步伐显然更快。美国商务部下设的美国国家信息和技术研究所(National

---

① John Arquilla and David Ronfeldt, Information, Power, and Grand Strategy: In Athena's Camp: Preparing for Conflict in the Information Age, CSIS, 1996.

② 典型的合作案例包括中国电科与微软合作、浪潮与思科合作成立合资公司、清华紫光集团收购惠普旗下公司等。

③ 韦宗友：“国际议程设置：一种初步分析框架”，载《世界经济与政治》2011年第10期，第38-52页。

Institute of Standards and Technology)为政府制定信息安全的物理、技术和管理标准，在标准化方面发挥的作用最为显著。[①]而欧洲在欧盟的框架内也设有欧洲网络信息安全局（European Network and Information Security Agency），后者致力于欧洲网络和信息安全规则的制定。[②]只有优化网络安全治理的顶层设计并辅以完善的标准化体系，才能增强在国际对话及规则制定和制度建设中的竞争力。

在网络安全治理的布局中建立规范，也是通过掌握制度性权力，对其他国家或行为体施加影响的表现。为避免其中的恶性博弈，我们坚持将网络安全治理规范置于联合国框架内，正如 2015 年 G20 峰会公报所指出的，“我们还注意到联合国在这一背景下所制定相关规范所起到的重要作用，并欢迎联合国电信专家组在当前的国际安全形势之下所作的电信与信息领域 2015 年报告，遵守其确认的国际法，特别是联合国宪章，适用于信息与通信技术的运用及承诺范围内的国家行为这一观点。所有国家都应遵守联合国在 A/C.1/70/L.45 号决议中提出的各国须在信息与通信技术的使用过程中承担相关责任的原则。我们致力于协助保障整体环境，旨在参与各方皆能享受由信息与通信技术的安全使用带来的收益。”[③]

国家及其他行为体在网络空间中交往和互动的主要任务之一，是传播和推广其所推崇的理解方式、价值观和规范。这便涉及一种有“解释性权力”之称的权力表现方式。“国家软实力”的这一表现形式“取决于深层次的心理、文化和观念结构”，因而更为隐蔽，主要通过解释、说明和说服等途径发挥效用。[④]当在全球范围内制定富有权威性的治理规范的“任务”尚未完成之际，抢占诠释先机，引领治理规范的解释更凸显其重要性。在一些核心概念和治理理念的构建过程中，美国一再千方百计地主导其解释口径的设定。以“全球公域”（Global Commons）[⑤]为例，为在极地、海洋、太空和网络等领域扩展势力范围，分一杯羹，美反复强调其“公域性质”；而当某些概念开始限制或妨碍自身利益时，它也会毫不犹豫地加以摒弃或者创制新的概念（作为倡导海洋共同治理的国家，美

① http://www.nist.gov/
② https://www.enisa.europa.eu/
③ http://www.g20.org/hywj/lnG20gb/index.html
④ 蔡文之：《网络：21 世纪的权力与挑战》，第 5 页。
⑤ Abraham M. Denmark, “Managing the Global Commons” , in *The Washington Quarterly,* Vol. 33, No. 3 (June 2010), pp. 165-182; John Vogler, *The Global Commons: Environmental and Technological Governance*, Chichester, West Sussex, England: J. Wiley & Sons, 2000; Michael Goldman, ed., *Privatizing Nature: Political Struggles for the Global Commons*, London: Pluto Press, 1998; Magnus Wijkman, “Managing the Global Commons” , in *International Organization*, Vol. 36, No. 3, (Summer 1982), pp. 511-356; Susan J. Buck, *The Global Commons: An Introduction*, Washington, D. C.: Island Press, 1998, p. 1.

国却没有批准《联合国海洋法公约》，未将自身行为置于公约的规制之下）。在治理流动于网络空间中的数据和各种网络行为时，解释性权力十分重要。在治理网络内容和网络文化方面，掌握解释性权力的意义尤为突出，如有益于树立积极的社交传媒观，对绝大多数事物与现象作出正面解释，避免犯罪意图、恐怖主义行为等在网络空间中萌生。

结 语

网络空间治理的核心问题包括由谁治理、治理什么、如何实现公平有效的治理等。其中就治理什么而言，网络安全治理的议题包括对网络基础设施、流动于其中的数据、网络内容与文化和网络行为等的治理。本文梳理了上述议题领域，发现了网络安全治理规则相对缺失的现状并指出新兴国家和发展中国家在参与治理的过程中，也需要注意提升本国的相关能力。国家参与网络安全治理的能力会受到三种权力的影响，即各国间的博弈围绕技术性权力、解释性权力和制度性权力展开，三者相互联系，共同作用。[①]

在强调治理规则的制定和权力博弈的同时，各国都不能忘记的是，网络安全治理必须重视合作，面对网络空间的安全隐患，没有一个国家能够独善其身。例如，打击数据窃取，维护数据安全绝非一个国家或一个行为体之力所能及。地下信息黑市上，从对数据的盗取到对其被买卖、发包和利用，都形成了长长的产业链，且攻击方可能来自第二、第三国，无法加以有效的监管和防御。打击和治理此类行为，需要各国共同商讨。小到微型互动游戏平台，大到推特类的社交平台，再到网点遍布全球的跨国金融机构，均存在大量的数据安全隐患。如果没有共同监管和合作制定的治理规范，一些违法行为便难以得到防范和治理，用户的信息安全也无从说起。一些以网络设备等为载体的发电站、航空等关键基础设施也很可能因信息泄密而给人们的生活带来极大的损失。再如，打击网络恐怖主义，必须考虑其跨国性和信息不对称性。亟需各国信息共享，合作治理。但就目前而言，尚缺乏在国际层面上推动各国积极提供公共产品、参与治理网络恐怖主义的顶层制度设计。没有配套的治理规范，无法针对网络恐怖主义的特性，围绕跨境防御与依法打击网络犯罪进行合作。加之网络恐怖活动防不胜防，难以有效治理，且目前的技术手段颇为有限，对其的治理可谓困难重重。

总之，网络安全的合作治理乃大势所趋。对网络基础设施、流动中的数据、

① 任琳："多维度权力与网络安全治理"，载《世界经济与政治》2013年第10期，第38-57页。

网络内容与文化和诸多种类的网络行为的治理宗旨或目标予以概括，无疑为三个方面：一是通过治理确保国家安全（谨防网络军事化趋势、避免陷入网络战漩涡）；二是保障社会稳定（反对网络恐怖主义、网络犯罪，确保基础设施安全、个人信息及人身安全）；三是促进经济繁荣（营造安全的网络空间环境，为互联网经济提供边界，以此带动经济增长）。这三个方面的治理目标符合国际社会的根本利益，亟需通过各国间的合作得以实现。

（**作者简介**：任琳，中国社会科学院世界经济与政治研究所副研究员，博士，北京，100732；吕欣，国家信息中心研究员，北京，100045）

收稿日期：2016 年 4 月
（责任编辑：胡传荣）

Cyber Security Governance in the Era of Big data: Issues and Power Game

Ren Lin　Lv Xin

Abstract: The core issues of cyber security governance include who, what and how. The cyber security governance are governance of cyber infrastructure, the flow of data, cyber culture and cyber behavior, etc. The goal of governance is to ensure national security, avoid the trend of cyber militarization and even warfare, maintain social stability, be against cyber terrorism and cybercrime. During the governance process, in order to create a fair and order governance environment it is necessary to pay attention to enhance countries' ability to participate in cyber space governance, including technical power, interpretative power and institutional power.

Key words: Cyber Infrastructure; Global Governance; Cyber Security; Power Game