

美国网络安全审查制度发展、特点及启示

张孟媛¹, 袁钟怡²

(1. 国际关系学院, 北京 100091;
2. 国家计算机网络与信息安全管理中心, 北京 100029)

摘要: 美国建立的网络安全审查机制, 针对网络安全审查不仅有较为完备的立法, 还依托专门审查机构构建了全方位、强制性的审查程序, 并将网络供应链安全审查上升至国家战略高度。美国的网络安全审查机制具有内容广泛、审查严苛、标准模糊等特点。考察美国网络安全审查机制背后的路径选择、顶层设计和制度体系, 对完善我国网络安全审查制度有一定参考意义。

关键词: 美国; 网络安全审查; 网络安全; 国家安全

中图分类号: D73/77

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019057

Evolution, characteristics and revelation of the US cyber-security review system

ZHANG Mengyuan¹, YUAN Zhongyi²

1. University of International Relations, Beijing 100091, China
2. National Computer Network Emergency Response Technical Team/Coordination Centre of China, Beijing 100029, China

Abstract: As the founder of the global internet, the United States has established a well-structured cyber-security review system. It is based on a series of systematic and complete laws, regulations, and has constructed independent and efficient organizations. Such all-around and compulsory system is structured with distinctive characteristics, such as the extension and the procedure of the review in an orderly way, the vague standard and the compulsory results. Thus, it has certain reference significance to the establishment of a sound Chinese cyber-security review system.

Key words: the United States, cyber-security review system, cyber-security, national security

收稿日期: 2019-05-06; 修回日期: 2019-07-08

通信作者: 张孟媛, nancy-zmy@163.com

基金项目: 教育部人文社会科学研究规划基金资助项目 (No.15YJAZH108)

Foundation Item: Social Science Research Project Funded by Ministry of Education of China (No.15YJAZH108)

论文引用格式: 张孟媛, 袁钟怡. 美国网络安全审查制度发展、特点及启示[J]. 网络与信息安全学报, 2019, 5(6): 1-9.
ZHANG M Y, YUAN Z Y. Evolution, characteristics and revelation of the US cyber-security review system[J]. Chinese Journal of Network and Information Security, 2019, 5(6): 1-9.

1 引言

第43次《中国互联网发展状况统计报告》显示,截至2018年12月,中国网民规模达8.29亿人,普及率达59.6%^[1],已是名副其实的网络大国。但我国还不是网络强国,随着中国向目标要求更高的网络强国努力迈进,我国网络安全风险仍然持续高企。根据国家互联网应急中心《2018年我国互联网网络安全态势综述》报告,2017年我国境内感染计算机恶意程序的主机数量约1 256万个,移动互联网恶意程序数量超过253万个,收录安全漏洞数量15 955个^[2],网络安全总体形势不容乐观。为维护我国网络空间主权、安全和发展利益,中央网络安全和信息化领导小组办公室于2016年12月发布了《国家网络空间安全战略》,明确了以总体国家安全观为指导,实现网络强国的总目标,并宣布将“建立实施网络安全审查制度,加强供应链安全管理,对党政机关、重点行业采购使用的重要信息技术产品和服务开展安全审查”^[3]。相比之下,美国作为互联网强国和霸权国家,针对互联网和网络产品供应链早已建立起较为完备的安全审查机制,认真研究其有关制度、机制和考察期发展过程,在当今中美贸易摩擦、美国频频以国家安全为由对我国企业发难的背景下,有很强的学术借鉴意义和现实参考性。

2 网络安全审查的内涵与外延

习近平总书记指出“没有网络安全就没有国家安全,没有信息化就没有现代化”^[4],全面阐明了网络安全和国家安全的辩证关系,将网络安全纳入总体国家安全观统筹考虑。网络安全审查在很大程度上已经成为实施国家安全审查最主要的依托和手段。囿于国家安全的特殊性、其概念本身很大程度的宽泛性与不确定性,目前对于国家安全审查和网络安全审查的概念尚无权威一致

的定义,由于各国在网络安全内涵外延认知的不同,在涉及网络安全审查问题时很少直接使用网络安全审查的术语,而一般采用国家安全审查的概念。网络安全审查在多数情况下可以认为是针对计算机、互联网产品和服务的国家安全审查。

一般而言,网络安全审查是指为维护一国政府机构和关键信息基础设施的网络安全,在政府和关键信息基础设施的计算机软硬件设备、系统、网络、应用和服务的采购、运营和管理过程中进行的,运用特定网络安全测试、采购商资质考察等方式进行调查、评估和审核的过程。其中,关键信息基础设施的定义因各国根据自己对国家利益的评估而确定,通常包括政府机构、通信、电力、能源、金融等部门。而网络安全审查概念常常可能与信息安全审查概念发生冲突。对此,在具体的探讨中存在两类观点:一类是将信息安全审查等同于网络安全审查,另一类是将外资并购过程中的国家安全审查纳入网络安全审查制度中。两种观点均有一定道理。在2014年中央成立网络安全和信息化领导小组之前,信息安全概念通常与网络安全混用,其在宏观上的含义基本相同。而外资并购国家安全审查制度可以认为是一种广义上的网络安全审查。外资并购过程中实施的国家安全审查主要目的是通过政府干预,通过“合理怀疑”降低外国资本对美国的影响,主要着眼点在于国家经济安全,而计算机与电子产品则是受审查最多的行业^{[5]注1}。根据2008年8月1日颁布的《中华人民共和国反垄断法》,我国针对外资并购已经建立国家安全审查制度^[6]。具体看来,针对网络安全产品和服务的审查聚焦于技术层面。而针对外资并购的审查通常关注的是资本进入的风险,更关注经济层面。美国外资并购的国

注1:2008—2012年,制造业领域受CFIUS管辖的交易数为223起,占同期受管辖总交易数的41%。制造业中,计算机和电子产品行业占比45%。

家安全审查制度无疑为其网络安全审查制度的建立打下了良好的基础和提供了有益借鉴。由此，美国通过政策立法、机制保障、技术手段等多个层面推出系列举措，建立了较为完备的网络安全审查制度。

3 美国网络安全审查制度的建立

美国是网络安全审查制度的先行者。经过多年的立法实践和政策完善，美国已经从政策立法、机制保障、技术手段等多方面构建起了较为完善的网络安全审查制度。

3.1 循序渐进，逐步构建完备的政策立法

立法是一个国家和社会存在的根基，美国网络安全审查制度的构建同样遵循了这一路径。1950年，美国通过了《国防生产法》，赋予了总统对外国投资行使安全审查的权限。1988年，美国国会通过《埃克森-弗罗里奥修正案》(Exon-Florio amendment to the defense production act)，强化了总统审查外国对美投资的权力^{注2}。1988年，美国总统里根发布行政令，授权由外国对美投资委员会(CFIUS, The Committee on Foreign Investment in the United States)负责开展外国投资的安全审查，并就是否应当组织外国投资向总统提供建议。2007年，美国国会正式通过《2007年外国投资和国家安全法》，确定了外国对美投资委员会的结构、职责和审查程序，进一步提高该委员会的审查权限和审查范围，并要求委员会对所有“由外国政府控制或所有的经济实体的对美投资活动”开展国家安全审查^{注3}。该法案同时确定了部门牵头制度，即在每个外资对美投资

并购过程中，财政部部长应当指派一个或多个部门的代表牵头负责，代表外国对美投资委员会与外国投资方进行谈判协商。一般而言，牵头部门应当是并购交易所在领域的主管部门^[7]。2008年，时任美国总统小布什签署第13456号总统行政令，对外国对美投资委员会成员的构成进行了进一步明确。根据该行政令，委员会由11名成员组成，其中9名来自财政部、商务部的成员拥有投票权，2名成员为劳工部部长和国家情报总监，可以提出建议但无投票权。该行政令同时设立5名观察员负责全程参与和监督委员会活动，并随时向总统汇报情况^[8]。2018年8月13日，特朗普签署《2019财年国防授权法》(NDAA, The national defense authorization act)，其附带《美国外国投资风险审查现代化法》获得通过。《美国外国投资风险审查现代化法》进一步强化了网络安全审查机制，扩大了外国对美投资委员会成员管辖权限，并将特定类型的交易引入强制申报流程，还特别提出要重点并区别对待来自中国的投资^[9]。

3.2 专设机构，建立严苛完善的审查机制

根据美国《2007年外国投资和国家安全法》和《2018年外国投资审查现代化法》，美国网络安全审查的牵头机构是外国对美投资委员会，该委员会负责对拟向美国联邦政府部门、特别是国防部门提供的云计算等信息技术产品和服务的企业进行安全审查^[10]。委员会职责是就外国对美投资开展审查、调查、做出决定，并向总统提出建议。委员会受国会的监督和管辖，由财政部部长负责召集，其成员来自财政部、贸易代表办公室、国防部、商务部、司法部、能源部和国土安全部等部门，并根据需要增加来自总统经济顾问委员会、白宫管理和预算办公室、国家安全委员会和国土安全委员会的成员。在涉及具体的外资并购项目审查过程中，总统和财政部长可依据具体的专业领域邀请有关部门负责官员参与审查过程，

注2：该法亦称《外国投资、国家安全和核心商业修订案》(Foreign investment, national security and essential commerce amendment)，是美国规制外资并购的基本法。

注3：1975年，美国总统福特签署11858号总统行政令，专门成立了外国对美投资委员会，委托其对外国投资方进行监管和分析。

以便实现审查的专业性和有效性。与此同时,委员会下设美国总统关键基础设施委员会、国家基础设施咨询委员会和信息分析与基础设施保护局3个专设机构。多部门统筹协调是外国对美投资委员会行使职能的突出特点,从而最大限度地加强了外国对美投资委员会审查的专业性,尽量避免决策的主观性和片面性。此外,在技术性审查方面,美国联邦政府的云计算产品和服务安全审查是由国防部、国土安全部和审计署组成的联合授权委员会(JAB)共同依法开展,联合授权委员会负责制定要求,审批第三方评估机构认可准则并做出审查决定。

3.3 强化标准,形成全面完善的技术支撑

2015年,美国率先明确了全球供应链安全审查具体要求,明确规定美国财政部、贸易代表办公室、商务部等部门应当依据美国国家标准与技术研究所(NIST)制定的国家标准开展供应链安全风险审查^[11]。美国NIST是美国网络安全审查技术标准的制定者和推广者。2011年,美国NIST颁布《公有云计算安全和隐私指南》和《完全虚拟化技术安全指南》两项标准,为美国政府开展云计算服务安全审查提供了技术标准和执行依据。2013年和2015年,美国国会相继通过《提高关键基础设施网络安全法》和《网络安全信息共享法》,进一步确定了NIST在制定安全标准中的权力和责任。2014年,美国NIST公布《提高关键基础设施网络安全框架1.0版》,向包括联邦政府在内的所有公共和私营部门开放安全技术标准指南建议,试图将国家制定的网络安全技术标准推广整个美国^[12]。为配合执行相关技术标准,美国国防部、国家安全局等部门成立了全球供应链风险评估机构,商务部则成立了由40人组成的供应链竞争顾问委员会。

3.4 令行禁止,明确强制审查的安全规范

目前,美国的网络安全审查已经实现了对联

邦政府机构系统、国防系统和国家安全系统的全覆盖。2000年,美国国家电信与信息系统安全委员会(现国家安全系统委员会)发布11号文件,规定拟进入国家安全部门使用的网络安全产品及相关服务,必须经过国家信息保障联盟(NIAP)通用准则框架下的风险评估和认证^[13]。相关产品涵盖入侵检测、防火墙、操作系统、数据库管理等多个类别。2008年,美国国会通过的《外国人兼并、投资和收购规则》进一步明确,外国投资者必须依据美国国家安全审查制度,自愿或强制向美国的外国对美投资委员会申报投资并购的有关细节,没有通过国家安全审查则不能开展投资并购活动^[14]。2011年,白宫行政管理和预算局制定并正式实施《联邦风险和授权管理计划》(FedRAMP),将开展网络安全审查作为联邦所有政府部门的应尽义务,强制要求各部门依据有关标准对云计算产品和服务安全开展风险评估、授权与过程监管。为此,美国在《云计算环境信息系统安全授权》《联邦风险及授权管理计划》和《联邦信息安全管理法案》(FISMA)等立法和标准的框架下,组建了由国防部、国土安全部和审计署三方共同构成的联合授权机构,负责对有资质开展安全风险评估的第三方机构开展认证工作,并统筹联邦政府云计算服务安全基线标准规范。

3.5 全局统筹,供应链安全上升为国家战略

网络安全所涉及的计算机软硬件设备和技术服务范围非常广泛,牵涉的人员也非常复杂,有系统终端用户、采购专家、系统集成商、网络提供商、软硬件提供商以及政策制定者^[15]。真正的网络安全有赖于对全产业链的人和物开展监督和管理,开展全面审查的难度极大。美国政府采购的信息技术产品和服务来自全球,为了监控其网络安全情况,控制安全风险,2012年,奥巴马政府发布了《全球供应链安全国家战略》,要求在信息网络环境下,构建一个有韧性的全球供应链,

以实现美国在商贸服务高效的同时,最大可能维护网络安全。《全球供应链安全国家战略》首次以顶层设计文件的形式确立了美国网络安全审查的对象和范围,表达了美国对于全球信息技术产品供应链威胁的重大关切,提出联邦政府应当了解并解决企图引入有害产品或材料的系统开发和由恶意攻击、事故或自然灾害引起的中断导致供应链脆弱性,同时明确说明其重点不仅是全球交通、邮政网络以及运输途径、资产和可以确保货物从生产到送至最终消费者的基础设施,还有配套通信的设施及系统^[16]。为了控制联邦政府网络和关键基础设施的网络安全风险,美国提出强化国内标准与法律规范,改善全球供应链治理结构,加强全球供应链系统风险的识别与评估,加强供应链过程透明化管理,加强区域合作和全球资源整合等具体目标。此外,美国政府还成立了跨部门全球供应链工作小组,负责开展包含网络安全领域的网络安全风险评估,并向总统做出报告和改善建议。具体来说,美国所实施的各项网络安全审查行动已经不是单一产品、单一服务甚至单一投资并购项目的技术性安全审查,而是站在全球供应链管理视角开展的多维度网络安全风险评估,除了针对有关设备关键模块的漏洞、后门检测外,还纳入与产品和服务相关的物理安全、工具安全、持续监控、安全人员安全以及制度安全等全产业链、全生产周期的审查和评估。

4 美国网络安全审查制度的主要特点

由于多年来不断改进,美国已经形成了较为完整的网络安全审查制度,相关法律、政策、标准不断健全完善,工作机制已经趋于稳定。具体来说,主要呈现出以下特点。

(1) 范围持续扩大:从政府采购到全球供应链安全管理

美国网络安全审查的范围渐进拓展,从国家

安全系统的信息技术产品延展至国防供应链、联邦政府云计算服务等,逐步构建了系统性、综合性强的审查机制。在政府采购涉及的网络安全审查方面,美国国家安全系统委员会(CNSS)发布的《国家信息安全保障采购政策》明确规定,美国国家安全系统使用的信息技术产品、信息安全产品及有关产品必须经过国家信息保障联盟(NIAP)通用准则评估与认证体系(CCEVS)框架下的风险评估和认证^[17]。在联邦政府部门和有关机构的采购过程中,必须从美国国家信息保障联盟审查通过的产品清单中选择符合国家安全要求的产品,相关产品包括防火墙、入侵检测设备等信息安全产品以及操作系统、数据库系统等计算机软硬件产品^[18]。美国国家信息保障联盟负责定期更新符合网络安全要求的产品清单。

在外国对美投资的网络安全审查上,由外国对美投资委员会负责对涉及美国关键基础设施、关键技术资源的外国对美投资并购开展网络安全审查。委员会审查的项目主要有两方面:一是对产品和服务的安全性本身进行开展技术性审查;二是出于美国国家整体安全和利益考量,对外国投资企业、研发和生产历史、高管和员工等进行更为严苛的背景审查。在通过委员会的初步审查之后,外国的投资企业还必须与美国国防、安全等部门签署安全协议,要求有关企业的信息基础设施必须位于美国境内,所有的数据存储、交换和采集也都必须在美国境内进行。如果出现外国政府要求该企业提供或采集数据的情形,相关企业必须事先获得美国包括国防、安全以及对口部门的批准,并配合美国政府部门对这一流程进行监管。此外,如果遇到涉及外国政府控股或有外国政府背景的企业对美开展投资并购活动时,委员会更加审慎,会充分考虑该国政府与美国的关系,通常视政治需要决定审查是否通过。

在联邦对全球产业链的网络安全管控方面,

2008 年美国白宫发布的《国家网络安全综合计划》中明确：要制定多措并举的全球供应链风险管理方法，对本国和全球的供应链进行从产品、系统和服务整个生命周期的风险管理^[19]。据此，美国《2011 财年国防授权法案》中明确规定，国防部有针对其信息技术产品采购过程中开展供应链风险审查的权利和职责^[20]。为此，国防部专门制定了《国防采购系统运行》文件，进一步明确了国防采购的权责机构和软硬件采购的详细流程^[21]。

(2) 机制日臻完善：从产品技术审查到企业背景审查

《全球供应链安全国家战略》为美国政府开展网络安全审查提供了最基本的战略指引，将美国的网络安全和国家安全着眼点扩大至全球，并逐渐在此基础上构建起一套从产品审查到企业审查的完整机制。首先是着眼大局，建立起全方位的安全风险控制机制。继 2014 年美国国家标准和技术研究所公布《提高关键基础设施网络安全框架 1.0》，2018 年 NIST 再次公布《提高关键基础设施网络安全框架 1.1》^[22]，试图将美国联邦的网络安全技术标准和政策标准推广到所有私营部门运营的关键基础设施之上，敦促更多的企业和个人根据政府制定的安全标准来审查和运营自己的网络基础设施。其次是抓住要害，对进入联邦政府网络和要害部门计算机网络系统的产品进行严苛的安全审查。以国防部为例，该部门必须从美国国家信息保障联盟审查通过的产品清单中选择符合国家安全要求的产品，并在采购过程中有权以安全风险为由拒绝相关产品的采购而不说明原因。通过运用“白名单”机制，最大限度地控制网络安全风险来源。同时，不断更新相关准入产品的清单，以适应技术发展和系统升级的需要。第三是御敌门外，通过外资进入美国之前的审查，将对国家安全可能带来风险的外国企业排除在外。一般投资审查均遵循“国家安全例外原则”，

安全审查可由美国总统或外国对美投资委员会成员发起，也可以由交易双方依法申请，并向委员会提交书面的申报材料。如果存在满足强制要求申报情形而交易双方均不主动申报的，委员会将主动发起对有关交易的审查，以规避相关风险。通常其审查期限为 30 天，但可能延长。如果被委员会认定不会对国家安全产生威胁，那么相关交易即可继续进行，如果存在任何可能威胁国家安全的苗头或现象，则该交易会进入至少 45 天的详细调查期。在涉及外国政府控制的企业进行对美投资或涉及美国关键基础设施的投资方面，将可能有更长的调查时间和流程。如果未通过，则相关投资并购案会立即终止，所涉及有关企业的产品和服务也不能进入联邦政府采购的目录中。

(3) 标准严重模糊：从安全管理到政治工具

美国国家安全审查遵循逐案审查机制，审查标准存在严重模糊、缺乏透明等问题，且因国家安全概念解释的随意性过大而饱受诟病。首先是审查的范围广，跨度大。根据 2000 年美国国家安全系统委员会发布的《国家信息安全保障采购政策》，涉及国家安全应当是涉及联邦政府部门的涉密信息及军事、情报等敏感信息系统的技术产品及服务。相关标准由美国国家标准技术研究所、国家信息保障合作联盟和美国国家安全局进行确定^[23]。然而，到 2007 年《外国投资与国家安全法》，国家安全概念被扩大到涉及美国关键基础设施、关键技术资源等方面，由外国对美投资委员会来自由裁量是否符合国家安全标准。到 2013 年，美国政府再次对关键基础设施进行分类，将通信、信息技术、金融服务、核设施、交通运输等 16 个行业领域界定为关键基础设施，其网络安全审查覆盖的范围进一步泛化和模糊化。其次是流程复杂，缺乏透明度。根据美国的安全审查流程，正式的审查程序包括依法申报、初步审查、正式调查和总统决定 4 个流程。安全审查没有明

确时间限制,在完成后会选择性公开一部分信息,但非常有限,委员会不提供审查通过与否的判定依据,也不受理进一步申诉。事实上,在外国对美投资委员或掌握巨大自由裁量权的情况下,网络安全审查在多数时候已经沦为美国处于政治需要,为外国企业针对性设置投资准入壁垒、控制外资进入本国金融、能源、交通等领域的手段。出于配合美国总统或有关部门的政治需要,委员会通常采用拒绝接受申请材料、拖延调查时间等方式刻意为外国企业进入美国设置“隐性壁垒”,其审查的方式、节奏、时间、效率,完全由美国总统或者有关部门负责人掌控。多数情况下,宣布对外国投资并购案启动国家安全审查一开始,就已经给外国投资进入美国判了死刑,或已经沦为本国政府对外讨价还价的筹码。第三是针对中国的趋势明显。随着中美贸易摩擦在2018年集中爆发,开展外资安全审查已经成为美国借以打压中国的政治工具。中兴、华为的在美投资和销售活动历来是美国重点审查和刻意刁难的对象。而2018年《美国外国投资风险评估现代化法》提出,外国对美投资委员会应每两年提交一份关于中国在美国投资情况的报告。其关注的重点审查领域包括飞机制造、电脑存储制造、某些导弹及空间行业、电池制造、生物技术、纳米技术、半导体设备等在内的27项关键技术^[24],几乎涵盖了《中国制造2025》的所有领域,配合贸易摩擦打压中国的意图极其明显。

5 美国网络安全审查制度的启示及建议

“程序正义”历来是美国政治和法律推崇的最高标准之一。尽管安全标准在其网络安全审查中仍然有很大随意性,但只要程序公开、透明、合法,有明确的法律依据,就可以证明其正当性。有了明确的法律法规和完备的执行程序,一方面为有关部门具体执行提供了明确的法律依据,另

一方面为各类外交场合开展对外合作博弈提供了合法性基础。我国已通过立法形式初步明确了建立网络安全审查制度的方向。《中华人民共和国国家安全法》第59条明确规定:“国家建立国家安全审查和监管的制度和机制,对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目,以及其他重大事项和活动等进行国家安全审查,以便有效预防和化解国家安全风险”^[25]。《网络安全法》第35条明确规定:“关键信息基础设施的运营者采购网络产品和服务,可能影响国家安全的,应当通过国家网络信息部门会同国务院有关部门组织的国家安全审查”^[26]。与美国相比,有关制度规章仍在发展之中,涉及的具体机制也在形成过程中。具体而言,可以从以下4方面推动相关法律和制度进一步完善。

(1) 进一步完善和理顺相关立法

目前,《中华人民共和国国家安全法》和《中华人民共和国网络安全法》这些上位法已经为实施网络安全审查提供了明确的依据。在具体实施过程中,应当进一步完善下位法,注意与外资准入安全审查、网络安全产品认证、网络安全等级保护、政府采购等有关法律和制度规定进行衔接,明确有关部门在相关工作中的权责。此外,对于《网络安全法》规定的网络关键设备和网络安全专用设备的界定,应当尽快制定相关实施细则,出台相关产品服务指南或名录。

(2) 完善网络安全审查工作机制

根据2017年中华人民共和国国家互联网信息办公室公布的《网络产品和服务安全审查办法(征求意见稿)》,网络安全审查的实施机制是由国家网信办会同有关部门成立网络安全审查委员会,负责审议国家网络安全审查的重要政策,统一组织网络安全审查工作,协调网络安全审查相关的重要问题^[29]。在安全审查的具体工作中,需

要平衡国家关键基础设施网络安全风险评估检查和等级保护测评和检查机制,并建立第三方专业检测机构认证机制,以帮助跨部门联合审查机制更加高效、专业运行。

(3) 优先开展政府内部网络安全审查试点

随着云计算、大数据等基础设施建设的快速发展,政府部门正在更多采购和利用云计算服务来运行政务信息系统,其所承载信息系统的网络安全直接关系到国家安全。建议以党政机关及所属企事业单位为切入点,率先开展内部网络安全审查试点,制定相关采购及安全测评技术标准,在试点中逐步积累经验,再进一步向其他关键信息基础设施和行业推广。

(4) 以全球供应链视角审视网络安全审查

美国网络安全审查的标准和方式有很大的随意性,特别是外国对美投资过程中,夹杂了很多政治要素、经济利益考量。我国应当借鉴相关经验,以全球供应链视角审视网络安全审查,将网络安全管理渗透到信息技术产品生产的全生命周期,将技术审查、产品审查、资质审查、企业审查全面结合,并以立法的形式予以确认,在维护我国关键信息基础设施安全的基础上,最大限度地维护我国网络空间主权、安全和发展利益。

6 结束语

随着互联网及有关信息技术新应用的普及,网络安全已成为事关国家安全的重大战略问题。美国在网络安全审查的研究、立法和实施方面已取得了许多成果,而我国的网络安全审查制度和实践才刚刚起步,需要进一步实践和发展。构建中国特色的网络安全审查制度,应当在借鉴美国有关经验基础上,从我国国情和网络空间战略利益出发,以网络强国为战略总目标,有依据、有步调、有力度地逐步展开,构建既符合发展需要又能保障安全的网络安全审查制度体系。

参考文献:

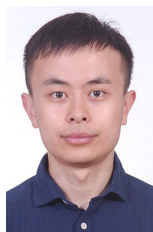
- [1] 中国互联网络信息中心. 第 43 次中国互联网络发展状况统计报告[EB]. 2019-4-30.
China Internet Network Information Center. The 43th report on the current development of china Internet network[EB/]. 2019-4-30.
- [2] 国家互联网应急中心网站. 2017 年中国互联网络网络安全报告[EB]. 2019-4-30.
National Computer Network Emergency Response Technical Team/Coordination Center of China Website. China Internet cybersecurity report 2017[EB]. 2019-4-30.
- [3] 中国网信网. 国家网络空间安全战略[EB]. 2019-2-1.
China Cyberspace Network. Strategy on national cyberspace security[EB]. 2019-2-1.
- [4] 人民网. 习近平的网络观: 没有网络安全就没有国家安全[EB]. 2019-4-3.
People.cn. Xi Jiping's view of the network: without cybersecurity, no national security[EB]. 2019-4-3.
- [5] 杨长湧. 美国外国投资国家安全审查制度的启示及我国的应对策略[J]. 宏观经济研究, 2014(12): 33.
YANG C Y. Revelation of us national security review system on foreign investment and china's coping strategy[J]. Macroeconomics, 2014(12): 33.
- [6] 中国政府网. 中华人民共和国反垄断法第 25 条[EB]. 2019-4-1.
English.gov.cn. Antimonopoly law of the people's republic of china, article 25[EB]. 2019-4-1.
- [7] Executive Order 13456[EB]. 2019-4-1.
- [8] 美国总统行政令 13456 号. Further amendment of executive order 11858 concerning foreign investment in the United States [EB]. 2019-4-1.
Executive Order 13456. Further amendment of executive order 11858 concerning foreign investment in the United States [EB]. 2019-4-1.
- [9] 美国国会网站. Foreign investment risk review modernization act of 2017[EB]. 2019-4-1.
US Congress Website. Foreign investment risk review modernization act of 2017[EB]. 2019-4-1.
- [10] 美国国会网站. Foreign investment risk review modernization act of 2017[EB]. 2019-4-1.
US Congress Website. Foreign investment risk review modernization act of 2017[EB]. 2019-4-1.
- [11] 美国白宫网站. National strategy for global supply chain security[EB]. 2019-5-5.
White House.gov. National strategy for global supply chain security[EB]. 2019-5-5.
- [12] 美国国家标准和技术研究所网站. Framework for improving critical infrastructure cybersecurity version1.1[EB]. 2019-4-1.
US National Institute of Standards and Technology Website. National strategy for global supply chain security[EB]. 2019-5-5.
- [13] Committee on national security systems frequently asked questions[EB]. 2019-4-1.
- [14] Regulations pertaining to mergers, acquisitions, and takeovers by foreign persons[EB]. 2019-4-1.
- [15] OLSIK J, MCKNIGHT J, GAHM J. Assessing cyber supply chain security vulnerabilities within the U.S[R]//Critical Infrastructure.

- Enterprise Strategy Group. 2010: 10.
- [16] 美国白宫网站. National strategy for global supply chain security[EB]. 2019-5-5.
White House.gov. National strategy for global supply chain security[EB]. 2019-5-5.
- [17] Committee on national security systems frequently asked questions[EB]. 2019-4-1.
- [18] About NIAP[EB]. 2019-4-3.
- [19] 美国白宫网站. The comprehensive national cybersecurity initiative[EB]. 2019-4-3.
White House.gov. The comprehensive national cybersecurity initiative[EB]. 2019-4-3.
- [20] National defense authorization act for fiscal year 2011[EB]. 美国国会网站. 2019-4-3.
US Congress Website. National defense authorization act for fiscal year 2011[EB]. 2019-4-3.
- [21] Operation of the defense acquisition system[EB]. 2019-4-3.
- [22] 美国国家标准和技术研究所网站.
US National Institute of Standards and Technology Website. Framework for improving critical infrastructure cybersecurity version1.1[EB]. 2019-4-1.
- [23] National information assurance acquisition policy[EB]. 2019-4-3.
- [24] 搜狐新闻. 美国对外国投资监管审查的新规落地[EB]. 2019-4-30.
Sohu News. New rules of US regulatory review of foreign investment put into practice[EB]. 2019-4-30.
- [25] 全国人大网站. 《中华人民共和国国家安全法》[EB]. 2019-4-30.
NPC Website. Cybersecurity law of the People's Republic of China[EB/OL]. 2019-4-30.
- [26] 全国人大网站. 《中华人民共和国网络安全法》[EB]. 2019-4-4.
NPC Website. Cybersecurity law of the People's Republic of China[EB]. 2019-4-4.
- [27] 中国网信网. 《网络产品和服务安全审查办法》[EB]. 2019-4-30.
China Cyberspace Network. Measures for the security review of network products and services[EB]. 2019-4-30.

[作者简介]



张孟媛（1974—），女，河北乐亭人，博士，国际关系学院副教授，主要研究方向为美国社会文化研究。



袁钟怡（1989—），男，山西晋中人，国家互联网应急中心助理研究员，主要研究方向为互联网治理、网络政策研究。