DOI 10.15302/J-SSCAE-2016.06.002

网络主权保障问题研究

邹鹏[1]，何骏[1]，邹红霞[1]，刘韵洁[2]

（1. 中国人民解放军装备学院，北京 101416；2. 中国联合网络通信股份有限公司，北京 100089）

摘要：随着网络空间承载国家公共和私人利益的日益广泛，网络主权及其保障问题已引起了国际社会的高度重视。本文结合当前我国网络主权的现状，从网络独立权、网络平等权、网络自卫权和网络管辖权的角度分析了我国网络主权保障目前应当关注的主要问题，并给出了相应的对策建议，力求推动网络主权观的确立，增强我国在国际网络空间治理规则制定方面的话语权，提升维护国家网络空间安全利益的能力。

关键词：网络主权；网络独立权；网络平等权；网络自卫权；网络管辖权；网络边防

中图分类号： C911　　**文献标识码：**A

Research on the Issue of a Cyber Sovereignty Guarantee

Zou Peng[1], He Jun[1], Zou Hongxia[1], Liu Yunjie[2]

(1. Academy of Equipment of PLA, Beijing 101416, China; 2. China United Network Communications Limited, Beijing 100089, China)

Abstract: As cyberspace carries more and more national, public, and private interests, the issue of a cyber sovereignty guarantee has attracted great attention around the world. From the perspective of China's cyber sovereignty situation, this paper analyzes the main problems related to China's cyber sovereignty guarantee, including the implications of the cyber rights of independence, equality, self-defense, and jurisdiction. Corresponding countermeasures and suggestions are also provided. The purpose of this paper is to promote the establishment of cyber sovereignty, enhance China's discourse right on international cyberspace governance rules, and enhance the ability to safeguard national cyberspace security interests.

Key words: cyber sovereignty; cyber right of independence; cyber right of equality; cyber right of self-defense; cyber right of jurisdiction; cyber border defense

一、前言

中国是网络主权的坚定倡导者和有力维护者。自 1994 年接入互联网以来，在短短的 20 多年时间里，我国网络事业取得了高速的发展和长足的进步，但在实践过程中，由于不断面临来自部分网络强权国家在政治、安全和经济上的威胁与挑战，促使我国不断提升有效保障和维护网络主权的战略认识，并逐步形成了比较系统的战略观点，形成了以尊重主权平等原则为核心诉求的全球网络空间治理的新主张[1]。虽然网络主权的内涵和外延还没有一个统一的、国际公认的严格界定，但是随着各国注入网

收稿日期：2016-10-16；**修回日期：**2016-10-22

作者简介：邹鹏，中国人民解放军装备学院，教授，博士生导师，研究方向为网络安全；E-mail: zpeng@nudt.edu.cn

基金项目：中国工程院重大咨询项目“网络空间安全战略研究”(2015-ZD-10)

本刊网址：www.enginsci.cn

络空间的利益及其冲突的增加，网络主权的基本原则已经被国际社会普遍接受，在此背景下，网络主权保障能力成为国家实现有效主权管辖的关键。网络空间主权（简称网络主权）是国家主权在网络空间的延伸和拓展。我国作为新兴的经济和网络大国，与美国为首的西方强国相比，存在网络控制能力的先天劣势，导致我国网络主权的保障能力与国家安全利益需求差距很大，与强国网络对抗水平差距很大。为此，就网络空间涉及的主权问题以及国家有效提升网络主权保障能力的战略举措开展研究，对增强我国在国际网络空间治理规则制定方面的话语权和维护国家网络空间安全利益具有重要的现实意义。本文主要从保障网络独立权、网络平等权、网络自卫权、网络管辖权现实需要的角度提出网络主权当前应关注的问题及应对策略。

二、保障网络独立权

网络独立权面临的主要问题在于根域名解析体系能够不受制于人。现有域名系统（DNS）采取“集中式”管理架构，即网民提出域名解析请求时，在没有缓存的情况下首先提交给最核心的根域名服务器进行解析，然后在根域名的引导下逐级向下进行递归解析。如果根域名服务器出现了问题，将导致整个域名系统出现异常甚至崩溃，使得全球网民无法正常访问互联网。

全球有 13 台根服务器，10 台在美国，2 台在欧洲，1 台在日本，这其中由美国威瑞信公司运营的 1 台根服务器为主服务器，其他 12 台是从服务器，受制于主服务器。为了提高域名解析的效率和可靠性，目前包括中国在内的多个国家还建立了上百台根服务器镜像，但这些镜像也完全受制于根服务器。可见，全球互联网核心枢纽和关键基础资源已被美国控制，在非常时期，其他国家境内的互联网可被美国单方面断网或瘫痪，这成就了美国控制互联网“开关”的新型战略威慑能力。

应对根域名体系对我国网络独立权带来的风险，核心的解决方法是提出“去中心化”的技术解决方案，构建国家自治根域名体系，形成国家间根域名解析联盟[2]，简称“互联根”方案，其核心思想是联合关注网络独立权的国家构建一个联盟。盟员国各自构建自己国家的根域名服务器，称为国家“互联根”，用于取代根域名服务器承担首次解析的功能，使得所有域名解析请求不再是先指向根域名服务器，而是先指向位于本国的“互联根”，在没有可解析信息时再递归到根域名服务器进行查询。国家“互联根”之间是平等的，相互交换自身的顶级域名地址（如中国的 .cn、俄罗斯的 .ru）。国家“互联根”可以为其他盟员国代理域名解析服务。

“互联根”方案具有开放性、平等性、自主性、兼容性的特点。任何国家可以自由加入或退出根联盟系统，“互联根”的解析服务向全球用户开放，人们可以自主决定选择哪个根域名服务器进行首次解析。各个“互联根”的地位平等，相互不受控制，国家根之间的数据可对等交换。国家“互联根”及所承担的解析服务受本国域名管理机构的管理。“互联根”可与当前的域名授权管理同时存在，不影响现有体系的运行，愿意选用“互联根”的解析服务器直接指向“互联根”，而希望保持现状的解析服务器仍像过去那样直接指向根域名服务器。从国际上多次的交流效果来看，“互联根”方案受到俄罗斯、古巴以及一些拉美国家的认同和赞许。

三、保障网络平等权

网络平等权面临的主要问题是目前的域名体系是各国和互联网名称与数字地址分配机构（ICANN）签约所形成，ICANN 是甲方（租方），其他国是乙方（承租方）。ICANN 是注册在美国的非盈利企业，受美国商务部的管辖。目前，其他国家如果要更改一个顶级域名的 IP，必须通过 ICANN 向美国商务部备案。因此，中国的国家和地区顶级域名（.cn）仍然是中国向美国的承诺约定，并无平等可言。

为保障各国在互联网方面的平等地位，让互联网资源还原其公共属性，利于建立全球共治的互联秩序，需要推动 ICANN 的国际化。应由联合国发挥主导作用，推动互联网空间共享共治，各国平等参与互联网治理，构建解决网络重大冲突的国际仲裁组织。ICANN 的国际化能够使各国的网络以平等的方式实现互联互通，改变少数国家拥有占绝对优势的网络资源并利用这种优势制造网络权利不平等的局面，保障在网络资源分配不均情况下的网络平等权。2016 年 10 月 1 日，美国政府已宣布放弃

互联网资源管理权，移交给多利益攸关方，但从本质上并没有改变互联网资源分配不平等的现象。

四、保障网络自卫权

网络自卫权面临的主要问题是：从国际上看，目前缺少网络空间攻击与自卫的相关法律依据，难以解决网络攻击的归责问题。《联合国宪章》对主权国家自卫权的行使前提、对象、时间、方式、限度等进行了明确的限定，但都是基于以陆、海、空、天等有形的、物理空间为作战空间的传统战争行为而制定的，仅适用于可区分攻击源头的敌对武装行动，而对于网络战这类在无形的、虚拟的网络空间发生的战争行为，由于网络攻击可以有效地隐匿攻击源头，因而可以轻易地嫁祸于人。如果只是简单地将现行法律直接应用于网络空间中，可能使一个国家在没有充足证据的情况下基于怀疑而发起战争，国际法建立起来的禁止滥用武力的堤坝可能崩溃[3]。因此，必须加强国际合作，在联合国主导的框架下，研究并制定适用于网络空间的国际武装冲突法，防止滥用武力以及网络攻击可能触发的全面军事冲突。

我国应尽快部署和开展对网络空间国际武装冲突法的研究。一方面，对西方大国网络战争法的制定动态进行跟踪分析；另一方面对我国制定相关法律规则进行前期研究，待时机成熟时，通过国际合作，制定有利于广大发展中国家的网络战争国际法。对于中国这样的发展中国家，目前的重点是防止网络空间武装冲突而大力开展技术储备和战场环境建设，大力宣扬我国反对网络军备竞赛和通过网络侵犯他国利益行为的立场，为防止个别网络强国利用对其有利的网络战规则干涉他国争取道义支持。

从国内来看，国家网络边界未能有效设防，未能有效防御和反制大规模的网络攻击。对网络疆域的守卫是捍卫网络主权的重要措施之一，我国网络空间缺乏类似于国家边防那样的边界、沿边、口岸等边防设置，网络边防防卫体系和结构力量缺乏，应对网络攻击和对网络攻击实施反击的能力不足，主要表现在技术上网络防御、攻击溯源和攻击反制的方法手段水平不高，缺乏有效威慑的网络防御武器；制度上未能形成部门整合信息情报的共享机制，制约了网络防御能力的发展；体制上缺乏网络防卫的武装防御力量，军队未能参与到捍卫网络空间主权的保障中。目前网络空间军队的职责主要是保护军用的网络，对民用网络基础设施未明确其保卫的职责，这显然与新时期捍卫国家主权、安全和领土完整的军队历史使命不吻合。因此，需要明确在危害国家主权的情况下，军队在保卫国家网络基础设施与重要信息系统方面的责任，加强军民融合的我国网络空间国防力量的建设，构建国家网络边防。

网络边防是指在网络空间保卫国家政治、经济、军事、文化利益所采取的一整套网络防御与攻击反制措施。为有效提升我国网络边防的保障能力，提高应对大规模网络安全突发事件的能力，可以以“国家信息关防”为依托，以军民融合的网络防卫力量为主体，以军队网络战部队为后盾，启动国家网络边防建设工程，构建网络国防体系。这就要求将国家重要网络安全基础设施纳入国家网络国防的建设体系中，并且要以“大国防”观来指导建设新的“网络国防”安全体系[4]，重点是将网络空间防御体系中的各重要网络安全信息系统纳入统一管理、联动协调的运行机制中来，让国家网络边防承担更多的职能角色，包括网络入侵的防范功能、有害信息的过滤功能、跨境电子身份的认证功能、跨境电子商务的海关功能等。

五、保障网络管辖权

网络管辖面临的主要问题是大数据所带来的数据管辖问题，即数据主权问题和信息自由流动所带来的网上信息监控与管理问题，也就是信息主权问题。如果把土地与矿产比作是领土主权管辖的核心资源，那么网络上的“数据”与“信息”就应该是网络主权管辖的核心资源。

数据主权是网络主权的一个子集，是指一个国家对其政权管辖地域范围内个人、企业和相关组织所产生的文字、图片、音视频、代码、程序等全部数据在产生、收集、传输、存储、分析、使用等过程拥有的最高权力，这种权力包括数据所有权和数据管辖权两方面。数据所有权指主权国家对于本国数据排他性占有的权利。数据管辖权是主权国家对

其本国数据享有的管理和利用的权利[5]。数据主权意味着数据即使被传输到云端或远距离服务器上，仍应受其主体控制，而不应被第三方所操纵。当前大数据时代下的国际关系中，数据主权出现的问题主要表现在：产生数据国家所管辖下的企业、机构或个人，拥有数据实际管理权的云服务提供商，以及具有行政和法律管辖权的主权国家三者新的复杂权责关系。由于各国在网络空间的技术水平存在参差不齐的情况，导致现实中出现强国对于弱国数据资源的掠夺，严重侵害到了弱国的主权[6]。尤其是在物联网和云计算技术成熟的条件下，大数据可以随时随地采集，可以跨地区、跨国界存储，可以毫无阻碍地在网络空间传播，使数据管理本身变得异常困难。各利益集团以及主权国家之间对于数据权的争夺变得越来越激烈，数据主权已逐渐引起了各国的重视[7]。

信息主权是指一个国家对其政治管辖地域范围内任何信息的制造、传播和交易活动以及相关的组织和制度拥有的最高权力，包括信息的保护、管理和控制权[8]。信息管辖主要涉及的是对网上信息监控与管理的问题。当前民众诉求多元化，意识形态斗争复杂，通过互联网发动信息战、推动颜色革命、危害国家政权稳固的事件时有发生。国家在网络空间维护信息的主权，实质上是为了构建一个良好、健康的信息传播和资源共享环境。反之，一个充满了垃圾邮件、造谣欺诈、病毒木马的差的网络信息环境，则直接危害信息安全、社会安全，乃至国家的安全。

为有效行使网络管辖权，有力地保障数据主权和信息主权，总体的要求是在法律法规层面积极推进国家层面的网络管辖权范围的立法；在体制机制层面要积极理顺网络监管的机构设置和职能划分，逐步建立网络可信身份管理系统；此外，应注重提高组织机构和广大民众的网络安全和主权保障意识。

具体来说，一是要规范数据的跨境传输、存储与使用，对于跨境数据流动的限制，目前国际上管理的主要趋势是要求在境内建设数据中心和存储数据。俄罗斯、日本和欧盟等相继出台了对数据保护的相关法律法规，我国也应在数据跨境传输、存储与使用上尽快有所作为。二是通过多边和双边谈判，参与跨境数据流动国际合作，构建共同的跨境数据流动规则，降低规则差异带来的风险和成本。坚决反对网络大国利用自身的网络信息技术优势，以强调网络信息自由的名义肆意攫取他国的网络大数据，或对数据、信息资源等实施单边控制，损害其他国家的利益。三是在网络空间实施可信电子身份管理战略，加强舆情监控和内容管理。身份认证是实现网络攻击溯源、履行网络管辖权的基础。通过网络身份统一认证创造安全、可信的网络空间，降低网络诈骗、造谣等犯罪行为以及网络匿名攻击给国家主权带来的危害。出入境管理部门对进入我国的合法境外人员办理临时电子身份证，建立网络关防；海关基于电子身份证履行好网上交易商品的关税征稽等职能，实现网络海关；网络安全部门基于电子身份证和可信网络标识统一规范人员的上网行为管理，筑牢信息关防。

六、结语

本文围绕网络主权四权——网络独立权、网络平等权、网络自卫权和网络管辖权开展网络主权保障所面临的问题和应对策略的分析研究，这一视角瞄准的是当前网络主权保障最迫切和最当务之急的问题，所提出的措施具有比较强的针对性，并力求能够便于进一步的可操作实施。网络主权保障体系的建立是一个全方位、多层次的复杂问题，还需要从长远体系建设的角度进行研究，从法律法规保障、体制机制建设、技术措施发展等多个方面来统筹部署并加强规划。

参考文献

[1] 沈逸. 美国国家网络安全战略[M]. 北京: 时事出版社, 2013.
Shen Y. The US national cybersecurity strategy [M]. Beijing: Current Affairs Press, 2013.

[2] 方滨兴. 从“国家网络主权”谈基于国家联盟的自治根域名解析体系[J]. 信息安全与通信保密, 2014(12):35–38.
Fang B X. Discussion about the resolution system based on autonomy root domain name of national league in view of “national cyber sovereignty” [J]. Information Security and Communications Privacy, 2014(12):35–38.

[3] 崔传桢. 网络空间安全“大国战略”之2015新动向[J]. 信息安全研究, 2015,1(1): 2–8.
Cui C Z. New trends of the main countries cybersecurity strategy in 2015 [J]. Journal of Information Security Research, 2015,1(1): 2–8.

[4] 武成刚. 加快中国“网络国防”建设的战略思考[J]. 国防科技,

2012,33(3):1–4.
Wu C G. The strategic thoughts on accelerating the Chinese cyber defense construction [J]. National Defense Science & Technology, 2012,33(3):1–4.

[5] 杜雁芸. 大数据时代国家数据主权问题研究[J]. 国际观察, 2016(3):1–14.
Du Y Y. National data sovereignty in the big data era [J]. International Review, 2016(3):1–14.

[6] 蔡翠红. 国际关系中的大数据变革及其挑战[J]. 世界经济与政治, 2014(5):124–143.
Cai C H. Big data reformation and challenge in international relations [J]. World Economics and Politics, 2014(5):124–143.

[7] 沈国麟. 大数据时代的数据主权和国家数据战略[J]. 南京社会科学, 2014(6):113–119.
Shen G L. Great state to unite people: Data sovereignty and the national data strategy in a Big Data Era [J]. Nanjing Journal of Social Sciences, 2014(6):113–119.

[8] 牛博文. 信息主权的法律界定探析[J]. 北京邮电大学学报: 社会科学版, 2014,16(4):25–33.
Niu B W. Legal definition of information sovereignty [J]. Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition), 2014,16(4):25–33.