中国社会科学院世界经济与政治研究所
国际战略研究组
Working Paper No.201702
March 19, 2017
本文已发表于《国际观察》2017年第1期

任琳：renlin@cass.org.cn

大数据时代网络安全治理:议题领域与权力博弈 *

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。其中，就治理什么来说，网络安全治理的议题领域包括网络基础设施、流动中的数据、网络内容与文化和诸多网络行为等。治理目标包括是通过治理确保国家安全，谨慎网络军事化趋势、避免陷入网络战漩涡；维护社会稳定，反对网络恐怖主义、网络犯罪，确保基础设施安全、个人信息与人身安全；营造安全网络空

*本文作为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；任琳，中国社会科学院世界经济与政治研究所国际战略研究室副研究员；吕欣，国家信息中心研究员。

间环境，带动经济增长。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，进而努力营造公平、有序的治理。

关键词：网络基础设施　大数据　信息共享机制　网络安全

治理网络空间的安全问题，首先需要厘清治理的领域、对象、内容和方式。知道问题所在，才能进行有针对性的治理。网络空间的物理载体、其中流动的信息、以及与前两者有关的行动，都是治理的对象。网络空间及以其为载体的信息与数据像一把“双刃剑”，它带来了进步，也带来而来前所未有的安全隐患。那么，应对这些问题的国际规范又是否成熟呢？很遗憾，答案是否定的。网络作为一个新的战略增长点和新安全领域，其治理规范仍处在一个相当不完善的初步阶段。尽管我们看到了国际上很多尝试性的努力，例如：中美等主要大国积极谋求双边网络安全对话与合作；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积极谋求在制定网络安全规范方面发挥作用。然而，我们不得不承认网络安全的治理依然处在非常不完善的阶段，治理工作面临诸多难题，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。这些难题都构成了网络安全治理难解的法律困境。

一、网络空间治理的挑战与机遇

从既有的概念上理解，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。前者强调的是网络空间中流动数据的；后者强调的是空间本身作为物理介质的安全。前

者借助后者在网络空间里传输。而信息借助网络传输和储存，标志着一个大数据时代的到来。

以大数据为特征的网络时代，是如何推进人类社会进步的呢？首先，带来经济发展之动力。云计算、移动、互联网和物联网的普及造福于商业活动的迅猛发展。互联网作为知识、信息和财富的新载体，逐步承载起探索世界经济发展新动力的重任。信息产业迅速扩散 1，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，网络空间进入国际关系领域，参与国际事务的主体骤然多元化，个人、团体和组织等行为体借助网络空间这一渠道，迅速地了解和传递信息，大大增强了它们参与全球事务的能力。最后，互联网信息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技术依托。

大数据在带来商业机遇、通讯便利和提高国防能力的诸多进步之外，也带来了不少治理难题与挑战。

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，就有可能将之转化为实现霸权的工具。前者安全是实现后者安全的基础。物理层面的技术主导权具有决定性作用，能够决定国家在网络空间竞争中的地位。网络弱国往往对物理层面没有主导权，进而难以确保数据安全。

其次，由于信息具有带来财富或提升暴力的能力，网络空间里的“马太效应”能够迅速扩展到现实生活，并进一步扩大效能。因此，如何治理流动中的信息成为人们需要深思的重大课题：一方面，要合理界定数据产权，避免窃密或侵权；另一方面，使必要的技术进步与

信息扩散服务于人类的进步。信息革命加大了发达国家与落后国家之间、发达地区与落后地区之间的“数字鸿沟”，加剧了不平等的产生几率，增加了社会的不稳定因素。

再次，互联网的普及使相对弱势文化获得平等传播渠道的同时，却无法避免强势文化“大量涌入”， 滋生不公平竞争。西方发达国家在网络空间里占有传播优势，例如，英语作为世界语言的普及性强、发达国家借助其主导的全球化进程，在世界范围内大量生产和传播强势文明。

最后，亟需规范网络空间行为。例如，因为全球金融信息联动，部分掌握了全球金融网络的国家或其他行为体可以操动一方经济命脉，可能导致该区域或世界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就是恐怖主义隐身的“港湾”，通过渗透社交网络或是借助黑客活动，恐怖组织传递信息、招募成员、筹集资金、扩张实力、危机社会的稳定[2]。

在大数据时代对网络安全的方方面面进行治理，内容庞杂、困难前所未有、难度巨大。在一些重要的国际论坛或组织平台上，主要国家之间围绕网络安全问题与治理开展了不少对话，试图共同商议，有针对性地解决这些难题，例如 2015 年 G20 峰会公报围绕网络安全治理问题就有所论述[3]，将 G20 公报中的相关内容总结起来，所谓该领域的治理，无非是指网络空间的物理介质和其中流动数据的治理，而治理的目标是实现国家安全、社会稳定与经济繁荣。

二、网络安全治理的议题领域

结合国际上诸多的官方讨论和学术研究，将网络空间安全治理进行梳理和总结，大概分为以下几个治理领域。当然，很难在各领域之间进行明晰的划分，彼此之间存在着诸多交叉。领域一是治理网络“物理疆界”，即网络基础设施管理；领域二是治理网络空间里流动的大数据；领域三是网络内容治理与文化传播；领域四是网络空间内的行为治理，主要涉及治理借助网络平台的跨国网络犯罪、恐怖主义与规范金融制裁等行为。

（一）网络基础设施安全治理

网络基础设施的安全是网络安全的物质基础，因此网络基础设施的重要性受到世界各国的重视，例如 2014 年 1 月 10 日，俄罗斯通过了《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，在谈网络空间治理规则的时候，必须首先重视在该层面上塑造合理的治理规则，确保关键网络基础设施的安全。这种安全主要表现在 CPU、操作系统和网络三个技术层面。[4] 在这三个层面上实现技术自主，是实现物理层面的国家网络安全之必经之路。通过“市场换技术”、合资和引进，一些电信企业已经逐步实现了交换机等联网设备的自主研发。在自主 CPU 和操作系统的道路上，中国电科等大企业也在做出努力。

此外，落实网络基础设施的管理，避不开借助规范清晰界定网络的“物理疆域”。要实现物理疆域的有效与合法治理，须在互联网之“根”的管理中实现治理的合法性。合法性的基础是共有、共治。然而，现实的治理状态并没有那么乐观。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[5]长期未实现全球共同监管，即使，ICANN 私有化也并非是移交联合国，而是交由“全球利益攸关者”。

交由“利益攸关者管理”，意味着松散化治理和寡头垄断。这种松散化治理的结果必然是享有技术和管理经验优势的国家或者行为体将会继续垄断 ICANN 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性。基础性的界定做不好，更难以塑造治理规范，进而确保监管电力、交通、银行等关键基础设施的安全。

再从规范层面看，治理中也相应地会遇到的一些争议点和难点。网络空间的运行逻辑与现实世界不同。主权国家的地理边界并非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。由于互联网已经成为当今世界的主要信息传播渠道，国家行为体很可能因为愈加高度依赖互联网而受到巨大损害。如果许多核心领域内的网络基础设施暴露于不安全的外部环境，或是受制于人，就很难确保国家的安全。例如，一条光缆线被破坏，可能造成交通瘫痪；又或是操控水电站的网络瘫痪，成千上万的人就可能生活受到影响。因此，避免网络基础设施受到破坏，成为如今时代国家利益的重要所在。

然而，某些大国以此为借口，诉诸网络军事化的趋势依然非常明显。例如 2015 年 2 月 6 日，美国《国家安全战略》中提出，美国国防司令部加强网络能力建设，用网络行动破坏敌人指令、基础设施、武器[6]。为了给网络军事化造势，美国一方面要继续倡议借助互联网继续打击恐怖主义；另一方面，美国积极构想假想敌，指摘其他国家。在一定程度上，政治化解读攻击方并不确定的黑客行为，是为了军事化网络空间找到说辞。政治化解读是通过无限夸大所谓来自中国黑客的攻击行为，将黑客的个人行为等同为国家行为，并认定这些攻击危害

了美国关键的信息基础设施，例如“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”[7]。加之个人层面的黑客攻击，也被美渲染为中国的政府授意，严重扭曲了言论方向，损害了双边关系。要实现网络空间的有效治理，需要避免恶意的政治化行为，避免军事化。网络军事化的趋势一旦升级，极有可能将网络空间推入军备竞赛的漩涡，同时也很难避免网络军备竞赛的“硝烟”漫延到现实世界，带来巨大的损失。

综上，明确网络安全优先事项、保障方向、全面系统保障措施。确保信息与通信技术之使用安全，才能进而确保国家安全。维持网络基础设施安全并不意味着以此为借口扩军备战，而需依赖国际社会的对话、合作和共同治理。在源头上寻求治理合法性，明确与保护“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）治理流动的数据

信息泛指流通在网络空间之内的各类数据。就数据“流动”来说，主要涉及跨国的流动、数据开放、隐私和机密等。所谓的信息或数据安全并不陌生。“棱镜门”无疑给大家提了个醒。通过监控流动中的数据，美国对世界各处各方一览无余。网络信息安全不仅仅涉及个人隐私，而且涉及到国家安全，为各国所重视。一国的国防安全和经济安全都与数据安全息息相关。

首先，从军事国防安全来看，数据的疆界并不清晰，难以有效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带来互信缺失，战略行为失范，甚至逐步走向网络空间的“军事化”，最终致

使系统陷入战略不稳定。比较典型的案例就是“棱镜计划”，其前身是 911 后美国为打击恐怖分子所采取的监听计划。通过秘密地“政治化”和“军事化”，局部性的监听逐步演化为监听内外、无所不知的棱镜计划。根据已披露信息，美国国安局监控了中国、法国、德国、英国、西班牙和墨西哥、巴西。加之苹果公司参与其中，不少使用苹果手机的国家决策层人士也人人自危。棱镜计划给人民提了个醒，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守。“棱镜门”折射了美国将信息安全“军事化”的图谋。该事件后，美国不仅没有向受害国家道歉，而是进一步替“军事化”找到借口，转移视线。例如，美国想方设法在网络空间的视角下，大加渲染中国威胁论。美国带有明显“政治化”的导向地解读美国遭受的黑客袭击，常常是模糊事实，从而以此为契机加强网络军事能力建设的步伐，最终会妨碍双边或多边关系的健康发展。因此，有必要在全球层面塑造顶层设计、塑造共识性规范，在全球范围内探讨数据流动的合理管辖范围，尊重各国的国防与军事安全，避免部分国家的过度军事化行为。

其次，从个人隐私层面看，行走在网络空间的个人，很难确保个体的信息安全。例如，今年 2 月 Twitter 的密码恢复系统故障，可能导致了 1 万网名的信息泄漏。如果没有相应的治理规范和应对措施，类似 Twiter 泄漏用户信息的事件很难得到有效处理，用户的信息安全无法得到足够的尊重与保障。再如，英国宽带服务提供商 TalkTalk 受到攻击，泄漏了约 400 多万用户的隐私数据。不仅仅包括姓名、家庭或工作地址、电子邮箱和账号等常规数据，甚至用户的信用卡账等数据都被严重泄漏。多次遭受攻击后，即使 TalkTalk 已采取预警措施，攻击后给用户造成的损失依然巨大。此外，美国医疗保险公司 Anthem

受到网络攻击，大量用户的私人信息被曝光，这些信息包括用户姓名、出生日期、ID、社保等。此类事情繁不胜数。

再次，经济层面的信息安全治理包括了非常丰富的内容，例如商业机密（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巨大，因此治理这些领域内的网络安全问题非常紧迫。治理经济数据的流动，需要关注信息产业治理，包括完善行业标准、贸易投资规则等。在过去的两年内，不少著名的 500 强企业都曾遭受黑客袭击。这里面甚至包括索尼和苹果等著名的电子产业公司，还包括一些金融巨头，例如摩根大通。这些企业深受数据泄漏之苦，不仅带来的经济损失惨重，波及的范围也非常广。就摩根大通银行 2014 年受到攻击，影响波及 1/4 的美国人口，泄漏了 7600 万家庭和 700 万小企业的数据。包括银行信息在内的个人数据被全部窃走，有碍正当的商业竞争。

当个人和企业深受信息泄露之苦，在国际上却没有相应的规则、规范和法律予以治理与规范。如果没有足够的安全意识、特别是完备的法律体系与国际规范、以及防御技术，行走于网络空间里的个人与企业几乎如同“透明人”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，一方面建立全球顶层设计，另一方面建立针对性措施，如此才能有效落实数据安全的保护、问责与惩罚。如果没有完备的治理规范，这个领域内的“责任人”必定缺位。随着信息通讯手段在经济领域内更为广泛的运用（例如大量的电子商务），数据安全监管不足的危害和带来的损失将以难以估量的速度跃升。

最后，在发展层面，通过数据流动造福人类发展，要防止地区不平衡，即“数字鸿沟”现象的出现。在互联网时代，保护知识产权要有一个合理的限度。在强调保护知识产权的同时，也需要避免数据资源分配不均带来的区域不均衡发展，借助合法的技术与商业数据、数据产业促进经济增长。以美国为代表的发达国家在高技术领域占据优势地位，苛刻地强调知识产权保护，制造高技术产品贸易壁垒，妨碍了世界经济一体化和人类共同繁荣。先进技术和产品的扩散受阻，在一定程度上阻碍发展中国家和人民共享人类科技进步的机会，阻碍了人类社会的总体进步。因此，治理的规则也应该避免“数字鸿沟”的加深，兼顾世界各国的发展权。

（三）网络文化空间与内容治理

互联网时代对各国的文化传播带来新机遇的同时，也有挑战。各国越来越将文化视作国家发展的重要战略资源。强势文明对弱势文明的“蚕食”历史上比比皆是。互联网传播速度更快，范围更广，加剧了强势文化对弱势文化的不对称竞争强度，网络信息霸权和文化帝国主义[8]给人类社会带来了前所未有的威胁，因此产生了相应的文化安全问题[9]。面对强势文明的挑战，各国捍卫“文化主权”是一方面，不过分封闭，以开放和自信的态度，通过文化传播与交流，增强文化软实力也是同等重要。在拓宽视野、了解与吸收丰富的世界文明视野之际，还需要发掘民族文化的宝库，向世界传播我们先进的文明。以我国的文化传播为例，通过讲中国故事，使中国文化走出去，增强文化自信。

此外，围绕互联网内容治理的争论很多。有人认为，网络空间里的内容应该完全自由流动，不受任何限制；但如果暴力、色情、谣言

等内容，一旦以网络空间为介质，大肆传播，极有可能威胁到现实社会的安全与稳定。网络文化空间需要有包容性的发展理念，也要有针对性的治理规范。确保文化创新、文化包容与文化传播是保持网络文化空间活力的重要途径。而缓解恶性的网络舆情，维持社会稳定，又是确保网络文化秩序合法有序的必要保障。如果引导恰当，保护和规范互联网言论，网络文化空间可以大大推动文化产业的发展，带来巨大的现实利好；可以以网络空间为媒，建立其民间与政府的良性对话机制，提高国家治国理政的能力；可以反映民情，有效打击腐败等违法犯罪行为等等。在完善内容领域治理规范的时候，可以结合实际情况，从多元化利益相关者的角度考虑问题，鼓励引导相关互联网企业和网民参与进来，让它们在规范自身行为的同时，勇于承担更多的社会责任，参与到治理活动中来。

（四）网络行为治理

谈到网络空间里的行为治理，就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对传统意义上个人与个人、个人与国家、国家与国家的交往与互动方式具有重塑作用。网络环境的重塑作用主要表现为以下几点：一是网络空间没有地理意义上的地缘辖制，不受现实世界中实力投放的“射程”限制；二是网络空间中的行为体具有力量的不对称性，即使作为个体的人（例如网络黑客、网络恐怖主义者）都有能力发动针对例如国家等更大行为体的袭击；三是随着网络技术的突飞猛进，传统意义上对弱国、强国、中等国家的分类方法似乎不再那么适用。此外，网络空间还具有开放性、交互性、虚拟性、分散性等独特的环境属性。

其中，与虚拟性相伴而生的信息“不对称性”，成为事前预警和事后治理网络行为的桎梏。所谓信息“不对称”描述的是无法确认攻击源、无法预知攻击时间和攻击涉及对象的一种状态。在计算机终端背后可能坐着一位恐怖分子，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。这种新形式的恐怖主义之危害常常超过以往任何形式的恐怖行为[10]。信息“不对称性”增加了网络犯罪行为的治理难度。

网络行为治理问题主要涉及借助网空间实施的跨国网络犯罪、恐怖主义、非适度的金融制裁等。对这些行为进行打击、惩罚、规范或者治理，同样亟需塑造成熟的国际规则和规范。如果对此类行为不予以有效治理，不仅仅会造成网络空间内的混乱，还会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，例如美国在 2001 年（911 之后），就增加相应开支，加大打击网络恐怖主义力度。还有大国之间建立信息（情报）共享机制，合作打击恐怖主义行为。在上合组织的框架下，“规定了各方应当根据国内法原则，通过立法等措施，监控金融交易，防范和打击恐怖主义融资活动”。[11]由于恐怖主义的招募和融资行为往往是通过网络进行的，打击这些行为，信息共享和合作网络监管成为必须之策。

在合作治理网络空间行为方面，不少国家和地区纷纷建立起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”，旨在打击网络行为犯罪，保护企业与民众免受网络犯罪侵害。2013 年，《欧盟网络安全战略》：建议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全面收集和分析大数据产生依赖。网络空间治理依赖大数据，却也不得不面对大数据之数据量庞大、时效性极快、内容非常复杂的问题。这就需要突破数据瓶颈，对复杂且看似无规律的大数据进行有效整理与分析。使用超越原始 CPU 处理速度和非常规的数据处理方式，有效整合大数据，在庞杂无章的大数据中寻得“数据中的模式”[12]，指导制定现实对策。一些诸如相关性分析的手段，可以被用来支持大数据的分析。[13]最后，在强调分享数据、利用数据、共同治理的同时，还需要规范大数据的运用。这就需要配套的法律规范，对大数据收集与利用的边界予以明确界定，将之限定在合理、合法的范围之内。

网络的连通性使一些现实的战略行动以更强的力度得以实现。由于网络空间介入战略领域尚且是新现象，但其打击力度、“杀伤性”或“破坏性”极大，因此亟需有效手段予以监管。例如通过金融制裁[14]的巨大威力，威慑或“惩罚”他国，制造战略压力。2012 年，在美国施压下，世界各国金融机构赖以进行金融交易的 SWIFT 发出禁令，禁止伊朗使用 SWIFT 进行石油交易、发展资金、技术与设备。随后，紧随美国，欧盟也向伊朗“关门”。如此，受制裁的伊朗银行与实体行业统统无法利用 SWIFT 网络进行交易。石油生产与出口受阻，无疑将伊朗经济拖入寒冬。伊朗货币里亚尔大幅贬值。一时间，伊朗国内物价上涨、通货膨胀率极高与失业率大幅提高。由此带来重重的社会问题，伊朗国内局势一度不稳定。由此，我们看到，借助网络实现金融威力之大，超乎前人之想象，但也带来一些行为的合理性边界的认定

问题。如果没有有效与公正的治理规范的介入，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

网络空间作为一个崭新的战略增长点和国家互动领域，治理规范尚不健全。一方面，这与网络空间作为非传统安全的典型领域，具有与现实空间不同的互动逻辑，治理起来具有巨大的不确定性和复杂性。另一方面，这一领域新近才进入人们的生活，在国际和国内层面，都还没有能够形成成熟的法律和规范体系，应对各国所面临的新挑战。在这种客观状况下，治理法规不健全，导致了治理活动中存在大量的“灰色地带”。该界定的概念、权利和义务主体与客体，仍未理清。此外，谁在治理规范的塑造过程中占有先机，谁将占据设定制度议程和解释制度条款的优势权力。换句话说，由于技术优势或者其他客观优势，哪个国家或其他行为体在网络空间治理的规范塑造过程中抢占了先机，它就拥有了设置议程的“先行者”权力，可能将自身利益“嵌入”国际制度与规范当中，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参与治理的过程中，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，进而努力营造公平、有序的治理。这三种权力相互联系，共同作用，影响到网络空间的真实博弈。

首先，技术性权力是一种基础性权力，具有助推剂的作用，占据技术领先地位确保了其他两类权力的优势。其次，制度性权力一方面是技术领先的制度表现形式，另一方面又是奠定未来网络空间内基本权力分配格局的基本规制性力量。最后，网络空间的运行秩序和规范

并非定型的，也不是一成不变的，而是具有解释空间的，这就是解释性权力。解释性权力是其他两种权力的“压仓石”，避免偏颇，维持中性的解释话语，能够奠定治理的合法性；解释话语被强权控制则会将整个治理秩序推向非中性的歧途。

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在根本上依赖的是技术进步。正如俄罗斯决心要“决战”信息化，普京强调信息资源和信息基础设施已成为争夺世界领先地位的舞台，未来的政治和经济均取决于信息资源。技术型权力指的正是国家以网络技术为支撑的权力，而网络技术的核心是信息与知识等“软化”的权力[15]。技术领域中往往存在“马太效应”，所以，强者越强，弱者越弱。强者可以利用高技术门槛，把其他国家挡在门外，进一步扩大优势。一方面，继续保持技术领先；另一方面，也把这种领先拓展到更广阔的领域。发达国家在尖端互联网技术领域保持领军地位，如果关键性产品的源代码不开放，数据安全就难以监管。再者，主要的软件供应商（例如微软）主要来自美国，没有实现软件自给，就难以确保数据安全。而目前的不管是硬件还是软件的自给之路又愈发复杂。通过合资、引进和“市场换技术”[16]，国内技术研发逐步实现自主。然而，又该如何处理国内技术研发和国际合作的关系？是否可以单纯依赖企业和市场行为，承担起维护国家网络安全的重任？这些都是悬而未解的问题。

技术上比较发达的国家，往往在对外交往和国际标准、规则制定中处于优势地位。制度性权力就是以技术性权力为基础的这样一种权力表现，当然后者不一定是前者的必然条件。这种制度性权力尤其指在一个领域规范尚且不健全的初创时期，各种建制并不完善，由于各

种客观原因巧妙利用这种“制度中空”的机会，国家或者其他行为体积极谋求“制度先行权”、相对权力优势、主导性话语权。通过掌握议程设置，进一步塑造治理规范的导向，进而将自身利益嵌入其中。之所以说制度性权力的主要表现方式为主导议程设置，主要原因是每个国家和行为体都有自己心目中的轻重缓急，对不同的议题有不同的偏好。谁掌握了制度性权力，谁就能把自己的议题偏好放置于组织的议程之上，并以此作为指定行为规范的依据。是否能够将自己感兴趣的议题和有利的规范，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”[17]。只有增强自身的治理能力建设，才能够在国际建制中增强竞争力。例如在进行全球对话，涉及网络安全标准方面，发达国家显然步子走得更快。美国商务部下设美国国家信息和技术研究所(National Institute of Standards and Technology)[18]，在标准化方面作用最为显著，在物理、技术和管理等层面为美国制定信息安全标准。而欧洲在欧盟的框架下，也设有欧洲网络信息安全局（European Network and Information Security Agency）[19]，致力于建立欧洲网络和信息安全规则。只有加强网络安全治理的顶层设计，并辅以完善的标准化体系，才能在国际对话、制定和塑造规则与制度层面，增强竞争力。

在网络安全的治理安排中塑造规范，也是通过掌握制度性权力，影响其他国家或别的行为体。为了避免其中的恶性博弈，我们坚持要

将网络安全治理规范放在联合国框架之下，正如 2015 年 G20 峰会公报中指出的“我们还注意到联合国在这一背景之下所制定之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国际安全形势之下所制定的电信与信息领域 2015 年报告，遵守其肯定国际法、特别是联合国宪章应适用于信息与通信技术使用及承诺范围内的国家行为这一观点。全部国家都应遵守联合国在 A/C.1/70/L.45 中提出的各国须在信息与通信技术使用过程中承担相关责任的决议。我们致力于协助保障整体环境，旨在参与各方皆能够享受到由信息与通信技术安全使用所带来的收益。”[20]

国家及其他行为体在网络空间中交往与互动，主要任务之一就是传播和推行其崇尚的理解方式、价值观和规范。这就涉及一种叫做“解释性权力”的权力表现方式，“取决于深层次的心理、文化和观念结构”[21]。这种“国家软实力”的表现方式，更为隐蔽，主要通过解释、说明和说服等途径发挥作用。当在全球范围内，尚未塑造完成具有权威性的治理规范之际，抢占解释先机，主导治理规范的解释路径，具有更为显著的重要性。在一些核心概念和治理理念的塑造过程中，例如“全球公域”（Global Commons）[22]，美国一再设法主导解释口径。提及极地、海洋、太空和网络等领域的“公域性质”，有助于扩展势力范围，分一杯羹；而当某些概念开始辖制或妨碍自身利益的时候，也会毫不犹豫的摆脱旧概念或者创制新概念（作为倡导海洋共同治理的国家，美国却没有批准《联合国海洋法公约》，没有将自身行为置于公约的规制之下）。在治理网络空间中流动的数据和网络空间里的行为时，解释性权力非常重要。在治理网络内容和借助网络渠道传播文化方面，掌握解释性权力的重要性尤为突出。例如树立积极的社交

媒体观，用正能量解释事物与现象，避免犯罪思想、恐怖主义等行为萌生于网络空间。

结　语

网络空间治理的核心问题包括由谁治理、治理什么、如何实现公平有的治理等。其中，就治理什么来说，网络安全治理的议题领域包括网络基础设施、流动中的数据、网络内容与文化和诸多网络行为等。本文梳理了这些议题领域，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，又需要注意提升国家参与网络空间治理的能力，有三种权力会影响到国家参与网络安全治理的能力，即技术性权力、解释性权力和制度性权力三种权力 23 上的博弈。这三种权力相互联系，共同作用。

在强调塑造治理规则和权力博弈的同时，各国都不能忘记一点，治理网络安全必须重视合作，面对网络安全隐患，没有一个国家可以独善其身。例如，打击窃取数据，维护数据安全不是一个国家或一个行为体之力所能及。地下信息黑市上，从数据的窃取，到数据的买卖、发包和被利用，都形成了长长的产业链而且攻击方可能来自第二、第三国，无法监管和有效防御。打击和治理这种行为，需要各国共同商讨。小到小的互动游戏平台，再到 Twitter 类的社交平台，更大到跨越许多国家的金融机构，存在大量数据安全隐患，如果没有共同监管和合作主导的治理规范，一些违法行为也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领域的安全，关系到人民生活的稳定，也很可能因为信息泄密，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。但是，目前来说，来没有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，进行合作跨境防御与打击网络犯罪执法。加之网络恐怖活动防不胜防，很难有效治理，且目前的技术手段非常有限，治理起来非常困难。

总之，网络安全治理合作大势所趋。归总网络基础设施、流动中的数据、网络内容与文化和诸多种类的网络行为等各大领域内的治理宗旨或目标，无非落在三个方面。一是通过治理确保国家安全（谨慎网络军事化趋势、避免陷入网络战漩涡）；二是社会稳定（反对网络恐怖主义、网络犯罪，确保基础设施安全、个人信息与人身安全）；三是经济繁荣（营造安全网络空间环境，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，符合各国的根本国家利益，亟需合作治理予以达到。

注释

[1]曼纽尔喀斯特著，夏铸九、王志弘等译，《网络社会的崛起》，中国社会科学出版社，2001 年版，第 91 页。

[2]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"》，《中国信息安全》，2014 年第 10 期，第 90-101 页。

[3]http://www.g20.org/hywj/lnG20gb/index.html，登录日期：2016 年 5 月 20 日。[4]苏金树：《网络空间基础设施核心要素的自主之路》，《信息安全研究》，2016 年第 5 期，第 462-466 页。

[5]域名解析系统或曰 DNS（Domain Name System）是互联网运行与管理的中枢，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。

[6]https://www.whitehouse.gov/the-press-office/2015/02/06/fact-sheet-2015-national-security-strategy，登录日期：2016 年 5 月 18 日。

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

[8]蔡文之：《网络：21 世纪的权力与挑战》，上海人民出版社，2007 年版，第 42 页。

[9]哈拉尔德·米勒著：《文化共存—对塞缪尔·亨廷顿"文明冲突论"的批判》，郦红译，新华出版社，1998 年版，第 18 页。

[10] Walter Laqueur, Postmodern Terrorism, *Foreign Affairs*, September/October, 1996, p.35.

[11]http://legal.people.com.cn/n/2014/1230/c188502-26297011.html，登录日期：2016 年 5 月 10 日。

[12] Pang-Ning Tan 等著，《数据挖掘导论（完整版）》，范明、范宏建译，背景：人民邮电出版社，2006 年班，第 1,5 章。

[13] Kennetch Cukier, Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think About the World," *Foreign Affairs*, Vol.92, No.3, 2013, pp.28-40.

[14]东鸟：《网络战争》，九州出版社，2009 年版，第 121-148 页。

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

[16]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。

[17]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。

[18]http://www.nist.gov/，登录日期：2016 年 5 月 30 日。

[19]https://www.enisa.europa.eu/，登录日期：2016 年 5 月 30 日。

[20]http://www.g20.org/hywj/lnG20gb/index.html，登录日期：2016 年 5 月 20 日。

[21]蔡文之：《网络：21 世纪的权力与挑战》，上海人民出版社，2007 年版，第 5 页。

[22]Abraham M. Denmark, "Managing the Global Commons," *The Washington Quarterly,*Vol. 33, No. 3 (June 2010), pp. 165-182; John Vogler, *The Global Commons:*

Enviromental 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," *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.

[23]任琳:《多维度权力与网络安全治理》,《世界经济与政治》, 2013 年，第 10 期，第 38-57 页。