doi:12.3969/j.issn.1672-0598.2015.01.014

国际网络安全话语权博弈及中国进路*

王 祎

(中国传媒大学 传播研究所,北京 100024)

摘 要:网络的诞生及其相关技术的不断革新,使“国际网络安全话语权”成为各国在国际话语权博弈场中新的角力点,大数据技术进一步拷问民族国家政府的决策甚至执政能力。美国凭借技术、语言、内容优势占据网络安全话语权博弈主导地位,中国须借鉴美、欧经验,秉持“和平发展”一贯立场的同时,制定网络安全战略,完善相关机制,加强基础设施建设和技术研发,推进国际合作,维护互联网正义,树立中国在互联网领域“负责任的大国”形象,全面提升中国的国际网络安全话语权。

关键词:网络安全;话语权;网络攻击;网络犯罪;网络战争

中图分类号:F49 **文献标志码**:A **文章编号**:1672-0598(2015)01-0090-05

继“斯诺登事件”引发的“棱镜监控计划”曝光后,“网络安全”再次成为多方关注的焦点。伴随网络的普及和信息技术的发展,国际网络安全话语权逐渐跃升为国家战略体系不可或缺的组成部分。尤其是在网络传播媒介高度发达的 Web2.0 时代,能否确保网络安全,在国际网络安全话语权博弈中占据主动,在很大程度上决定着我国的整体安全以及在国际社会的地位和形象。

一、网络时代的国际话语权

“话语权”是近年来备受关注的关键词,“仅从字面上理解,话语权就是说话权、发言权,亦即说话和发言的资格和权力。这样的话语权往往同人们争取经济、政治、文化、社会地位和权益的话语表达密切相关。”[1]从葛兰西基于意识形态角度对“文化领导权”的强调,福柯对“话语即是权力”的阐述,到哈贝马斯的“合法化”理论,罗兰·巴特的“泛符号化”之说,以及鲍德里亚的“仿像”观点,关于“话语权”的理论从诸多思想中汲取养分,不断丰富立体起来。伴随媒介革命的发生及其促动的人类传播的深度与广度空前,话语权已超越话语层面,成为研究社会行为与人类互动的关键问题。

全球化的深入搅动着国际格局与权力结构的深层变动,日趋频繁的国际交往与互动使“国际话语权”成为各国际行为体间相互竞争的新内容。具体而言,“国际话语权”是以主权国家为主体的国际行为体在国际社会的话语影响力,关涉到该行为体(国家)在国际规则制定、国际事务处置、国际议程设置和国家利益实现等方面的主动性和自主权。国际话语权是综合国力的重要体现,以国家政治、军事、经济等“硬实力”为基础,并受文化、意识形态、社会制度等“软实力”影响,与国家对“巧实力”的综合运用高度匹配。伴随国际力量对比的消长,为维护对内统治的合法性与国际利益的正当性,各

* [收稿日期]2014-11-14

[作者简介]王祎(1986—),女,河北省人;中国传媒大学传播学博士生,主要从事国际传播、跨文化传播研究。

国纷纷加紧国际话语权的争夺,并将其纳入国家整体战略,作为国家安全体系的重要环节。

如果说 20 世纪中叶以后电视媒介的发展和普及,给国际话语权争夺开辟了新的场域,那么网络的诞生及其相关技术的不断革新,无疑将各国间围绕国际话语权的博弈带入了一个全新的时代。由于电视节目本身需要依靠卫星转播而实现,因此各国尚可以通过法规管制设置壁垒,防范全球化媒介集团及其节目在本土落地,从而在国境之内稳操话语权。然而,网络的出现直接消解了这种可能,其开放性不断突破着国家的物理疆界,侵蚀着国家的传统主权。网络已经成为继领土、领海、领空之后民族国家赖以生存和发展的“第四空间”,并与三种传统现实空间形成互动与制约。“国际网络安全话语权”逐渐进入视野,成为各国在国际话语权博弈场中新的角力点。所谓“国际网络安全话语权”,是指以主权国家为主体的国际行为体在网络安全相关事务中的话语影响力。

进入 Web2.0 时代,以社交网络为代表的媒介进一步在开放性上大幅提升,并以其鲜明的交互性被称为“新媒体”,以区别于广播电视等单向传输为主的“传统媒体”。“新媒体”的崛起在重塑传播格局的同时,对国际事务也带来了深远的影响,其架构的扁平性、去中心性和边界隐匿性,促使较之以往更为迅猛的“全球化”的发生。超越国家物理疆界的交往借助“新媒体”平台可以轻易实现,从而在深度和广度上都大幅提升,这给各民族国家带来了新的安全挑战和战略议题。

大数据技术的发展与应用,是新变局的开端。这一新兴计算机技术逐渐从商业领域辐射社会生活的各个方面,并蔓延到政治、军事领域。在国家决策中,基于经验材料的感性判断日渐退出历史舞台,基于大数据挖掘与计算的理性分析成为“新宠”。在不久的将来,数据获取与处理能力在一定程度上将决定政府的决策甚至执政能力。在这一背景下,数据安全、网络安全在整个国家安全体系中的地位将不断上升,国际网络安全话语权将成为各国争夺的重要战略目标。

二、国际网络安全话语权博弈与中国困局

当前,国际网络世界的权力格局与总体国际格局呈高度同质性。各国围绕国际网络安全话语权展开的博弈在变动中重构,但明显优势仍被美国所占据。

首先,美国占据国际网络安全话语权博弈中的技术优势。世界上第一台电子计算机于 1946 年诞生于美国,世界上第一条通讯光纤干线由美国于 20 世纪 70 年代铺设,而计算机网络则肇始于美国军方因冷战需要建设的“阿帕网(ARPA NET)”。克林顿执政时期,美国便提出建设“信息高速公路(Information Superhighway)”计划。此后,美国不断扩大在计算机网络技术领域的优势。从服务器和 PC 制造商 IBM,芯片制造商英特尔,路由器制造商思科,移动网络终端和应用服务供应商苹果,到操作系统和软件开发商微软,数据库供应商甲骨文,搜索引擎开发商谷歌……这些在互联网核心环节的生产销售中居领导地位甚至垄断地位的公司,几乎都来自美国。此外,根服务器和域名体系可视为国际互联网的命脉所在。目前,全世界共有 13 台根服务器,其中 1 台为主根服务器,位于美国;其余 12 台辅根服务器有 9 台位于美国,2 台位于欧洲,1 台位于亚洲(日本)。所有根服务器均在美国政府授权的互联网域名与号码分配机构 ICANN 的统一管理之下,统领全世界互联网域名根服务器、域名体系和 IP 地址等事务,美国政府在全世界的互联网安全事务中拥有发达的欧洲也难以企及的话语霸权。这些核心技术优势正是美国在国际互联网话语权博弈中谋求霸权的重要基础。

其次,美国等发达国家占据国际网络安全话语权博弈中的语言优势。网络时代伊始,这种新型传播方式被人们寄予厚望,被看做“公平”与“自由”的“使者”,负载着对未来“平权化”世界的美好憧憬。然而,多年的实践使人们逐渐认识到,网络世界“平等”表象遮蔽了其不平等权力关系的实质,西方发达国家的话语霸权主导着网络中明显的文化偏向。造成这一偏向的主要原因是语言因素:从编程到应用,英语都是计算机和网络通用的标准语言,这就从起点上造就了非英语国家的被动性,使之处于竞争中的不利位置。

最后,美国等发达国家占据国际网络安全话语权博弈中的内容控制优势。一方面,以英语作为表述语言的网络必然使英语民族文化在互联网中具有压倒性优势,同时限制了其他民族语言文化在网络传播的范围和可能性;另一方面,互联网的开放性直接导致其广泛参与性,众多普通民众的参与则

决定了网络文化的大众性。从根源上说,大众文化本身就是资本和文化结合的产物,美国则是大众文化全球推广中最大的生产者和受益者。通过产业化运作,美国不断通过互联网媒介向其他国家(特别是欠发达的第三世界国家)输出文化产品及其背后隐含的价值观和意识形态,强烈冲击着当地民众的传统文化和理念。据统计,互联网上的信息大约八成以上源自美国,在《1996 年电信法》通过之后,以 ABC、CNN 为代表的大广播公司跨越媒介形式壁垒,影响力蔓延至互联网,形成了对信息供应更大的垄断,造成其他国家和地区对其更大程度的依赖,以互联网为载体向全球推行更为隐蔽和强势的"文化帝国主义"。

凭借以上优势,美国等少数西方发达国家一方面渲染他国威胁论,大唱"维护自由"与"保障隐私"的颂歌,一方面私下进行侵犯他国信息安全的干涉行径。此类实例不胜枚举,如美国和欧洲一些国家大肆支持谷歌公司以"拒绝支持政治审查互联网搜索"为名全面退出中国大陆市场;美国和加拿大政府以"希望确保信息的自由传播"为由公开向中东和亚洲一些国家政府施压,限制其因黑莓手机制造商涉嫌侵犯各国安全信息而展开的合理调查与制裁;美国自"911"事件之后对他国实施秘密监控的"棱镜计划"……在"棱镜计划"被前美国中央情报局(CIA)工作人员斯诺登揭露之前,美国曾多次指责他国政府不尊重人权,对公民隐私权肆意侵犯,特别是针对秉持不同意识形态的社会主义中国,更是实行"双重标准",联手其他资本主义发达国家企图形成"合围"与"绞杀",网络话语霸权体现得淋漓尽致。伴随我国经济的腾飞和综合国力的迅速增强,国际网络安全话语权仍未得到与国际地位相匹配的发展,我国面临技术发展滞后、国际环境严苛的困局,如何突出重围,维护国家利益,捍卫国际网络正义,在网络时代占据国际话语权博弈中的有利位置,是我国未来一段时间必须破解的难题。

三、美、欧网络安全战略启示

(一)美国的网络安全战略

克林顿执政期间尚属互联网发展初期,因此美国将网络安全战略重点放在信息基础设施建设上。除"信息高速公路"计划外,克林顿于 1998 年颁布第 63 号总统令,首次提出"信息安全"概念;并于 2000 年颁布了《信息系统保护国家计划》,再次重申国际信息基础设施的重要性,确定了网络安全事项优先发展的原则,并提出要对新建和业已投入运行的重要网络信息系统实行全寿命安全周期管理,定期进行安全测试和风险评估,确定相应的安全等级,实施有针对性的保护,并由联邦机构高级官员根据安全控制有效性和参与风险值高低来决定该信息系统的运行或退出,从而建立起严密的网络安全防御体系。

小布什执政以后,美国国防部网站屡遭攻击,特别是"911"事件爆发后全球"反恐"进入白热化阶段之时,恐怖分子频繁利用系统漏洞攻击美国核心部门计算机网络。为应对新型的"网络恐怖主义",美国政府于 2003 年发布了《国家网络安全战略报告》,将网络安全上升到国家安全的战略高度,并大力发展网络战争武器,研发出以计算机病毒为主要形式的软件网络武器,以及通过摧毁根服务器等网络物理载体实现有效打击的硬件网络武器。同时,还创建了一支精锐的"黑客部队",随时准备入侵恐怖组织或其他国家的网络系统,占据网络战争的先机。

奥巴马当选总统以后,于 2009 年发布了由国家安全委员会和国土安全委员会联合负责拟定的网络安全评估报告,指出美国在多次网络和信息入侵中遭受数亿美元的巨额损失,多项军事机密和知识产权被窃取,并有大量数字信息基础设施被破坏。网络危险已成为美国面临的最为严重的威胁之一,并宣称美国要严肃应对这一挑战。为维护网络安全,保障国家利益,奥巴马政府在削减传统武器经费投入的同时,大力增加网络武器研发,筹建网络军队司令部,从"被动防御"转向"主动出击",谋求网络战争的"先发制人",对潜在威胁形成有效威慑。

美国是最早引入网络战争概念并将其理论化、系统化,并付诸实践的国家,其网络国防体系是最为成熟完备的,其未雨绸缪的战略前瞻性,周密的风险防控体系,各部门间有序的管理与配合,高度的核心技术自主性,以及在网络安全话语权争夺中的"主动出击",对我国网络信息安全体系建设有很大启发。

(二)欧盟的网络安全战略

自 2003 年美国政府发布《国家网络安全战略报告》后,全世界先后有 40 多个国家制定颁布了本国的网络安全战略,其中包括爱沙尼亚、芬兰、斯洛伐克、捷克、卢森堡、荷兰和英国等 10 个欧盟国家成

员。[2]伴随欧洲一体化的不断深入,经济上的相互依赖导致安全领域合作的加深,特别是网络时代全面到来后网络安全风险日趋严峻。在这一背景下,欧盟委员会于 2013 年发布了《欧盟网络安全战略:公开、可靠和安全的网络空间》。这是欧盟组织在网络安全领域的第一个综合性政策文件,评估了欧盟当前面临的网络安全形势,确立了网络安全工作的指导原则,明确了各利益相关方的权利和责任,确定了未来五大战略有限项目和具体行动举措。[3]

欧盟的网络安全战略旨在构建一个公开、可靠和安全的网络空间,大力打击网络犯罪,发展网络安全技术与相关产业,加强政府、企业与公民间的多维合作,增强欧盟在网络安全方面的整体防御力,保障欧盟成员国及其公民在网络空间的利益与权利。其具体措施展现出明显的合作性和立体性,具有一定的借鉴意义。

一是建立机制:通过立法手段,在欧盟层面进一步增加各成员国主权让渡范围,扩大欧洲网络和信息安全管理局(ENISA)的权限,完善其职能,增强统一应对网络袭击的应急响应机制和抵御侵犯能力;在各成员国层面各自建立网络安全事务职能机构,结合欧盟整体战略,制定各国网络安全战略和风险评级标准;在社会层面形成企业与政府联动机制,要求企业就网络安全重大事故必须向主管职能部门汇报,职能部门须向企业提供风险防控信息,并以激励手段对此联动加以保障;在公民个体层面加强教育培训,提高个人的网络安全意识和风险防控能力。二是加大投入:由欧盟统一设立并管理专项资金,用于支持成员国对网络漏洞分析、网络风险防控、网络犯罪调查与打击等转向行动;同时通过政策引导、激励手段和渠道平台支持,加强欧盟本土信息通信产品企业和计算机网络服务商的研发能力,完善产业链发展,摆脱对外依赖。三是加强合作:在欧盟内部,在共同防务框架下开展成员国间扎实有效的网络防务合作,为欧盟及其成员国军队提供网络安全防御训练机会,提升其实战能力;由欧洲警察局和欧洲法院合作向各成员国提供网络犯罪调查和侦破方面的支持;将企业和公民个体等民间力量纳入整体网络防务体系;在国际舞台,一方面深化与拓展欧盟与联合国、欧洲理事会、北约等国际组织的对话与合作,谋求在全世界范围的广泛理解与互信;另一方面,重视与美国等意识形态趋同国家的合作,促进基于双方共同利益的联合行动的开展;此外,支持并协助他国网络安全能力的提升,寻求更广泛的国际盟友与国际话语权的提升。

四、中国立场与破题进路

近年来,中国经济的腾飞带动着中国整体实力的增长和全球地位的上升。由于意识形态差异和国际格局变动带来的“失利者”恐慌,美国等对中国采取敌视态度的国家一直鼓吹“中国威胁论”。这种舆论“绞杀”从现实社会扩展到虚拟空间,一时间在网络世界也甚嚣尘上。中国网络多次遭遇的来自美国的 DNS 污染事件,以及近期美国司法部对 5 名中国军官的公开指控,便是这种敌意下的集中反映。不同于美国称霸全球的战略企图,中国向来秉持“和平崛起”的战略选择。中国在国际网络安全事务上也与中国外交的一贯秉承立场保持一致:尊重他国的网络主权,主张在国际范围内增进对话与理解,加强国际合作,捍卫国际网络正义,反对任何形式的网络信息霸权。

目前,我国的国际网络安全话语权仍明显滞后于综合国力提升,技术发展滞后、网络攻击频繁、国际舆论环境严苛,对我国网络安全形成了巨大挑战。为顺应形势,迎接挑战,我党在十八届三中全会上的《中共中央关于全面深化改革若干重大问题的决定》中明确指出:要“坚持积极利用、科学发展、依法管理、确保安全的方针,加大依法管理网络力度,加快完善互联网管理领导体制,确保国家网络和信息安全”。在这一大政方针指导下,中国的网络安全建设需结合国情,审时度势,谋求进路。

第一,加强网络主权意识,制定整体网络安全战略。互联网的发展普及也带来了风险的升级,美国和欧盟等发达国家和区域已先后制定了本国或本区域的网络安全战略,并逐渐将基于网络战争概念的网络武器研发和网络军队建设作为未来军备发展的重点。此外,“中国威胁论”在网络世界的蔓延以及美国主导的国际舆论压力,进一步加剧了中国面临的网络安全严峻性。因此,中国必须在夯实硬实力基础前提下,充分重视“领网”主权,将网络安全上升到国家战略安全的高度,高瞻远瞩,积极筹划,根据国情制定切实可行的长远规划。

第二,形成多元多维互动,建立立体网络安全机制。网络的开放性和匿名性,决定网络安全的维护无法仅依靠国家或政府的力量实现。特别是交互性日趋加强的 Web2.0 时代,政府的权限和掌控

力不断缩减,在充分发挥政府相关职能部门作用的同时,必须积极动员社会力量,鼓励非政府组织等民间力量对网络安全维护的参与,同时加强国民教育,普及网络安全知识,提高风险防范意识,形成多元主体间的多维互动。

第三,加大基础设施投入,掌握国际先进网络技术。技术优势是美国掌握国际网络安全话语权的基础和先决条件,也是中国扭转被动局面,寻求话语权提升的关键所在。为缩减技术方面的差距甚至实现赶超,需要加大基础设施方面的资金投入,并通过制定政策、提供平台来引导企业在网络安全产业的技术研发,发展有自主知识产权的网络信息技术和基于汉语的操作系统及软件应用,建设立足本土、全球领先的根服务器和域名体系,降低对外依赖所形成的漏洞与风险。

第四,加强网络信息管理,守卫网络信息安全"国门"。美国在国际网络安全话语权的争夺中,很大程度上依托大量的植入本国利益诉求和意识形态的网络信息产品输出来实现。因此,我国必须提高警惕,加强监管审查,同时继续加强网络防火墙建设,力求将不利于社会稳定、有损于国家利益的网络信息产品及内容、文化隔离在"国门"之外。

第五,充分利用国际平台,提升国际网络安全话语权。网络对于时间和空间的压缩使全球社会更加紧密地联系在一起,各国家各民族都无法脱离这种联系而"独善其身"。据有关数据统计,自2006年至2012年间,世界上的网络攻击事件已从5 503起增至48 562起,增幅高达782%,[4]"北约"每天遭受的网络攻击也高达百余次,[5]网络安全已成为事关各国家和地区切身利益的重要问题。网络攻击对于国家边界的轻易跨越,使集体安全的实现必须依赖各国更为频繁的对话与更为紧密的合作。同时需要指出的是,美国的霸权企图并未因互联网的去中心性和扁平性而有所收敛,而是以更为隐蔽的方式继续谋求对全球事务的主导。在这种双重压力下,中国必须充分利用国际组织、国际会议、国际论坛等平台,展现中国维护互联网正义与和平的立场与诚意,开展双边、多边网络外交,寻找共识,破解"安全困境",在国家间、区域内、区域间以及全球范围内谋求更广泛的对话与合作,推进全球网络治理的长足发展,在互联网事务上树立中国"负责任的大国"形象,谋求与综合国力和国际地位相匹配的国际网络安全话语权。

[参考文献]

[1] 张国祚.关于"话语权"的几点思考[J]. 求是,2009(9):43.

[2] [3]雷小兵,黎文珠.《欧盟网络安全战略》解析与启示[J]. 信息安全与通信保密,2013(11):52.

[4] GAO,Cyber Security:National Strategy,Roles,and Responsibilities Need to Be Better Defined and More Effectively Implemented,February[R],2013.

[5] Alexander Klimburg Ed., National Cyber Security Framework Manual, NATO Cooperative Cyber Defense Center of Excellence Publication[R],Tallinn 2012.

(责任编校:朱德东)

Game of International Network Security Discourse Power and the Approach of China

WANG Yi

(*Communication University of China*, *Beijing* 100024, *China*)

Abstract: The birth of network and the related technology innovation make the "international network security discourse power" become a new field of wrestling game around international discourse power. Big data technology further tests the decision and ruling ability of nation-state government. The United States takes the leading position of network security discourse right game by taking the advantage of the technology, language and contents, China should learn the experience of Europe and the United States, uphold the constant principle of "peaceful development", meanwhile, make the network security strategy, perfect the related mechanism, strengthen the infrastructure construction and the technology research, promote international cooperation, safeguard internet justice, build the image of China as a "responsible country" in the field of Internet, and overall enhance the international network security discourse power of China.

Key words: network security; discourse power; network attack; network crime; cyber war