

# 国际网络安全规则创制与政府话语权博弈 ——技术维度的阐释

刘小燕 崔远航

## 摘要

“网络安全”概念，大体被置入技术、犯罪和恐怖主义、军事三大维度或领域内予以讨论，不同维度下的各个利益相关者的权力分配与话语权博弈情况亦有所差别。网络安全领域规则创制中的话语权力（主导权力）的构成，更多体现为权力不对称分布特点。政府话语权的拓展有赖于技术开发与应用。技术开发应用能力，是网络安全领域中各行为主体话语权力的基石，网络技术强国和网络技术弱国在相应技术标准和协议制定上的话语权差异巨大。在网络安全的技术维度上，各国在相应安全标准或协议制定上的权力大小由两个因素决定：历史和技术。政府话语权力博弈集中体现为国际网络技术标准创制竞争。然而，技术性权力仅提供给一国扩张话语权的基础，话语权的强固，仍有赖于一国政府的制度性权力和解释性权力的强化，能否将本国开发的技术标准推向全球、使其成为国际通行标准则为关键。从技术维度阐释国际网络安全规则创制中的国家（政府）制度性话语权力博弈，为本文核心所在。

## 关键词

国际网络安全规则、政府话语权、国家利益

## 作者简介

刘小燕，中国人民大学国家发展与战略研究院研究员。中国人民大学新闻学院教授，新闻与社会发展研究中心研究员。

崔远航（通讯作者），传播学博士，国防大学政治学院讲师。

本文系国家社科基金项目“政府话语权与国际规则之关系研究”成果（项目编号：14BXW022）。

## The Creation of International Cyber Security Rule and Game of Government Discourse- Interpretation of Technical Dimensions

LIU Xiaoyan, CUI Yuanhang

## Abstract

The concept of "cybersecurity" has been generally discussed in three dimensions: technology, crime and terrorism, and military. The distribution of power and discourse among stakeholders varies in different dimensions. At present, the discourse power of all parties are in contention for international rules of cyber security. The discourse power (the leading power) in the "cybersecurity" appears uneven in its distribution. The government expands its discourse power depending on technological development and application. Technology is the most basic and earliest determinant of "cybersecurity", while technology development and application are the cornerstone of the discourse power of all actors in the field of network security. The strong power and weak power in the "cybersecurity" have great differences of discourse power in making relevant security standard or agreement. In the technology of "cybersecurity", the right of making security standard and agreement is determined by two factors: history and technology. The game of the government's discourse power is reflected in the competition for making international internet technological standard. However, technology only provides the basis for the expansion of discourse power. The reinforcement of discourse power still depends on the enhancement of institutional power and interpretative power of a government, among which the key is to transform the nationally developed technology standards to international practices.

## Keywords

international cybersecurity rules, government discourse, national interest

## Authors

LIU Xiaoyan is a research member of the global public foreign affairs research center, the strategic college of state development of Renmin University of China, a professor at the School of Journalism and Communication and a research member of the Journalism and Social Development Research Center of Renmin University of China.

CUI Yuanhang (corresponding author) is a doctor majoring in communication; and a lecturer at College of Political Studies, NDU, PLA, China.

The paper is supported by National Philosophy and Social Science Foundation. (No. 14BXW022)

从国际政治角度而言，网络空间的出现和发展所产生的系列议题并非仅囿于网络，而同样拓宽了传统政治领域的问题视域，并增加了这些问题的复杂性。其中作为典型议题之一的网络安全，在2010年后成为全球范围国际政治和国际法领域关注热点<sup>1</sup>。国内外众多学者围绕网络安全的界定、其对传统国家安全和相应国际规则制定的挑战进行了探索，尤其关注了各国于网络安全领域有共同利益，但仍未形成全

球性的网络安全规则的情况（魏英哲，2016；刘建伟，2013）。

至今网络安全的概念界定仍不清晰（刘杨钺，2015:117-138），诸多学者论述的视角亦有较大差异。学界开始探讨作为网络安全领域主要的利益相关者之一，民族国家政府在其中的角色和作用，但整体而言，较少涉及民族国家政府出于各自利益、在网络安全国际规则制定中博弈情况。考虑到“安全不仅是客观存在的状态，也应被理解为具有主体间性的社会建构产物”（Williams，2003：513），不同民族国家政府对网络安全的认知和判断也直接影响了其国内网络安全策略话语表述；而在相应国际规则创制中，尽管多个国家政府、国际组织、跨国互联网公司等都意识到国际规则创制的必要性，但各个行为体之间的利益差异致使至今并无全球性、成型的国际规则出台，多是双边协议或附带条款。

值得注意的是，国际规则的制定与实施，和政府话语权之间存在着密切且复杂的关系。国际规则制定过程的复杂性，使得各国政府话语权的作用方式有所差异，在国际规则的创新与变革中都可以看到不同国家为自身利益的话语权争夺。目前网络安全国际规则仍然处于各方话语权的争夺状态，应从何种维度界定网络安全、如何看待网络安全与国家主权之间的关系、如何判断网络威胁等级与武力回击是否合法等，都构成了各国政府在网络安全国际规则制定中的话语权博弈主题。

本课题拟从当前“网络安全”的技术、犯罪和恐怖主义、军事等多个维度以及不同维度下主要的利益相关群体的构成，以及其中体现出的权力分配特点入手，分析国家政府作为网络安全国际规则创制的行为主体或重要参与者，在此领域进行话语权争夺的主要议题和方式。囿于篇幅限制，本文暂先从技术维度考察国际网络安全规则创制中政府话语权角力。另文将从犯罪和恐怖主义、军事等维度解析。

## 一、网络安全的多元维度概念与权力分配状况

“网络安全”作为概念至今仍非固定，伴随网络技术的发展与网络社会环境的变化，这一概念的内涵不断更新，其外延也有所拓展。但这也并不意味着对这一概念的讨论无从下手。若梳理前人研究与当前网络安全涉及的主要议题，清晰可见“网络安全”概念大致被放入技术、犯罪和恐怖主义、军事三大维度或领域内予以讨论，不同维度下的各个利益相关者的权力分配与话语权博弈情况亦有所差别。但整体而言，技术发展的重要意义、网络威胁的不对等性以及国际组织的角色凸显等特点，上述各个维度均有所体现。

### （一）网络安全的概念界定

就当前研究状况而言，学界尚未就“网络安全”这一概念的内涵和外延达成共识，其中涉及的主体和对象所属领域的差异直接构成了不同的界定。如有学者（王

世伟, 2015:72-84) 认为“网络安全”与“网络空间安全”属于两大不同领域, 后者与军事领域的陆海空天四大空间并列, 前者更侧重线上和网络社会安全。也有学者(陈颀, 2014; 廖丹子, 2014; Nir Kshetri, 2014; Glennon, 2013) 持有相反观点, 认为这一概念更主要指军事意义上网络攻击、网络间谍行为对国家带来的安全威胁。还有学者(李旻、山秀明、任勇, 2014; 刘跃进, 2014; Mathieu, 2015) 更倾向于从技术角度评估网络威胁, 将重点放在黑客攻击、隐私泄露等网络犯罪行为上, 这也是国际电信联盟在2007年颁布的《发展中国家网络安全手册》(ITU, 2007) 中所强调的内容。但更多学者(林婧, 2017; 王世伟, 2015; 任琳、吕欣, 2017; Johnson & Lincke, 2014) 从多个角度论述网络安全的内涵, 包括网络犯罪和恐怖主义、网络战、网络间谍行为等, 尤其在2010年后出现的超级工厂病毒、以及此后中俄、中美、俄美之间就网络安全展开的数项协商, 促使之前仅从数据保护、网络钓鱼和黑客攻击等角度观察网络安全的学者和国际组织将网络武器、或者说网络攻击纳入到考察视野中。这也是为何在2009年ITU(国际电信联盟)颁布的文件(ITU, 2009) 中将军事维度同样纳入到网络安全的视域中。

学界就网络安全治理的目标已基本达成共识, 即包括促进经济繁荣、保障网络社会稳定、确保国家安全等。但对网络安全治理的主要主体——民族国家而言, 不同国家政府对治理目标强调的重点, 以及网络安全的参与方、网络安全与网络主权之间的关系等议题的看法亦有不同, 这也构成了各国在争夺网络安全国际规则创制主导权的重点议题。根据2013年由UNIDIR(联合国裁军研究所)出具的一份报告(Lewis, 2013) 显示, 全球范围内已有一百多个国家制定了与网络安全相关的国家政策。若比对美国、英国、德国等主要发达国家和俄罗斯、中国等发展中国家所制定的网络安全政策要点, 可见其中已然形成两大派别(刘建伟, 2013; Johnson & Lincke, 2014): 美欧等发达国家与俄中等发展中国家, 其主要差异点: 首先在于是否认为网络安全的对象应包括网络信息内容。美欧等国秉持“网络自由”理念, 认为网络安全主要指基础设施安全、并不涉及网络信息内容, 俄中等国则认为网络信息内容应被管制以防其破坏国家政治和社会稳定。其次在于网络安全治理中国家政府应扮演的角色。美欧等国强调私营部门在网络安全治理中发挥主要作用, 而俄中等国认为国家政府对于网络安全环境的营造、网络信息的监管和审查十分重要, 更加强调“网络主权”。第三在于网络安全政策制定的主要目标上, 欧洲等国家更加强调网络安全对互联网经济发展的重要意义, 重点关注网络犯罪、网络恐怖主义等维度; 而俄中等国的网络安全政策则将军事维度纳入其中, 将网络在战争中的应用视为政策要点之一, 更强调网络安全的政治和军事意义。各国政府在网络安全上的理念和认知差异直接体现在该领域国际规则创制的话语权争夺上。



## （二）网络安全领域内的权力不对称构成

无论从政治领域还是社会领域，网络对权力结构带来的巨大变革已成为众多研究者的共识。境内外学者中既有从微观角度乐观看待互联网对政治领域的影响，认为去中心化的网络传播必然赋权草根民众、为公民社会的营造创造了更大的可能性（Kellner, 1999:103）；伴随明显地理边界的消失，国际政治参与主体多元化使得国际规则制定充满了更多变数（喀斯特，2001:91；弗里德曼，2016）。也有从批判角度分析当前互联网的宏观发展，认为信息技术的全球普及并未带来国家边界的消失，线下实际的国际政治结构再次于网络上复制生产，互联网自身迅速普及与20世纪80年代西方推行的新自由主义政策的密切相关，资本在全球流动的过程和权力分化等问题仍旧存在等等，都意味着民族国家政府与大型跨国资本集团仍然是互联网信息社会中掌握最大话语权的主体（赵月枝，2003）。尤其是凭借历史优势，美国等西方国家得以通过控制传播渠道与影响传播内容主导全球话语体系的形成，推行西方文化与价值观；相应在国际规则的制定上，也得以将符合自身利益和价值取向的规则条款推向全球、获得其他国家的认可和支持。但互联网同时提供给俄罗斯、中国、印度等话语权弱势国家扩大本国话语影响力的机遇，并使其参与国际规则制定和修订的能力增强<sup>2</sup>。

上述权力构成体现于较为稳定的网络空间中。网络安全领域中的权力构成一方面同样具备网络社会的整体特点，但同时也更多体现为明确的权力不对称分布特点：

第一，技术即权力的意义更为重要。互联网中技术和权力的关系密不可分，技术实力构成了对互联网规则解释权的重要组成部分（任琳，2013:38-57）。正因如此，网络技术的发展水平直接构成了各国政府话语权的分水岭。而掌握有数据储存与传输等相关技术的专家、程序开发人员以及提供相关业务的互联网服务运营商、云计算等私有企业在这一领域明显掌握有更多话语权，在该领域积极发声并推动互联网安全协议的制定。而在互联网上积极参与政治运动、社会议题的讨论、构成网络公民社会神话体系中重要组成部分的广大普通网络用户，则作为网络犯罪和网络攻击的潜在受害者话语权相当有限。

第二，现实弱势主体对现实强权主体构成威胁并不少见。正如查德威克在其著作《互联网政治学》（查德威克，2010：7）中所说：“线下的机构（政府、公司或主流媒体）权力当然会蔓延到线上，但是网络空间中的权力较为脆弱且要视条件而定”。在线下，在网络安全领域，网络攻击所具有的不对称本质（Nir Kshetri，2014）意味着恐怖分子、激进分子、黑客、网络诈骗集团等群体纵使在现实生活中掌握的资源有限、属于权力相对弱势群体，但因能够借助网络攻击对大型商业集团

和国际组织、国家政府等现实强权机构造成损害，并挑战国家政府等主体在相关领域的权威性，由此成为虚拟强权主体。较典型者如ISIS等恐怖组织借助社交网络招募成员、有效扩大自身影响力。相应而言，纵使经济规模较小、整体政治实力有限的国家也能够对美欧等发达国家构成威胁，而现实国际政治中主要凭借先进的经济发展水平和雄厚的军备水平（如核武器）获取最大话语权的国家，和其他不发达国家一样都会面对网络攻击和网络威胁。

第三，国际组织重要性日益凸显。对于国际规则的制定而言，若某领域内强权国家之间、强权国家和发展中国家之间存在较大冲突，往往较难形成有效规则；一旦形成规则也多依靠霸权国家单边行为推行，并不具备国际性；尽管话语霸权国家能够在国际舆论场上阐释己方标准合法性，污名化或削弱异见国家的观点，但一个切实有效的国际规则的出现，必然有赖于国际组织在其中作为基本协商形式和机制发挥作用。如国际电信联盟等国际组织作为平衡各国利益、保障网络社会良好发展的机构，其角色主要在于提供平台促使该领域议题进入各国政府决策视野、推动安全技术的发展等。此外，网络信息跨越主权国家的地理边界对一国国内电力、交通、金融等基础设施加以攻击和破坏的情况下，主权国家难以对信息发出者和发出地进行定位，如准确发现嫌疑人仍存在管辖权问题，若不依靠建立有效的双边、多边合作机制，面对跨境网络犯罪行为，国家政府仅凭本国之力很难对此类行为予以追责和惩戒。因此，哪怕在各国利益趋于一致的领域——打击网络有组织犯罪和恐怖主义，仍然亟需长期、有效的国际合作机制的支撑。这也是国际组织能够发挥有效作用、对相应国际规则的创制产生影响的重要领域。

## 二、网络安全规则的技术维度：技术强国话语权占优

技术是“网络安全”最根本的决定因素之一，技术维度是认识、维护“网络安全”最基础也是最先的抓手。互联网技术标准和安全协议的拟定从一开始并不由国家政府决定，而是由国际社会内的非政府行为体——如互联网顾问委员会等科学家团体、研究机构制定，其所关注的更多是互联网自身使用的准则问题（查德威克，2010：59；Salter，2004），并不牵涉网络的商业或政治军事目的。之后网络标准和系列协议的制定者主要由国际电信联盟、互联网名称与数字地址分配机构、互联网工程任务组等国际组织牵头完成，同时也有大量的白帽黑客个体和卡巴斯基等网络安全公司在其中监测并修复网络安全漏洞，保证各项网络协议的顺利实现。不过，国家政府在其中的角色仍不容忽视，毕竟在众多学者眼中，网络信息技术的诞生与“冷战”时期的大国战略博弈密切相关（Madeline，2012）。而此后各类网络安全协议和标准的构架与发展也无法彻底脱离主权国家而存在。技术被视为网络安全的

基础，也是网络安全领域中各类行为主体话语权力的基石，网络技术强国和网络技术弱国在相应技术标准和协议制定上的话语权差异巨大。

### （一）政府话语权强弱整体受限于历史因素

在网络安全的技术维度上，各国在相应安全标准或协议制定上的权力大小由两个因素决定：历史和技术。历史因素主要体现为各国的网络技术沉淀，即网络技术的历史积累直接决定了网络安全领域的权力格局。互联网发展的历史进程、其中产生的各项协议标准是当前互联网运作的重要基础，而最先探讨这一领域的国家无论在基础设施上对网络数据服务器的占有、还是从数据流通上安全协议和技术标准的开发和改进、安全产品的资格认证等都占据了先天优势，相对而言互联网技术后发国家则处于先天劣势地位，因缺乏物理层面对技术的主导权，而难以从基础设施和数据流通等各个领域确保数据安全。

以根服务器和域名分配为例，历史形成的网络数据根服务器的分布，决定了美国在网络安全领域的最大话语权。在互联网发展早期，学术机构与研究人员构成了网络技术规则制定的主体。但自20世纪90年代中期起，大型商业集团和美国政府进入这一领域并成为规则制定者或规则制定的主要参与者。由技术人员和研究机构尝试考量顶级域的全新治理模式应对互联网的扩张和商业化，编制了《通用顶级域谅解备忘录》的文件，但遭到包括美国政府在内的多方反对，美国商务部最终介入了互联网域名系统的治理。在1998年美国决定将域名系统的管理交于一家新设立、具有全球参与性质的非营利美国企业，即ICANN（互联网域名与数字地址分配机构）。美国商务部对相关纠纷（的解决）仍然掌握有最终决定权<sup>3</sup>。ICANN主要负责全球互联网域名根服务器、域名体系和IP地址等的管理。根服务器是全球网络中的基础服务器，现有的13台根服务器中包括1台主根服务器，设在美国；12台辅根服务器，9台在美国，剩余3台分别设置在英国、瑞典和日本。这也是为何ICANN组织对互联网产生强有力的控制作用和重大影响，而这一组织对域名的分配和监督本质上仍然是美国政府的单边行为。2005年联合国设立的互联网治理工作组号召美国放弃对互联网域名和号码的单边监督，但被美国政府拒绝（NTIA，2005）。尽管2016年ICANN与美国商务部签署的执行合同到期，美国政府对批准域名根区文件调整的审批权最终消失（NTIA，2016），并自2017年后开始由全球多利益相关方社群对该组织进行职能管理（IANA，2016）。但全球网络域名和服务器分配格局已基本形成，美国在这一基础技术领域内占据了最大优势，并依靠旧有制度掌握了最大话语权。

在网络安全的其他技术领域同样如此。技术先发国家凭借诸多技术专利拥有了国际网络安全标准上的创制权，并借此机制对后发国家的技术专利申请和标准创制

进行打压,以防不利本国网络安全技术发展的标准通过。典型事例如IPV6(互联网协议第6版)技术框架的推进使得域名得到极大拓展,能够支撑更多根服务器的运行。但是在21世纪初镜像根服务器(Mirror server)在中国等国家得以设立,然而根服务器数量并未增加(韩夏,2013:13)。而相应美国对顶级域名的掌控使其能够在国际政治事务中借此增强自身攻击能力,如伊拉克战争期间,在美国政府授意下,伊拉克区域的顶级域名.iq的申请和解析工作被终止,所有网址以.iq为后缀的网站消失,直至2005年才获得重新授权,此期间伊拉克无法通过新媒体渠道进行自我宣传,无异于在战争期间对本国行动目的与合法性的宣传丧失了极大话语权。

## (二) 政府话语权的拓展有赖于技术开发

除了历史因素导致的技术沉淀对各国网络安全领域话语权的决定性作用外,技术开发和发展也是各国得以扩大自身话语权和影响力的必要基础。尤其对于网络技术后发国家而言,鉴于网络技术的强迭代性,能否掌握网络系统和信息传输协议中的最先进技术标准成为各国在该领域扩大话语权的基本,也成为一国能否在网络空间竞争中占据优势地位的基本。

在现有的国际网络安全协议和技术标准下,仍存在众多的遭受远程攻击和数据窃取的安全漏洞,各国专业技术人员和网络安全公司竞相开发在数据加密和身份认证上相关算法,以期使其成为国际认可、并可全球范围推行的标准;而伴随移动技术的开发,关于移动网络运行、无线网络接入等不同领域协议仍存在多种可能,技术的迭代性使得掌握最先进技术、且将其推向全球成为国际标准的国家必定会在之后的网络运行中受益。

首先,对于网络强国而言,在不断开发新技术、申请专利的同时,试图通过与盟国签署网络安全合作协议、设置网络安全技术贸易壁垒以强化对网络空间主导权。如根据国际标准委员会统计的自2006-2016年间各国获得认证的网络安全治理技术专利项目(ISO,2017),可见排前两位的是日本和英国。美国的国家标准技术协会(NIST)发布的关于网络安全系列手册、指南成为其他国家制定本国安全规则的重要参考。美国还与传统盟国签订了系列网络安全合作协议,并“胁迫或诱使其他中小国家”与其立场保持一致(任琳、吕欣,2017:130-143)。同时网络先发国家对安全相关技术的进出口设置贸易壁垒,以试图把控核心技术,使本国在网络基础设施、数据传输等多个领域占据主导地位(OECD,2012)。

第二,后发国家积极开发、采用新技术(如大数据、IPV6),抗衡美国等强权国家,并试图通过技术创新与突破转变历史劣势、主导网络空间安全规则。强权国家若在某一技术领域不能保持领先地位,其所相应推行的规则也难以在国际上获得认可。如美国曾推行WiMAX移动通信技术,并在2004年获得国际机构IEEE批



准,在2007年由国际电信联盟分配频率,成为全球3G移动通信标准,但是这一技术和中国等发展中国家普遍采用LTE技术相较存在更明显的安全漏洞,难以在全球获得大规模应用。云计算和虚拟化等技术的应用,对网络安全新算法的开发提供了新的可能。已有研究者探索了大数据安全分析技术在对网络异常检测、攻击测定、网络安全态势感知、网络威胁情报分析等方面的运用(陈兴蜀、曾雪梅、王文贤、邵国林,2017:1-12),如俄罗斯、印度和中国等网络后发国家积极加入此领域的探索,并申请此领域的技术专利。在国际标准委员会统计的自2006-2016年间各国获得认证的网络安全治理技术专利项目(ISO,2017)中,排在第三位和第四位的是印度和中国。在军民通信领域都能够发挥重要作用的卫星导航系统开发上,当前国际通行的是美国主导开发的GPS系统,美国对这一技术的完全掌控使得后发国家在该领域处于完全依附状态,并在军民通信领域受到美国制约。典型代表如1999年美国曾通过关闭印巴地区的GPS信号直接干扰印巴卡吉尔战争进程。对此,欧盟、俄罗斯、中国和印度都竞相开发本国卫星导航系统,以期打破美国在这一领域的技术垄断,掌握本国在这一领域的话语权,如俄罗斯的格洛纳斯系统、中国的北斗系统,欧盟的伽利略系统、印度的区域导航IRNSS系统等,均突破了美国GPS系统的一统天下格局。

### (三) 政府话语权博弈集中体现为国际网络技术标准的创制竞争

技术开发的能力是一国政府在该领域内话语权的基础。但是技术性权力仅提供给一国扩张话语权的基础,仍有赖于一国政府的制度性权力和解释性权力(任琳、吕欣,2017:130-143)。能否将本国开发的技术标准推向全球、使其成为国际通行标准则是关键。

首先,强权国家借由把控行业协会或标准组织推行利于己方的技术标准。目前与网络安全标准化相关的国际组织主要有国际标准化委员会(ISO)、国际电信联盟(ITU)、国际电工委员会(IEC)、互联网工程任务组(IETF)等。这些组织分别就网络安全中的系统互联、数据加密、身份认证、安全评估、设备安全、安全框架和管理服务等多领域制定国际标准。美国等强权国家利用自己在这些行业协会或国际标准组织中的既有影响力<sup>4</sup>,推行对己方有利标准国际化,并迟滞或阻碍对己方不利标准成为国际标准。如国际电信联盟要求3G标准提交最终时间为1998年,但在9年后美国为了向全球推行本国开发的WiMAX技术,促使国际电信联盟召开专题会议、将其设定为3G国际电信标准,并获得全球频率,与此同时获得本国互联网企业英特尔等大型公司背书。这在当时无疑对中国自主开发的TD-SCDMA的3G技术构成极大威胁。而中国颁布的无线局域网安全标准(WAPI)在一开始就受到美国的极大反对,在2004年中国向国际标准化组织ISO/IEC提出该项国际标准提案后,



作为秘书处担任方的美国国家标准技术协会无故取消了中国方案（宽带，2004），此后中国提案屡被阻挠，2011年中国在ISO/IEC相关组的国家成员宣布撤回提案，停止了WAPI标准国际化的努力。尽管国际标准组织由来自多国的专家学者组成，但是担任秘书处的国家对各项标准方案能否进入大会讨论议程具有较大的决定权，美国恰是凭借自己作为秘书处单位的影响力对不利于本国安全技术他国标准进行阻挠，从而保证他国无法在该领域占据话语主导地位。

第二，美欧对技术领域各类标准和安全协议制定的争夺，凸显出技术强国就争夺技术主导权展开话语权角力。在航天领域已出现美国主导的GPS和欧盟主导的伽利略两类全球卫星导航系统的竞争，同样在网络电信领域美欧之间也存在此类竞争（黄爱民，2007；伽利略，2005；杨剑，2012），甚至在2014年法德两国曾商讨建设独立的欧洲互联网，以取代由美国主导的互联网基础设施。在“物联网”战略经由国际电信联盟提出后，欧盟是全球第一个系统提出物联网发展和管理计划的机构，并致力于物联网标准化的相关研究，在2009年欧盟委员会宣布了新的行动计划，以试图“确保欧洲在建构新型互联过程中发挥主导作用”（Commission，2009）。而美国则率先在全球推行了EPCglobal物联网体系标准架构，并获得沃尔玛等大型跨国公司的背书。对于物联网的技术标准和具体架构，美欧以及中、日等国仍然未达成统一，各国竞相开发技术标准与架构体系，并通过政府投资研发团队、企业加入标准体系、国际会议阐述本国标准优势等多种手段扩大自由标准影响力，以期成为全球范本，从而在新一代互联网发展中占取先机。

此外，弱势国家借助国际组织和联盟合作扩大自身话语权。国际组织一方面提供给网络发展有限国家以技术支持，帮助其国内网络安全技术的铺设和相应政策的制定，以提升国家网络安全能力。如国际电信联盟等先后颁布网络欠发达国家的网络安全建设指南<sup>5</sup>，联合国的援助行动帮助制定网络安全政策以推动国家层面的网络安全规范，此类技术和政策支持保证了网络发展有限的国家能够拥有自身技术的可能，并为未来技术开发奠定基础，促使其成为全球网络安全领域更为主动的角色。此外，国际组织与合作机制也成为网络后发国家挑战既有规则、既有权威的平台。如ICANN（互联网域名与数字地址分配机构）自2017年后脱离美国政府管控，实行新的“自下而上”“多利益相关方”共治模式，其中董事会与地址支持组织、国家和地区代码域名支持组织、政府咨询委员会等五个组织构成了主要决策者（ICANN，2014）。这一运行机制扩大了代表私营部门（互联网服务运营商）和普通网络用户的组织权利，限制了政府部门的权利，在这一情况下，网络后发国家反而能够摆脱一国一票的限制，通过对国内互联网企业在网络安全的管理和组织进行监管<sup>6</sup>、重视相关学科的资金投入和人才培养、提升本国网络用户网络

媒介素养、支持“白帽子”黑客群体的活动等,培育本国的技术人员群体、私营部门和用户群体成为这一国际组织的积极参与者,从而在根服务器的增加和设置地点上掌握更多话语权。在2012年国际电信世界大会上,近90个发展中国家签署了遭到美英等西方国家共同抵制的新电信规则。中国、俄罗斯等通过上海合作组织、金砖国家等国际组织框架展开多边磋商,签署适应于本区域需求的安全协议和标准(魏英哲,2016:31-34)。此外,2013年由中国研究机构下一代互联网国家工程中心(CFIEC)领衔发起,联合WIDE机构(现国际互联网根运营者)、互联网域名工程中心(ZDNS)等共同创立、于2016年实施的“雪人计划”<sup>7</sup>,不仅面向日益增长的互联网接入需求,更旨在以此制定新的互联网根服务器运营规则,从而为建立多边、民主、透明的国际互联网治理体系打下坚实基础。这一计划同时得到中国政府背书。中国政府通过出台《推进互联网协议第六版(IPv6)规模部署行动计划》以支持IPv6协议在中国境内互联网的推广和应用,推动新的根服务器体系能够在全球网络接入中占据最大份额、最终取代原有的IPv4根服务器的主导地位。“雪人计划”使中国以及其他参与国不仅能够摆脱过去没有根服务器的困境,亦助力这些国家在争取根服务器管理权(也即网络安全规则创制中的话语权)行动中迈出关键一步。

国际网络安全规则创制中,政府话语权的拓展有赖于技术开发与应用。技术是“网络安全”最基础也是最早的决定因素。技术的开发、应用能力,是网络安全领域中各行为主体话语权力的基石,网络技术强国和网络技术弱国在相应技术标准和协议制定上的话语权差异巨大。政府话语权角力集中体现为国际网络技术标准创制竞争,具体表现为:强权国家借由把控行业协会或标准组织推行利于己方的技术标准;技术强国就争夺技术主导权展开话语权博弈(如美欧对技术领域各类标准和安全协议制定的争夺);弱势国家利用国际组织和联盟合作扩大自身话语权威。然而,技术性权力仅提供给一国扩张话语权的基础,话语权威的强固,仍有赖于一国政府的制度性权力和解释性权力的强化,能否将本国开发的技术标准推向全球、使其成为国际通行标准则是关键。

## 余论

如上所述,一国政府在技术维度下的网络安全话语权威的提升,首先有赖于通过网络技术的创新和发展为话语权的获得提供保障。而话语权的进一步强固,则有赖于该国政府对国际网络安全事务的制度性权力和解释性权力的强化,取决于该政府能否将本国开发的技术标准推向全球,不仅拥有良好口碑而更能够作为权威成为公认并被普遍接受的行业标准。

具体而言,技术性权力的提升首先意味着网络技术的创新和发展不仅仅依靠科研团队或个人的主观能动性,还有赖于国家政府创新和实施包容性、激励性制度安排,以及国家的投资和扶持,尤其对涉及全国网络安全领域的技术研发项目、培训项目等提供制度支持资金支持,对其中杰出团体或个人予以表彰激励,以鼓励信息系统自主可控能力的提高。还有,对网络安全领域的国际杰出人才,大胆引进,以使中国在网络技术创新方面在尽量短的时间内赶超技术先发国家。此外,对互联网企业和其他各行业私营部门的网络使用,设定国家标准,要求这些机构将网络安全问题的防控、检测和应对等纳入网络开发和建设中。提升网络安全技术相关学科地位,并给予相应支持,保障该领域的人才培养。

(国际事务中)制度性权力(或者说制度性话语权力)更多体现为,代表国家的政府在基于国际经济政治安全制度(以及相关的国际标准、国际规则、国际秩序)的国际事务上所具有的定义权、制订权、评议权、裁判权,以及“话事权”和决断权、主导权等。具体到国际网络安全领域,其制度性权力的提升则要求一国政府能够在网络安全技术领域的国际标准和规则的制定上占据主导权。它表现为两大方面,一是本国技术标准或有利于本国利益的技术标准是否能够进入国际议程;二是进入国际议程后,是否能够掌握规则制定权使其成为普遍性标准。

对于第一点,一国政府需要提升在国际标准化组织或行业协会中的主动性,积极加入和介入其相关活动,无论是专家表态还是秘书处设立方面的主动参与,保证利于己方的标准能够进入到讨论议程。还可先在少数国家范围内推动本国技术标准成为区域标准,以吸引其他国家采用该技术标准,并以此进入国际议程。此外,更重要的是,提供全球公共、平等参与、专业化的网络安全技术讨论平台和替代制度,如成立行业协会或举办常态化的技术峰会、提出替代治理理念等,以拥有创制规则的话语动能,从而提升主动设立国际议程的能力。

对于第二点,一国政府需要增强对标准权威化方式的主导权。除了在行业协会或国际标准协会中的积极参与保证利于己方的标准获得通过,不利于己方的标准不被认可之外,更重要的是能够在同一领域多种技术标准竞争的情况下,推动最利于权威化本国标准的方式成为主导框架,如是推动技术标准在表决权均等的国际组织内的进行投票表决,还是借助有影响力的跨国私营部门背书,在实践中确保本国标准的应用范围;还是与霸权国家合作,增强本国标准的影响力。

解释性权力的提升,意指一国能够在与其他国家或行为体的交往互动中,对己方技术标准、技术理念以及对技术的价值判断有效推广。尽管技术本身并非具有政治性,但在复杂的国际关系中,鉴于应用技术的主体、范围和方式差异,不同的技术标准往往被赋以政治化的、褒贬色彩的“标签”,典型如中俄等自行开发的卫星

导航系统被西方媒体冠以“军事威胁论”或“挑战美国”的标签。中俄等国家对本国的卫星导航系统的界定与西方媒体完全不同。而这样的理念或价值判断能否被国际认可也直接影响到一国在该技术领域的话语权威。

因此,对本国的技术标准、尤其是附带的技术理念和技术价值判断的有效推广,有赖于:

首先,能够在国际舆论场上占据主动,达成充分表达与被充分理解的可能。不仅仅是制造话题和设置议程以保证关注度,更重要的是通过有效叙事,将己方的技术理念和技术价值判断嵌入到对方的文化背景中,从而获得最大的理解与认同。典型如对于网络内容审查,若放在信息自由语境下则带有明显负面色彩,若与反恐、打击ISIS等相连则带有正面意义。

第二,充分利用社交媒体扩充本国技术标准、技术理念和技术价值判断的影响力。社交媒体已成为国际传播格局中变数较大的领域,对于众多后发国家而言,能够以此作为平台突破强权国家对国际舆论的掌控,并将之作为表达自身观点、争取理解和合作、驳斥虚假和偏见的平台。在扩充本国技术标准、技术理念和技术价值判断的影响力时,对于潜在合作方强化双方共识点,以此为基础诠释己方合理性与合法性,获取多数认同;对于认同冲突方,在明确己方立场和对方立场的基础上,通过放大己方话语体系的“音量”应对对方偏见与否认。

第三,形成系统的网络安全观,提供对技术维度的解释性话语框架。譬如,何为技术领域的国家利益和国家安全,何为技术领域的“威胁”,对重要、核心概念进行重新阐述与定义,并将之以通俗易懂方式进行境内外传播,不仅扩大这一安全观的境外影响力,更重要的是提升境内民众自觉应用这一安全观解读和应对网络技术安全问题的能力。

(责任编辑:罗诗婷)

### 注释 [Notes]

1. 网络安全问题自20世纪80年代起开始进入学术领域。在21世纪初期国际电信联盟、欧盟等国际组织先后就网络安全召开会议、制定协约。但在2010年后对网络安全的关注度显著增加,境内外学术研究数量增加。
2. 2016年美国 and 欧盟对此甚至先后出台反制性法案,如《波特曼—墨菲法案》中明确将俄罗斯、中国列入其中。
3. 可参见 ICANN组织历史。ICANN历史项目,检索于 <https://www.icann.org/zh/history>。
4. 众多互联网行业协会都在发达国家设置。如欧洲电子产业组织“数字欧洲”、美国信息技术行业组织、日本电子与信息技术行业协会等。
5. 譬如ITU在2007年颁布了Cybersecurity guide for developing Countries。



6. 如欧盟要求这些私营部门必须有应对安全威胁的技术和组织手段;能够评估威胁或安全等级;鼓励使用可获取的安全标准。可参见 ISSA International Web conferences: Global Cybersecurity Outlook: Legislative, Regulatory and Policy Landscapes检索于 [http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/2015\\_Web\\_Conferences/6.23.15-WebConf\\_Global\\_Cyber.pdf?hhSearchTerms=%22Global+Cybersecurity+Outlook+Legislative%2c+Regulatory+and+Policy+Landscapes%22](http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/2015_Web_Conferences/6.23.15-WebConf_Global_Cyber.pdf?hhSearchTerms=%22Global+Cybersecurity+Outlook+Legislative%2c+Regulatory+and+Policy+Landscapes%22)。
7. “雪人计划”由中国下一代互联网国家工程中心于2013年联合日本和美国相关运营机构和专业人士发起,提出以IPv6为基础、面向新兴应用、自主可控的一整套根服务器解决方案和技术体系。2016年在美国、日本、印度、俄罗斯、德国、法国等全球16个国家完成25台IPv6根服务器架设,其中1台主根和3台辅根落户中国。它事实上形成了13台原有IPv4根加25台IPv6根的新格局。该计划将打破根服务器困局,全球互联网有望实现多边共治。

### 引用文献 [References]

- 安德鲁·查德威克(2010).《互联网政治学:国家、公民与新传播技术》(任孟山译).北京:华夏出版社.
- [Chadwick, Andrew(2010). *Internet Politics: States, Citizens, and New Communication Technologies*. Beijing: Hua Xia Publishing House.]
- 陈颀(2014). 网络安全、网络战争与国际法——从《塔林手册》切入.《政治与法律》, (07), 147-160.
- [Chen, Qi(2014). Cybersecurity, Cyber-war and International Law - Seen from the Tallinn Manual. *Political Science and Law*, (07), 147-160.]
- 陈兴蜀, 曾雪梅, 王文贤, 邵国林(2017). 基于大数据的网络安全与情报分析.《工程科学与技术》, (05), 1-12.
- [Chen, Xingshu., Zeng, Xuemei., Wang, Wenxian., Shao, Guolin(2017). Big Data Analytics for Network Security and Intelligence. *Advanced Engineering Sciences*, 49(3), 1-12.]
- 伽利略全球卫星导航系统——打破GPS统治地位(2005).《国外科技动态》, (1), 31-33.
- [GALILEO Global Navigation Satellite System - Breaking GPS Dominance (2005). *Recent Developments in Science & Technology Abroad*, (1), 31-33.]
- 韩夏(2013). IPV6根服务器设置上应考虑用户和地域因素.《中国教育网络》, (05), 13.
- [Han, Xia(2013). User and Geographical Factors should be Taken into Account in IPV6 Root Server Settings. *China Education Network*, (05), 13.]
- 黄爱民(2007). 伽利略(GALILEO)系统对美国GPS的冲击.《测绘与空间地理信息》, 30(3), 41-44.
- [Huang, Aimin(2007). The GALILEO Project Impacts to American GPS. *Geomatics & Spatial Information Technology*, 30(3), 41-44.]
- IANA管理权移交协调小组(2016). 互联网号码分配机构(IANA) 职能管理权移交提案.检索于 <https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-zh.pdf>.
- [ICANN(2014). Accountability mechanism. Retrieved from <https://www.icann.org/resources/>



- pages/mechanisms-2014-03-20-en.]
- 宽带无线IP标准工作组(2004). 2004 ISO/IEC JTC1 SC6 全会简报——WAPI 国际标准推进取得阶段性成果.检索于 <http://www.chinabwips.org/doc/gzdt-40.pdf>.
- [Broadband Wireless IP Standards Working Group(2004). 2004 ISO/IEC JTC1 SC6 Plenary Session Bulletin - WAPI International Standards Made Phased Achievements. Retrieved from <http://www.chinabwips.org/doc/gzdt-40.pdf>.]
- 李灵, 山秀明, 任勇(2004). 网络安全概述.《中国工程科学》, (01), 10-15.
- [Li,Ying.,Shan, Xiuming.,Ren, Yong(2004).Summarization of Network Security. *Engineering Sciences*, (01), 10-15.]
- 廖丹子(2014). “多元性”非传统安全威胁:网络安全挑战与治理.《国际安全研究》, 32(3), 25-39.
- [Liao, Danzi(2014). Challenges and Governance of Multi-Meta Non-traditional Security Threats: Taking Cybersecurity Threats as an Example. *Journal of international Security Study*, 32(3), 25-39.]
- 林婧(2017). 网络安全国际合作的障碍与中国作为.《西安交通大学学报(社会科学版)》, (03), 76-84.
- [Lin, Jing(2017). The Obstacles of International Cooperation regarding Safeguarding Cybersecurity and China's Strategies. *Journal of Xi'an Jiaotong University( Social Sciences)*, (03),76-84.]
- 刘建伟(2013). 恐惧、权力与全球网络安全议题的兴起.《世界经济与政治》, (12), 43-59.
- [Liu, Jianwei(2013). Fear Power and the Rise of Cybersecurity in the Global Agenda. *World Economy and Politics*, (12), 43-59.]
- 刘跃进(2014). 信息安全、网络安全、国家安全之间的概念关系与构成关系.《保密科学技术》, (05), 12-19.
- [Liu,Yuejin(2014).The Relationship of the Concepts and Composition among the Information Security, Cybersecurity, national security. *Secrecy Science and Technology*, (05),12-19.]
- 曼纽尔·喀斯特(2001).《网络社会的崛起》(夏铸九, 王志弘等译).北京: 社会科学文献出版社.
- [Castells ,Manuel(2001).*The rise of the Network Society*. Beijing: Social Sciences Literature Press.]
- 任琳(2013). 多维度权力与网络安全治理.《世界经济与政治》, (10), 38-57.
- [Ren, Lin(2013). Multi-Dimensional Power and Cyber Security Governance. *World Economics and Politics*, (10),38-57.]
- 任琳, 吕欣(2017). 大数据时代的网络安全治理:议题领域与权力博弈.《国际观察》, (1), 130-143.
- [Ren, Lin & Lv, Xin (2017). Cyber Security Governance in the Era of Big data: Issues and Power Game. *International Review*, (1), 130-143.]
- 托马斯·弗里德曼(2016).《世界是平的:21世纪简史》(何帆等译).长沙: 湖南科学技术出版社.

- [Friedman ,Thomas (2016). *The World is Flat: A Brief History of the Twenty-First Century*. Changsha: Hunan Science & Technology Press.]
- 王世伟 (2015). 论信息安全、网络安全、网络空间安全.《中国图书馆学报》, (03), 72-84.
- [Wang, Shiwei (2015). On Information Security, Network Security and Cyberspace. Security. *Journal of Library Science in China*, (03),72-84.]
- 魏英哲 (2016). 从多国网络安全协作看网络空间国际合作新趋势.《中国信息安全》, (10), 31-34.
- [Wei, Yingzhe (2016). A New Trend of International Cooperation in Cyberspace from the Perspective of Multinational Network Security Collaboration. *China Information Security*, (10), 31-34.]
- 杨剑 (2012). 伽利略与GPS竞争案和我北斗系统参与商用竞争.《国际展望》, (4), 13-24.
- [Yang, Jian(2012).The GALILEO -GPS Competition Case and the Participation of Our Bei Dou System to commercial competition. *World Outlook*, (4),13-24.]
- 赵月枝 (2003). 帝国时代的世界传播: 国家、资本和非政府组织力量的重新布局 (刘宏译).载陈卫星 (主编),《国际关系与全球传播》. 北京: 北京广播学院出版社.
- [Zhao, Yuezhi(2003). World Communication in the Age of Empires: Rearrangement of the Powers of Nations, Capital and Non-governmental Organizations. In Chen, Weixin (Eds), *International Relations and Global Communication*. Beijing: Beijing Broadcasting Institute Press.]
- Commission of the European Communities(2009).Internet of Things — An action plan for Europe. Retrieved from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF>.
- Glennon , J. Michael (2013).The Dark Future of International Cybersecurity Regulation. *JOURNAL OF NATIONAL SECURITY LAW & POLICY*,6,563-570.
- ICANN(2014).Accountability mechanism. Retrieved from <https://www.icann.org/resources/pages/mechanisms-2014-03-20-en>.
- ISO Survey(2017).ISO Survey of certifications to management system standards - Full results. Retrieved from <http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1>.
- ITU(2009).Introduction to Security Cyberspace, Cybercrime and Cybersecurity. Retrieved from <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf>.
- Johnson, Joseph &Lincke, Susan. J (2014). A Comparison of International Information Security Regulations. *Interdisciplinary Journal of Information, Knowledge, and Management* ,9,89-116. Retrieved from: <http://www.ijikm.org/Volume9/IJIKMv9p089-116Johnson0798.pdf>.
- Kellner, Douglas(1999). Globalization Form below? Toward a Radical Democratic Technopolitics. *Angelaki Journal of the Theoretical Humanities*, 4(2), 103.

- L. Salter(2004). Structure and forms of use: a contribution to understanding the effects of the internet on deliberative democracy. *Information, Communication and Society* ,7(2),185-206.
- Lewis, James."Cyber security and Cyber warfare: Assessment of National Doctrine and Organization", in UNIDIR , *The Cyber Index: International Security Trends and Realities*, New York and Geneva, 2013.
- Madeline, Carr(2012). The Political History of the Internet: A Theoretical Approach to the Implications for US Power, in Sean Costigan and Jake Perry, eds. ,*Information Technology and International Affairs*, Farnham: Ashgate.
- Mathieu, Gorge. Global Cybersecurity Outlook: Legislative, Regulatory and Policy Landscapes. ISSA International Web conferences: Global Cybersecurity Outlook: Legislative, Regulatory and Policy Landscapes. ISSA. 2015,June.
- Nir Kshetri. Cybersecurity and International Relations: The U.S. Engagement with China and Russia. FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, Argentina, July,23-25.
- NTIA(2005). U.S. Principles on the internet' s domain name and addressing system. Retrieved from <https://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system>
- NTIA(2016).Statement of Assistant Secretary Strickling on IANA Functions Contract. Retrieved from <https://www.ntia.doc.gov/press-release/2016/statement-assistant-secretary-strickling-iana-functions-contract>.
- OECD(2012). CYBERSECURITY POLICY MAKING AT A TURNING POINT: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.
- Williams, Michael(2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly* ,47(4),513.