【新闻与传播】

大数据时代我国网络安全治理:特征、挑战及应对

宋瑞娟

摘　要:网络安全治理体现了一个国家网络安全事业发展的方向和治理模式的变化。在大数据时代,我国网络安全治理呈现出内容繁杂、主体多元、主动防御、精准治理等特征。网络空间面临的国际竞争激烈、协同治理经验不足、数据安全问题凸显等一系列挑战,使得我国网络安全治理形势严峻。有鉴于此,我国应该从机制、战略、产业、技术、观念五个层面,促进多方协同合作,推动大数据战略发展,建立网络安全产业体系,注重科技创新和应用,加强网络安全意识的培养,以提升我国应对网络安全问题的能力,构建中国特色的网络安全治理模式。

关键词:大数据;网络安全治理;数据安全;主动防御

中图分类号:G206　　**文献标识码:**A　　**文章编号:**1003-0751(2021)11-0162-06

随着大数据时代的到来,网络犯罪、黑客攻击、数据泄露等网络安全事件频繁发生,造成巨大损失。据统计,自2018年以来,全球重大网络安全事件高达数十起,涉及金融、制造业、医疗、通信、教育等多个行业,严重威胁国家安全与社会稳定,频发的网络安全事件使网络安全治理成为世界各国不得不面对的问题。目前,我国正处于互联网快速发展阶段,成熟的网络安全治理措施与经验缺乏,网络安全事件不断发生。2020年12月,“蔓灵花组织”利用病毒邮件对我国政府部门和科研机构相关人员发起邮件攻击,扰乱了相关部门与人员的正常工作,造成难以估量的损失。2021年6月30日,依托大数据赋能的滴滴出行公司在美国纽交所突然上市,泄露了大量涉及我国城市交通、军事单位、医院、政府部门的地理信息以及个人隐私数据,对我国国家安全造成巨大的威胁。这些网络安全事件轻则泄露个人隐私,重则扰乱社会稳定、危害国家安全,我国网络安全治理迫在眉睫。本文深度挖掘大数据时代我国网络安全治理的内在特征,梳理网络安全治理面临的挑战,提出具有针对性的网络安全治理措施,以期为我国网络安全治理提供一些思路和方法,在此基础上形成具有中国特色的网络安全治理对策。

一、大数据时代网络安全治理的特征

在大数据时代,互联网的发展融合了大数据、云计算、人工智能等新技术,具有新的时代特征。互联网在迅速发展的同时也产生新的安全问题,网络安全治理的内容、治理的主体、治理技术以及治理模式等方面逐渐呈现出鲜明的时代特色。

1.内容复杂性

大数据时代一切皆可数据化,数据是基本的信息存储形式。海量数据隐藏的信息包罗万象,数据的整合能够促进不同领域的合作交流,组建一张资源大网,同时也增加了网络内容的复杂性。互联网的快速发展加速了数据的流动和信息的传播,信息之间的关联性错综复杂,耦合多种元素,内容庞杂,并由此出现了很多新的领域和行业。尤其是自媒体、短视频的出现,使得互联网内容生产和传播日趋多元,用户规模不断扩大,人人都可以在网络上表达自己的观点,由此产生的信息内容所引发的舆论关注远远超越传统媒介。随着互联网“生产模式和渠道日趋多元,内容的生产、传播和消费呈现出旺盛的

收稿日期:2021-08-27

作者简介:宋瑞娟,女,郑州轻工业大学马克思主义学院讲师,历史学博士(郑州　450001)。

势头,不良信息充斥其中,精品内容日益稀缺”。[①]不良信息甚至被反动势力恶意运用,煽动群众对政府的不满,影响社会的稳定和国家安全。由此催生了各种各样的网络安全问题,网络诈骗、钓鱼软件、网络病毒以及不断衍生的新型网络攻击方式,加大了网络安全治理的难度。

2.主体多元性

近些年,信息技术广泛应用到日常生活中,网络普及率更高。网络与人们的日常生活紧密相连,成为必不可少的工具。互联网改变了人们的生活方式,人们能够通过互联网传播获得新的认知和需求,这种网络化的传播生态拓宽了普通群众利益诉求和表达的渠道,使人们都有机会参与网络社会文化建设。互联网受众也从精英群体到包含不同地区、不同年龄层、不同领域的从业群体等,人人都可以成为互联网治理的一分子,政府、企业、网民等多主体参与网络空间治理,由此形成了治理主体多元的特性。在互联网的治理主体中,政府仍然占据主导地位,通过制定法律法规规范互联网运行。企业是网络安全治理的重要角色,尤其是高科技信息企业掌握大量的一手数据,能够快速应对潜在的安全威胁,并根据出现的网络安全问题提出具有针对性的解决办法,是网络安全治理的重要主体。截至 2021 年 6 月,我国网民规模为 10.11 亿,较 2020 年 12 月增长 2175 万,互联网的普及率达到 71.6%,手机网民规模大约 10.07 亿,网民使用手机上网的比例达99.6%。[②]广大网民成为网络安全治理必不可少、不可忽视的主体之一。

3.主动防御性

传统的网络安全治理具有滞后性,往往是网络安全事件发生之后,才采取措施进行补救,更多的是一种被动的防御措施。大数据、云计算等互联网相关技术的应用为网络空间治理提供了技术支撑,是网络安全治理能够进行主动防御的关键。其中,针对网络安全的大数据安全态势感知技术的出现,有助于构建主动的网络安全防御体系,提高网络安全防护的水平。安全态势感知技术能够迅速收集、整理网络空间的信息,通过对所收集海量信息的挖掘、分析、建模,有效预判网络态势的发展方向,判断危险事件发生的趋势和出现的概率,精准预警,提前做出防御方案,减少网络被攻击的风险。

频发的网络安全问题是推动主动防御发展的动力。现阶段网络安全问题频发,提前预测危险、主动进行防御能够减少网络安全事件的发生。尤其是在大数据时代,网络安全事件产生的消极影响不断升级,数据泄露导致的危害使得网络安全治理采取先发制人的方式进行预防,以降低危险,避免出现更大的安全风险。大数据时代网络安全治理与传统网络安全管理模式相比在技术方面有了明显的进步,使网络安全空间由被动防御向主动防御转变,提升了网络安全治理能力,能够有效地保护网络空间安全。

4.精准化治理

大数据时代里更多行业的发展依托大数据赋能,数据的融合、共享能够确保对治理对象进行综合分析,做出科学研判,提出具体且相对精准的解决措施。“精准治理主要以主动性、科学性、系统性为特征,基于知识管理创新和匹配,以实现可预知、可跟踪、可标准化等目标”[③],治理效果明显。大数据等技术的应用为精准治理提供了技术支持,改变了网络安全治理的模式,人们能够从碎片化的数据信息关联分析整体,对安全风险和即将出现的网络安全问题有更深入、全面的认识,网络安全治理呈现精准的模式特征。在新冠肺炎疫情期间,通过对病患和密切接触者的大数据流调,做到精准溯源,为疫情防控提供精准服务,迅速阻断疫情传播的源头和途径,对于及时控制疫情起到积极作用。此外,科学、系统地对数据治理主体的责任权属进行精确定位,能够明确安全责任,有助于政府、企业组织和公众承担起责任,共同合作应对安全风险,提出针对性的治理举措,快速提升网络安全治理的效率。

二、大数据时代我国网络安全治理面临的挑战

大数据与“互联网+”迅速发展的时代,数据化、智能化不断推进,在引领互联网向前发展的同时,也催生了新的网络安全问题。来自国际竞争的压力、协同治理经验不足和频发的数据安全问题构成了前所未有的挑战,这些挑战在大数据时代网络空间发展的过程中显得尤为突出,我国的网络安全治理形势仍然很严峻。

1.网络空间国际竞争激烈

在大数据时代,社会运行与国家发展严重依赖互联网的发展,网络安全直接关系到社会稳定与国家安全。作为非传统安全的重要内容,网络空间是世界各国权力暗中博弈的关键领域。首先是网络空

间话语权的争夺。在大数据时代,掌握足够多的网络空间话语权,对于未来国家的发展至关重要。网络主权和数字主权是影响国际竞争的重要因素,世界各国都认识到网络和数据的重要性,将大数据的发展提升到国家战略高度,纷纷加入争夺网络话语权的竞争中。西方反华势力利用其在网络空间的话语优势,传播抹黑中国的言论,以一种“审判者”的视角对中国的内政外交百般挑剔,阻碍中国正常的对外交往与合作。尤其是在新冠肺炎疫情期间,以美国为首的国家试图将新冠病毒溯源政治化,对我国进行政治施压,通过互联网传播虚假信息,伺机煽动民众不满,挑起国际矛盾和对抗。其次,中国与西方国家在意识形态上的差异,导致西方国家不断通过网络对我国进行意识形态渗透。网络空间是国际反华势力对我国攻击和渗透的重要途径,西方国家将网络空间当作维护和拓展意识形态和价值观的重要场域,长期打着自由、民主的旗号,频繁透过网络干涉我国内政,对我国进行意识形态的渗透。最后,互联网的匿名性与开放性使得网络霸权国家通过掌握的网络权,攫取我国的网络资源,建立垄断网络空间权力与资源分配的霸权,侵犯我国利益。以美国为首的西方国家对网络话语权的垄断以及有针对性的意识形态围困对我国的网络安全乃至政治安全威胁持续不断,扩大升级社会矛盾,严重威胁我国网络安全和人心稳定,使我国网络安全治理面临着巨大的国际压力。

2.协同治理经验不足

大数据时代的网络安全治理涉及多个部门和行业,想要实现社会各方力量快速有效地协同治理,需要的是打破行业壁垒。《中华人民共和国网络安全法》规定:“任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。”这明确规定了公民与社会组织等在保障网络安全、提升网络安全治理方面的责任和义务。在正常情况下,“网络主体的治理意向越共通、越具体,则网络生态治理的整体活力越高涨,越能形成合力”④。在实际运作方面,我国网络安全治理主要依靠政府的强制措施,缺乏多方协作共同治理的经验。现阶段网络空间仅依靠政府部门为主的治理不能适应网络现实发展需求,需要通过协作手段,联合不同部门、群体、社会组织及个人协同管理。

大数据时代网络技术的迅速发展和网络空间的复杂多变,暴露了国家网络安全治理能力的不足。大数据和互联网的发展解构了传统的以国家权力治理为主的模式,虽然我国已转变早期行政化的网络治理思路,正着力构建“党委领导、政府管理、企业履责、社会监管、网民自律等多主体参与,经济、法律、技术等多手段相结合的综合治网格局”⑤,但是政府在网络安全治理领域的资源和能力稍显不足。尤其是在立法方面,政府的政策法规与网络技术发展速度相比存在相对的滞后性,各种政策的执行过程中也经常出现偏差,因此仅依靠政府力量进行传统的安全治理不符合网络空间的发展需求,有待进一步优化与转变。企业缺乏承担网络治理的主体责任,各企业之间竞争激烈,往往以追求利益为目的,缺乏合作精神,忽视国家利益,容易因小失大。民众作为网络空间重要的参与主体,安全意识薄弱,主动参与网络安全治理的意愿不强。网络主体的心态和诉求不协调,导致主体之间没有形成具有共同意向的治理共同体。互联网治理主体与政府治理的深度融合,“有利于完善国家治理体系,提升国家治理的宽度和效率,促使政府为公民提供更好的公共产品和服务”⑥,是保障网络空间安全最有效的方式。然而,政府、企业、民众之间的配合出现脱节,容易导致信息不对称,不利于网络安全的有效治理。此外,这种多主体参与的特性,导致网络安全治理上存在“权责不清、履责不力,追责不严等问题,严重制约了治理效果的提升”⑦。

3.数据安全问题凸显

当前,人们通过对海量数据的分析能够轻松获得其背后的隐藏信息,如经济、城市建设、医疗、教育、交通等的发展,数据的价值凸显。我国更是将数据看作与土地、劳动力、资本、技术并列的重要生产要素,视其为国家基础性的战略资源,数据安全逐渐成为确保中国推进社会经济高质量发展的重要内容。数据的重要性引发各国争夺,加大了数据安全问题的严峻性,使数据安全问题凸显。

大数据技术的应用是一把双刃剑,一方面数据收集和爬梳功能强大,人们能够通过数据分析出其背后的隐藏信息,为社会经济的发展提供更多的技术支持和方向导引。另一方面,数据技术的发展和数据的可聚集性,加大了数据泄露的风险。大数据在医疗健康、金融、交通、教育等行业的应用,有利于这些行业通过大数据轻松获取客户信息,分析客户

的行为习惯和个人偏好,有针对性地开展商业行为,但也出现如“大数据杀熟”、数据贩卖等不良现象。同时信息的推送出现同质化、弱智化倾向,长此以往造成网民主观能动性认知减弱,思维活跃性降低。此外,数据引发的伦理问题受到广泛关注,“大数据技术的发展,改变了人们的生活、交往和思维方式,但同时使网络空间道德伦理问题进一步凸显”⑧。尤其是各类 App 的使用协议中的隐私协议往往包含霸王条款,强制获取用户信息,侵犯用户隐私。

数据的频繁跨境流动,加大了数据泄露的风险。2019 年,G20 峰会宣言强调:“数据的跨境流动在带来更高的生产力、更大的创新和更好的可持续发展的同时,也带来了与隐私、数据保护相关的挑战。”⑨数据具有易存储、易流通等特性,在促进社会经济发展的同时,也增加了数据泄露的安全隐患,强化数据治理已经成为确保大数据时代网络空间稳健发展的重要手段。此外,数据归属权的模糊增加了数据安全风险。数据在使用的过程中,不仅是生产要素,更附加了社会关系,但由于数据的收集、存贮、应用分属权不同,“数据应用的复杂性和数据分析挖掘的多样性增加了数据权属管理和抵御安全攻击的难度,另一方面,越来越多的跨组织间数据流通进一步加速了数据被盗用、误用、滥用的安全风险”⑩。此外,数据信息泄露成本小、传播快等特点使数据安全问题频发,提升了网络安全治理的难度。

三、我国网络安全治理能力的提升路径

目前,我国正处于从网络大国向网络强国转变的关键时期,网络安全事关我国网络强国建设顺利与否。因此,加强网络安全治理,规范网络行为,成为保障我国网络安全和国家安全、实现网络强国建设目标的必要举措。我国网络安全治理应从机制、产业、战略、技术、观念等多层面展开,全面提升我国网络安全治理的应对能力。

1.机制层面:建立多方合作机制

互联网具有高度全球化的特征,想要保障网络安全,必须要统筹国内和国际两个大局,团结利用一切力量。习近平指出:“互联网发展对国家主权、安全、发展利益提出了新的挑战,迫切需要国际社会认真应对、谋求共治、实现共赢。”⑪因此,我国应积极与世界网络强国合作,同时也要调动国内各方力量,统筹发展。

首先,中国应该积极寻求与其他国家的网络安全建设,加强网络安全对话,扩大共识,共同构建网络空间命运共同体。网络安全问题不分国界,世界各国通力合作才能更好地应对网络威胁,“加强各国之间的合作,制定共同适用的国际规则,形成有效的国际合作机制,是应对信息安全问题的必然途径”⑫。通过合作,可以借鉴学习他国网络领域先进的技术和管理经验,改善国际网络环境,积极主动争取网络空间话语权和主导权。其次,网络安全治理体系需要多主体共同协作,应对网络空间所出现的安全问题。对此,我国应处理好政府、企业、组织、个人之间的关系,统筹各方力量,促进资源在各行业之间的流转,实现资源共享,进而最大化确保网络空间的安全。因为只有打破行业限制,共享资源,互通信息,减少重复投入,才能调动各种资源优势,实现资源最大效用。此外,加强各方力量的协同配合,充分发挥各方的网络优势、技术优势和队伍优势,对资源进行有效的整合,共同协作推动网络安全治理,打击网络恐怖袭击活动,减少网络安全隐患。

2.产业层面:建立网络安全产业体系

我国拥有世界上最大的网络用户群体,网络空间的发展需要良好的网络安全环境,网络安全生态产业体系能够保障网络环境健康发展。据统计,2020 年我国网络安全产业规模达到 1702 亿元,增速约为 8.85%,呈现稳定的增长态势。⑬网络安全产业的发展,有利于提高网络安全系数。

基础设施是网络安全产业链发展的必要支撑。在我国网络安全产业发展过程中,产业基础设施建设跟不上大数据发展的步伐,相关配套和支撑性产业明显不足。我国应该在以下几个方面做出努力:第一,加大网络安全产业基础设施建设。在互联网发展过程中,我国应该紧跟时代步伐,面向互联网发展的现实需求,持续推进基础设施的优化建设,为网络安全产业链提供坚实的基础保障。第二,培育互联网高新技术企业,加强国家对网络安全技术的研发投入,突破核心技术,建立良好的数字生态体系和技术研发平台。第三,发挥互联网企业的行业主体作用,联合制定行业规则,调动各部门协同合作的积极性,健全数据要素市场秩序,规范数据应用和企业发展,积极参与网络安全治理。

3.战略层面:践行大数据战略

近些年,信息技术迅速发展,数据已经成为重要

的战略资源,社会的现代化建设与大数据的发展和应用紧密相连。数据的重要性使得世界各国纷纷将大数据确定为国家战略,并通过立法加强数据管理。如美国在 2012 年 3 月通过政府发布“大数据研发动议”,其目的是通过对采集来的庞大而复杂的数据进行分析,从中获得新的知识和洞见,加速科学发现,强化本土安全。⑭此外,英国、日本、澳大利亚、欧盟等国家和地区也陆续出台大数据战略,争取优势地位。我国自 2015 年以来开始推行大数据战略,在政策上给予重视,但如何更好地推动大数据战略的实施仍需继续探索。

推动大数据战略的实施应该从以下几个方面进行。第一,加快完善数字基础设施建设。数字基础设施是新基建的重要内容,也是推动大数据战略实施的基础动能。尤其是在社会不断向智能化、智慧化转型的过程中,以 5G 网络、工业互联网、智慧校园、智慧医院等为主的数字基础设施建设的作用凸显。第二,加快推进精准数据安全立法体系建设。数据立法是推行大数据战略的法律保障,近些年,我国逐渐认识到数据安全对网络安全和国家安全的重要性,不断在立法上保障数据安全和网络安全。如 2021 年 6 月通过的《中华人民共和国数据安全法》、2021 年 8 月通过的《中华人民共和国个人信息保护法》等,这些法律的推行对于保障数据安全和个人信息安全具有积极意义。然而,大数据时代网络安全面临的问题更加复杂、多元,仍然有很多安全漏洞需要法律去修复,需要持续推进、细致分类、精准立法。第三,提高数据治理能力。加强数据治理能力需要国家政策指导和政府部门发挥主体监管作用,推动数据流通、共享、整合,搭建数据沟通平台;企业协助参与治理,确保企业内部数据安全,优化数据安全保护系统,保障数据安全;个人要合法使用数据资源,做到文明上网,合法用网。

4.技术层面:注重网络科技创新

创新是社会发展的动力。习近平指出:“要深入实施工业互联网创新发展战略,系统推进工业互联网基础设施和数据资源管理体系建设,发挥数据的基础资源作用和创新引擎作用,加快形成以创新为主要引领和支撑的数字经济。”⑮一些重要的基建设施和有关国计民生的电网、交通、金融等领域深深依赖网络信息技术。信息技术和数字经济的发展离不开持续的技术创新和开发,先进的技术是确保网络安全治理的关键。其中人工智能技术的发展与运用能够有效地解决数据安全问题,促进网络安全生态智能系统发展。“新一代人工智能产业应用的驱动特征愈发明显,从生产方式的智能化改造、生活水平的智能化提升,到社会治理的智能化升级,都对新一代人工智能技术、产品、服务及解决方案有着旺盛的需求。”⑯

保障网络安全必须要依靠大数据、人工智能、量子计算等先进技术的支持,掌握核心技术,研发具有自主知识产权的互联网产品,以创新实现技术的突破。我国网络安全领域的许多核心技术较为落后,缺乏高端、自主的研发能力,网络安全产品和主要的防御技术大都来自国外,常常受制于人。与美国、以色列等创新强国相比,我国在科技创新、技术研发等方面仍有很大的提升空间。为改变科技创新不足、核心技术落后现状,我国首先应该建立完善的科技创新发展战略,以科技创新驱动网络安全建设,加强网络安全技术的自主研发,加大基础设施建设的投入力度。其次,着重提升我国网络科技创新水平,建立大数据实验室,探索数据技术的创新发展,研发具有自主知识产权和国际领先水平的安全技术产品,培养具有国际竞争力的网络安全创新团队和科技领军人才。最后,要提高技术革新和运用能力,加强大数据、人工智能等新技术在网络安全领域的应用。

5.观念层面:增强网络安全意识

网络安全意识对网络安全防护体系的建设十分关键,安全意识薄弱就可能引发严重的网络危机和网络安全问题。提升网络安全意识,“能够对潜在的网络安全威胁及时预警,提前制定对策,从预防的角度提高网络安全防范意识,降低网络安全风险”⑰。我们必须要认识到网络安全威胁与传统安全威胁的不同,提升民众的网络安全意识。首先,要树立起科学的网络安全观,通过宣传、教育提升公众安全认知。尤其需要注重学校教育,从小学开始开设网络安全课程,培养学生的安全意识和素养,在思维习惯、行为方式等方面提高网络安全意识。其次,要注重网络安全人才的培养。在我国,“网信领域除了技术人才的现实缺口,最为紧缺的还有应用型人才,中国在网络安全和信息化领域的人才数量和质量均不能满足现实需求”⑱。因此,想要实现网络强国战略,保障网络安全、培养网络科技人才是必要途径。最后,要调动群众的积极性,加强网络爱国主

义教育,培养民众对社会主义核心价值观的认同,抵御来自西方国家的意识形态侵蚀。

四、结语

在大数据时代,以大数据、人工智能、数字技术等为代表的新技术,推动国家发展向智能化、智慧化方向的转型,网络安全与国家安全的联系更加紧密。网络安全的重要性对网络安全治理提出了更高的要求,大数据时代网络安全治理体现出内容复杂、主体多样、主动防御、精准治理等特征。互联网在迅速发展的同时,不断衍生的新型网络犯罪形式等对我国网络安全治理产生挑战,因此,"要想有效地维护和捍卫国家安全和国家利益,就必须将国家安全治理界限向网络化和虚拟化拓展并不断延伸,采取合宜的治理策略来应对这种挑战"⑲。复杂的网络安全形势导致网络安全治理面临的挑战更加严峻,因此,我国必须要做出积极的应对措施。如建立多方联合的合作机制,加强网络安全产业链的发展,注重科技创新,提升网民的网络安全意识,这些措施的实施有助于全方位提升网络安全治理效率,更好地应对大数据时代日趋严峻的网络安全形势,确保社会稳定和国家安全。

注释

①王威:《大数据时代的互联网内容建设与治理》,《中国社会科学报》2018 年 5 月 7 日。②中国互联网络信息中心(CNNIC):《第 48 次中国互联网络发展状况统计报告》,2021 年 8 月,第 23 页。③王欣亮、任斐、刘飞:《基于精准治理的大数据安全治理体系创新》,《中国行政管理》2019 年第 12 期。④⑤阙天舒、莫非:《总体国家安全观下的网络生态治理——整体演化、联动谱系与推进路径》,《当代世界与社会主义》2021 年第 1 期。⑥陈潭、杨孟著:《"互联网+"与"大数据×"驱动下国家治理的权力嬗变》,《新疆师范大学学报》(汉文哲学社会科学版)2016 年第 5 期。⑦郭超:《大数据时代网络意识形态安全精准治理的三重向度》,《重庆邮电大学学报》(社会科学版)2021 年第 4 期。⑧张峰:《大数据时代隐私保护的伦理困境及对策》,《人民论坛·学术前沿》2019 年第 15 期。⑨G20 Information Centre. G20 Osaka Leaders' Declaration. June 29, 2019, http://www.g20.utoronto.ca/2019/2019-g20-osaka-leaders-declaration.html,2021 年 8 月 17 日。⑩中国信息通信研究院:《大数据白皮书(2020 年)》,2020 年,第 51 页。⑪《习近平向首届互联网大会致贺词》,新华网,http://www.xinhuanet.com/politics/2014-11/19/c_1113319278.htm,2014 年 11 月 19 日。⑫张新宝:《论网络信息安全合作的国际规则制定》,《中州学刊》2013 年第 10 期。⑬中国互联网协会:《中国互联网发展报告(2021)》,2021 年,第 26 页。⑭金江军、郭英楼:《智慧城市:大数据、互联网时代的城市治理》(第 4 版),电子工业出版社,2018 年,第 93 页。⑮习近平:《审时度势精心谋划超前布局力争主动　实施国家大数据战略加快建设数字中国》,《人民日报》2017 年 12 月 10 日。⑯中国互联网络信息中心(CNNIC):《第 47 次中国互联网络发展状况统计报告》,2021 年 2 月,第 78 页。⑰朱诗兵主编:《网络安全意识导论》,电子工业出版社,2020 年,第 121 页。⑱钱学森智库等组编:《2017 网信军民融合发展报告》,北京理工大学出版社,2018 年,第 158 页。⑲杨嵘均:《论网络虚拟空间对国家安全治理界限的虚拟化延伸》,《南京社会科学》2014 年第 8 期。

责任编辑:沐　紫

China Network Security Governance in the Era of Big Data: Characteristics, Challenges and Countermeasures

Song Ruijuan

Abstract: Network security governance reflects the development direction and governance model of a country's network security. In the era of big data, China network security governance presents the characteristics of complex content, multiple subjects, active defense and precise governance. Network security faces serious international pressures, insufficient collaborative governance experience, the urgent data security issues, which make China network security situation still grim. In view of this, our country should cooperate from the five levels of mechanism, strategy, industry, technology and concept, strengthen multi-agent collaboration, promote the development of big data strategy, establish a network security industry system, focus on technological innovation and application, and strengthen the cultivation of network security awareness, so as to improve our country's ability to deal with network security issues, and form a unique network security governance model with Chinese characteristics.

Key words: big data; network security governance; data security; active defense