

网络基础设施有国界,网民有祖国,网络公司有国家属性。网络主权是国家主权在网络环境下的自然延伸

网络主权:一个不容回避的议题



图①:2014年4月23日至24日,全球互联网治理大会在巴西圣保罗文化中心召开。图为会议期间,当地民众举行集会,抗议美国的监听行为,要求建立全球网络新秩序。

图②:2014年3月23日,在美国政府声明放弃对互联网名称与数字地址分配机构(ICANN)监管权后,第四十九届ICANN大会在新加坡召开,探讨未来的互联网治理方案。

人民视觉

版式设计:蔡华伟



②

权威论坛

- 方滨兴(中国工程院院士、北京邮电大学原校长)
- 王 军(中央民族大学马克思主义学院副院长)
- 郎 平(中国社科院世界经济与政治研究所国际政治研究室副主任)
- 俞晓秋(中国信息安全测评中心顾问)
- 汪晓凤(复旦大学美国研究中心博士)

互联网时代,国家主权从领土、领空、领海等领域拓展到“信息边疆”等新领域。全球互联网的互联互通以及网络空间的形成,是各国互联网自身建设与运行的结果。各国加强对本国网络空间的监管既是必然的,也是对保障全球互联网有序稳定运行和全球网络空间治理的一种责任担当。围绕网络主权这一话题,本版连续两期邀请国内权威专家进行解读

郎平:美国学者斯蒂芬·克拉斯纳提出了“相互依赖的主权”概念。越来越多的全球性问题出现,一国政府不可能独立应对,要依靠全球治理。网络主权就具有这样的性质。全球治理意味着要让渡部分主权,这也是国家间利益博弈的主战场。但前提是要肯定网络主权的存在。

一些国家对他国实施大规模网络监控和网络攻击,并通过网络传播干预他国舆论环境,使网络时代的国家安全面临全新挑战。强调网络主权势在必行

俞晓秋:如今,全球范围内的黑客攻击频繁上演,因跨境网络通信监控行为以及一国对他国互联网监管政策指责而引发的国家间矛盾纠纷不断,足见在当前提出并强调网络主权的必要性。网络主权是各国维护自身互联网发展权益以及保护本国互联网不受外部入侵和攻击的最基本的法理依据。迄今为止,国家依然是当今国际体系中最大且最具权威的实体,全球互联网的互联互通以及网络空间的形成,也是通过各国互联网自身建设与运行应用实现的。各国加强对本国网络空间的监管既是必然的,也是对保障全球互联网有序稳定运行和全球网络空间治理的一种责任担当。

汪晓凤:当前,网络空间国际行为规则体系尚未形成,网络资源分配极不平衡,各国网络行为能力存在巨大差异,一些国家滥用技术和资源优势,对其他国家实施大规模网络监控和网络攻击,并通过网络传播干预他国舆论环境,对国际秩序、国家安全和稳定形成重大威胁,强调网络主权原则就有了现实必要性和紧迫性。

其一,网络时代的国家利益已发展出全新的内涵。网络空间的可信、稳定和安全是一国经济社会运行的重要保障,网络数据信息蕴含着重要的经济、政治和军事价值,这些都构成了国家利益的新型要素。确立网络主权是维护网络空间国家利益的基本保障。

其二,网络时代的国家安全面临着全新挑战。防止源于网络空间的安全威胁或通过网络空间发起的攻击影响其它领域的稳定,已成为国家安全的重大关切。由于以互联网为核心的网络空间在设计上的缺失,多数国家应对威胁能力不足,难以有效应对匿名和来源不明的网络攻击。如2007年,爱沙尼亚政府、新闻媒体和金融机构网站遭大规模拒绝服务式攻击,全国网络瘫痪数日。由于攻击源分散在多个国家,难以辨识幕后操纵者,对攻击者的反击更是无从着手。可见,网络安全有赖于对网络空间主权的尊重和保护。

其三,网络空间的和平发展关乎国际社会的共同命运。网络空间面临如何实现公平、和平、安全及可持续发展的问题。由于一些国家极力阻挠,联合国等政府间国际组织无法在制定网络空间国际公共政策方面发挥主导作用,特别是在面临网络资源的不公平分配、网络技术优势的滥用、网络空间的军事化趋势等问题时显得无能为力。在此意义上,没有网络主权也就没有国际网络秩序,确立网络主权,并加强政府间合作,才能形成解决问题的制度基础。

网络主权包括独立权、平等权、自卫权、管辖权四个基本权力。在网络空间,技术的水平决定了主权的维护能力

方滨兴:网络主权具体包括四个基本权力。第一是独立权,指本国的网络可以独立运行,无需受制于他国的权力。从管理手段上,由于根域名解析体制的缘故,各国的网络不能独立存在,目前还受制于美国。虽然美国国家电信和

信息局已于2014年3月14日宣布将放弃对互联网名称与数字地址分配机构的监管权,称将会把监管职能移交给全球“多方利益相关者”,不可以由“主权国家”或者“政府间机构”接手,但只要美国的公司在“多边利益相关者”模式中占据优势,美国政府就可以天经地义地用美国国内法去管理该公司。

事实上,从技术手段上很容易实现网络的独立权,那就是各国建设自己的根域名系统,并相互之间交换各自根域名的地址;美国所托付的国际组织只负责通用的域名(如.com、.tv等),然后将这些解析服务器的地址共享。

第二是平等权,指网络之间的互联互通是以平等协商的方式进行,不受管辖制约的权力。首先,平等权要确保各国的网络之间可以平等地进行互联互通,而非单方受惠的建设模式。目前互联网国际接入仍受制于大的国际运营商,如美国斯普林特公司就凭借其在国际上的重要地位,致使互联网规模小的国家在接入国际互联网时受到不平等待遇。其次,平等权要确保各国对网络系统具有平等的管理权,保证一国对本国互联网的管理不会伤及其他国家。现有的互联网相互依赖性强,互联网强国国家所制定的政策可能波及接受其服务的国家。再次,平等权还包括国家在其领范围内的豁免权。

第三是自卫权,指主权国家对本国网络的任何攻击都应具有自我保护的能力。首先,自卫权要确保网络系统处于自我保护之下,而不是依赖于他国,不应该有因境外系统被攻击而致使本国网络瘫痪的情况发生。针对根域名系统被攻击、重定向导致分布式拒绝服务攻击、境外言论导致一国社会不稳定等事件,应有积极的自我保护措施。其次,自卫权要确保本国具备设置网络疆界、隔离境外攻击、抵抗与反击网络攻击的能力。

第四是管辖权,指主权国家对本国的网络可以实施管理的权力,包括国家在领范围内的立法管辖权、司法管辖权和行政管辖权,如准入许可、停止服务等。首先,管辖权要确保拥有对本国网络系统的管理能力。主权国家能实施本国网络准入机制,包括非授权用户不允许接入到网络中,并拥有发现非授权接入网络的能力。对于不服从管理的业务应该具有停止其服务的权力。其次,管辖权要研究类似于国际上的河床与河水的关系。一个国家对于河床拥有主权,尽管河水来自上游国家,但上游国家不能输出被污染的河水。如果上游国家输出了被污染的河水,输入国要有自洁能力,而且对不打算自洁的输出国要有相应的应对措施。

郎平:套用德国军事理论家克劳塞维茨“关键地形”的概念,网络主权的关键地形应该包括:数据中心、网络服务商、海底光缆、国际标准制定机构、基本输入输出系统、供应链、网络劳动力、技术创新等方面。这些领域可以被认为是网络主权维护中的关键领域。但是,在网络空间,技术的水平决定了主权的维护能力,很明显,美国在关键地形上已经占据绝对优势。

目前尚无将网络空间置于主权管辖下的国际公约,国家在维护网络主权时难免遭遇难题。维护网络主权任重道远

王军:在网络空间下,挑战一国主权的主体和内容是多种多样的。从主体上看,既可以

是国家行为体,也可以是国际组织、社会组织和个人等非国家行为体。典型的方式有以下几种:

第一,一国的互联网管制可能侵蚀他国的主权,即当事人的互联网侵害行为发生在一个主权国家领域,但其行为引起的损害结果却发生在另一个国家。此时出现了行为发生地国家的管辖权与结果发生地国家管辖权的冲突。结果发生地国对该互联网行为的调整和规范将不可避免地对该行为发生地国产生影响。如法国法律规定,所有针对法国公民的广告必须使用法语。相应地,所有针对法国公民出售货物和提供服务的互联网也必须使用法语。因此,如果一个在美国登记的互联网网站使用英语对法国公民发布广告,将会被法国政府起诉,即使该网站是符合美国法律规定的。

第二,外部国家干涉他国主权的言论通过互联网发表和传播,或外部国家通过互联网来干涉他国内政。譬如美国等国家通过互联网和其他途径对一些国家展开“颜色革命”,就是典型的对他国主权的挑战。

第三,一国内分裂国家的力量通过互联网招募成员、发动宣传、进行信息沟通和政治动员等,挑战了该国的主权和领土完整。

第四,挑战国家主权的思潮和组织在网络空间颇为活跃。不管是跨国公司还是非政府组织,通过互联网展示其主张,推进其业务,往往都与国家主权原则存在直接或潜在的冲突。

此外,互联网生活本身也可以在一定程度上削弱人们的主权认同。作为一种新的文化形态,互联网淡化了人们对本民族文化和本国文化的归属感和认同感,国家、民族以及对国家和民族传统的忠诚,在一定程度上受到虚拟世界的侵蚀,并因此对国家的内部主权构成潜在侵蚀。

汪晓凤:迄今为止,国际社会还没有形成关于将网络空间置于主管辖下的国际公约,网络主权的复杂结构和丰富内涵决定了国家在维护网络主权时面临各种难题。

难题之一是网络主权国际共识的达成。一些国家宣称拥有网络主权,但多数是一种政治宣示,并未从法律上对网络主权进行确认。难题之二是网络主权声索范围的确定。确定网络主权首先要对网络空间进行边界划分,国家对领土主权的声索可以通过边界线、领海宽度和领空高度等标准来确定清晰的管辖范围,但网络空间缺乏类似技术上可行、权益上清晰、法律上明确、国际上承认的划界标准。难题之三是网络主权损害行为的辨识。一方面,网络侵害行为具有欺骗性,由于匿名和开放的设计理念,网络身份识别和网络行为溯源难以进行;另一方面,网络侵害结果具有隐蔽性,一些重大损

害可能很长时间都不会被发现。难题之四是网络主权维护方式的选择。传统上,国家可以运用外交、军事和经济等各种国家资源维护本国的国家主权,还可以诉诸国际法、国际组织等国际机制寻求支持。而当网络主权受到攻击,诸如网络基础设施受到攻击、网络应用系统被入侵、网络数据信息被窃取时,可供选择的资源和应对手段却非常有限。

网络空间开放性的技术架构、虚拟化的利益表现、多元化的行为主体,构成了网络主权的复杂结构和丰富的内涵。网络主权的确定和维护任重道远,作为一个网络大国、网络空间发展的重要受益者和坚定支持者,中国应在其中承担大国责任。

俞晓秋:美欧信息化发达国家是互联网的源发地和先行者,无论在技术、规制、标准和法律等方面都占据着先发优势。在互联网与网络空间领域维护国家主权的复杂性在于,网络通信技术的特性和对互联网的依赖性决定了确保本国网络空间与国际网络空间的互联互通、信息流动,才能使互联网效益达到最大化。若将内外网络隔绝或自搞一套,就可能成为一个“信息孤岛”。

郎平:网络主权的维护面临与其他疆域不同的难题。首先,政府很难控制非法信息的跨国传递。网站可以通过在全球范围内不断变换服务器和域名的方式发布信息,利用不同国家的互联网管理规定的差异,和政府玩“打地鼠”的游戏,维基解密事件就是典型。政府不能控制信息的扩散,能做到的只是对相关公司的资产、人员实施控制或施加压力。

其次,信息的传递“通道”难以管理。网络空间的信息传递通道由私有企业控制,无论是民用信息还是军事信息的传递,都需要依赖这些企业所掌控的人口。政府要保障和维护关键设施的网络安全,就必须和相关企业配合,承担共同的责任。

再次,维护主权的对象难以界定。当面对难以追踪来源的网络攻击,如何判断攻击的来源究竟是个人还是国家,抑或是国家的代理人?网络攻击在何种情况下被界定为战争行为?应该找谁去负责?这些问题有待国家间协商和培养共识。

总的来看,网络主权概念的提出意味着国家行使主权去维护网络安全,但网络空间的特殊性决定了政府角色的有限。政府决策者应关注如何在维护网络主权的同时保证互联网行业的健康发展,并且在维护网络主权与行业发展前景之间寻求恰当的平衡。

(本报记者王远采访整理,复旦大学美国研究中心副主任信强也对本文做出贡献)