IT 供应链安全 ：国家安全审查的范围和中国应对

马民虎　马　宁
（西安交通大学 法学院，陕西 西安 710049）

摘　要 ：IT 产品和服务供应的全球化在客观上增加了 IT 供应链的复杂程度，不安全或恶意的 IT 产品和服务将有更多的渗透渠道，特别是国家关键基础设施愈发依赖 IT 产品和服务的安全性，建立 IT 供应链国家安全审查成为必然趋势。但目前各国基于国家安全的审查活动存在范围模糊、审查过程不透明的现象，需要通过立法加以矫正。为了弱化因技术依赖性产生的国家安全威胁，避免因 IT 技术控制不对等而对我国科技创新自主能力造成的损害，我国需要采取必要的应对措施。在综合国家安全观的视域下重新理解国家安全的内涵，以“ 合作包容 ”的理念指导安全审查的立法建设，并对审查范围进行“ 深度 ”和“ 广度 ”的扩展，对现行的相关立法进行调整。

关键词 ：IT 供应链安全 ；国家安全 ；信息安全 ；国家安全审查

作者简介 ：马民虎（1958— ），男，陕西周至人，西安交通大学法学院教授、博士生导师，主要从事信息安全法研究 ；马宁（1984— ），男，河北保定人，西安交通大学法学院信息安全法专业博士生，主要从事信息安全法研究。

基金项目 ：国家社会科学基金项目“ 网络安全监控的法律对策研究——以通讯协助执法法律制度的构建为视角 ”（项目编号 ：10XFX009）的阶段性成果。

中图分类号 ：D913.4　文献标识码 ：A　文章编号 ：1001-4403(2014)01-0090-06　收稿日期 ：2013-10-10

在 IT 采购全球化的态势下，IT 供应链安全与国家安全的关系愈发密切，通过 IT 产品进口安全审查、IT 产品安全性测试评估、外资国家安全审查等措施确保 IT 供应链安全已经成为各国普遍采用的管制手段。但现实发生的案例使国家安全审查与政治审查的关系变得模糊不清①，严重扭曲了 IT 国际供应链安全的国家管控体制。IT 供应链国家安全审查应当秉持必要的基本理性，避免滥用国家安全审查阻碍贸易自由，防止盲目排外与充斥“ 不信任 ”的国家安全审查阻断关键 IT 产品和服务的提供。为此，IT 供应链国家安全审查必须通过立法设置权力边界，明确审查活动的范围，提高审查活动的透明度，以确保国家安全审查活动的正当性。

一、IT 供应链国家安全审查的缘起

近年来，“ 脆弱性成为全球供应链安全较为突出的问题 ”[1]，针对 IT 供应链进行的攻击和侵入活动已经引起了国际社会的高度关注。鉴于国家关键基础设施和关键资源（CIKR）②对 IT 技术

①我国华为、中兴公司 IT 产品遭到美国国会“ 威胁国家安全 ”的无端指责，以及美方所谓中国黑客攻击其关键基础设施的抹黑言论都显示出 IT 供应链安全已经受到“ 国家安全审查 ”的非正当化影响。

②关键基础设施和关键资源（Critical infrastructure and Key resources），美国爱国者法案将 CIKR 定义为 ：“ systems and assets，whether physical or virtual，so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security，national economic security，national public health or safety，or any combination of those matters. ”

的依赖，IT供应链安全与国家安全的关系日益密切，通过国家安全审查识别和控制IT供应链风险成为保障国家安全的必然选择。

（一）全球化视域下的IT供应链

IT供应链是包含系统终端用户、政策制定者、采购专家、系统集成商、网络提供商和软硬件提供商在内的统一系统，是上述角色通过组织和交互等行为，参与IT相关基础设施的管理、维护和防御的过程。[2] 过去的IT供应链注重功能性，片面强调供应商的安全责任，现在则更多地关注IT供应链的脆弱性①，强调各参与角色的共同责任。如软件开发商需要管理软件谱系，保证代码的完整性，并排除人员和病毒对其开发过程的威胁 ；硬件供应商需要管理二级供应商，保证产品安全，防止假冒产品进入系统 ；等等。[3]

IT供应链尽管在结构和功能上与传统供应链存在共性，但也具有区别于传统供应链的特点 ：

（1）产品供应与服务供应的融合度更高。根据客体的不同，供应链理论将供应链划分为产品供应链与服务供应链，在技术风险控制、供应链安全管理和法律规制等方面二者均有所区别。例如，产品供应链更为实体化，提供有形的产品，因此更加侧重物流中的安全措施控制 ；而服务供应链提供无形的服务，更侧重服务质量标准（QoS）的优化和信息流中的信息共享和协调。在IT供应链中，产品供应和服务供应的融合度更高，很难进行清晰的划分②，如云计算应用中的三种基本服务模式③，本身就是产品的服务化。IT供应链是产品供应链与服务供应链相融合的新型供应链，是包含了物流、信息流和资金流的统一整体，在供应链的风险控制中需要兼顾二者的特点，更为全面地考虑供应链的安全问题。

（2）对国家运行的保障作用更为显著。现代社会的一切表征都可以泛化为信息，信息社会中国家运行的基础是对各类信息的收集、处理和利用，这是由工业经济向信息经济转变的必然结果，也是信息化所强调的基本路径。信息化彻底改变了国家运行的基本方式，由IT技术应用所构筑的经济和社会发展范式强化了IT供应链的基础性和全局性作用。可以说，国家信息化的过程本身就是国家生产生活向IT系统逐步迁移的过程，IT系统和资源的部署和维护成为支撑国家运行的必要保障。较于其他供应链，IT供应链风险可能对国防、经济和科技安全造成全面影响，与国家整体的生存和发展息息相关，而且随着IT供应链的延伸和分化，这种风险将更为严峻。

（3）对信息安全的要求更迫切。与传统供应链相比，IT供应链对信息安全的要求更为迫切。这不仅体现为IT供应链在自身信息化过程中对信息安全三性④的基本诉求，而且IT产品和服务也嵌入了供应链中的其他技术要素，技术本身的不确定性会导致信息安全风险的广泛存在。“ 产品规格的变化，持续改进的措施，外包，内部网络重设，IT更新，技术升级过程，供应商关系都会影响IT供应链的不确定性。”[4] IT供应链中任何关键节点都可能由于未经授权的访问、恶意或不合格的供应商、未经测试的软件升级和补丁、使用不安全的发送或存储机制等原因，造成IT产品和服务安全性的减损或关键IT产品和服务供应的中断。⑤

（二）IT供应链安全与国家安全的关系

“ 在重要关头，国家最终关心的并不是权力，而是安全。”[5] 包括国防、科研、金融、交通、教育、能源在内的国家关键基础设施和关键资源已经成为国家的“ 神经系统 ”，将CIKR保护纳入国家安全战略已经是各国的通行做法，美国在《国家基础设施保护计划》中更特别强调“ CIKR保护计划是一项国家安全任务。”[6]

全球化在客观上增加了IT供应链的复杂程度，不合格或恶意的IT产品和服务将有更多的渗透渠道⑥，CIKR保护越来越明显地依赖于IT供应链安全，这使得IT供应链安全和国家安全在本位价值上趋于一致。为了应对IT供应链风险，保障国家安全，早在2008年美国政府发布的《国家网络安全综合计划》（CNCI）中就曾提出，美国政府应当建立多元化的全球供应链风险管理，应对试

①对IT供应链脆弱性的认识通常都与风险相关，是IT供应链由于内外部风险而可能遭受破坏的性质。

②由于IT技术的专业性，供应商在提供IT设备的同时，往往需要提供相应的软件支持和设备及系统的升级维护，包含了产品供应链和服务供应链。

③云计算应用中的三种基本服务模式包括 ：基础设施即服务（IaaS）、软件即服务（SaaS）和平台即服务（PaaS）。

④信息安全三性是指信息的完整性、保密性和可用性。按照ISO27001的定义，完整性指保证信息的准确和完整，防止信息被非法篡改 ；保密性指信息不被未授权的个人、实体、流程访问披露 ；可用性指保证被授权的使用者需要时能够访问信息及相关资产。

⑤例如亚马逊云计算中心的宕机事件造成多家依靠该中心提供服务的机构受到影响。

⑥目前，IT供应链的安全风险主要包括 ：嵌入包含恶意程序（例如病毒、木马、间谍软件）的软硬件，安装假冒伪劣的软硬件，安装的软硬件存在非恶意的漏洞，恶意或不合格的服务提供商，关键IT产品或服务提供的中断，等等。

图通过供应链渗透进行未经授权的数据访问、数据篡改及通信信息拦截等供应链风险。[7] 美国政府在《全球供应链安全国家战略》中进一步阐明美国重点关注威胁供应链系统功能的风险，指出美国政府应当理解并解决那些企图引入有害产品或材料的系统开发和由恶意攻击、事故或自然灾害引发的中断所带来的供应链脆弱性。[8] 美国政府审计局（GAO）在给美国国会的报告中直言，通过全球供应链提供的IT产品和服务存在威胁，该威胁会降低联邦关键和敏感机构网络和数据的保密性、完整性和可用性，要求联邦机构识别和防范IT供应链风险。[9] 欧盟《供应链完整性》报告也同样认为，信息通信技术行业中的供应链完整性是国家经济发展的关键因素，提高供应链完整度对公私部门意义重大。[10] 中俄提交联合国的《信息安全国际行为准则》中强调，应当努力确保信息技术产品和服务供应链的安全，防止他国利用自身资源、关键设施、核心技术及其他优势，削弱接受上述行为准则的国家对信息技术的自主控制权，或威胁其政治、经济和社会安全[11]。

为了保证IT供应链安全，各国基于国家安全的保障要求，普遍着手开展或完善针对IT供应链的安全审查活动，通常涉及本国的政府采购限制、IT产品质量和服务等级、数据保护标准、密码控制制度等①，但各国现行的IT供应链国家安全审查制度的法治程度不容乐观，普遍存在审查范围模糊，审查过程不透明，审查结果存在主观臆断②的现象。

IT供应链国家安全审查应当揭开法制的“外衣”，推行实质性的法治化，即审查标准必须客观，审查范围必须明确，审查程序必须透明，不应当负载过多的政治因素，特别是在技术利用与国家发展愈发密切的今天，盲目排外的审查活动会造成国家丧失对先进技术的利用机会，在国际竞争中处于不利，这与维护国家安全的制度初衷相悖。应当认识到，立法的确定性和稳定性是规制国家安全审查“工具性倾向”的有效途径，在立法上怠于明确审查范围，会减损国家安全审查的正当性。我们尊重国家对以立法形式明确国家安全的审慎态度，但也不能无视在国家安全审查中任意解释国家安全范畴所产生的弊端。

二、IT供应链国家安全审查的范围

明确IT供应链国家安全审查的范围有两个层面的现实价值：一是为执法机关的审查活动提供指引和规范，提高审查活动的透明度，增加审查结果的公正性和可信度；二是为IT供应商提供法律遵从依据，建立平等的贸易环境，促进良性的经济交流与技术利用。

（一）确立综合国家安全观

作为IT供应链国家安全审查的本位价值，“国家安全”是IT供应链国家安全审查的逻辑起点和最终归宿，在何种程度，就何种事项，进行何种审查取决于对国家安全涵义的认知程度，确立合理的国家安全观是国家安全审查逻辑结构中的第一环。

作为与国际关系和地缘政治密切相关的概念，国家安全是动态变化的，在不同的历史背景和时代需求中反映出有差别的表征。冲突与对抗是“冷战”时期世界格局的主旋律，国家安全必须依靠军事能力和外交政策进行维系，领土不受侵犯，政治稳定和主权独立是国家安全的表现形式，也就是传统安全所强调的主权安全、领土安全、政治和军事安全。国际经济政治新格局的演变缓解了紧张的国际环境，促进了全球政治经济的合作与发展，虽然这一时期传统安全仍然是国家安全的核心内容，但内涵更为丰富的国家安全概念正在被各国重新认识。“随着冷战结束，军事—政治安全的比重相对下降，于此同时，安全的内涵与外延也获得了更为广阔的扩展。”[12] 特别是在9·11之后，非传统安全③开始成为国家安全考虑的优先事项，国家安全不仅包括国家军事安全和政治稳定，而且更多地指国家的经济利益、贸易自由、关键基础设施保障、科技利用等。

尽管对国家安全的理解存在差异，但在综合层面上阐述国家安全已经成为共识，如认为“当今的国家安全不仅指政治安全、军事安全，还包括经济安全、文化安全、科技安全、信息安全、生态安全等等”[13]。“有关国家经济秩序稳定、金融

①例如美国《贸易拓展法》规定美国商务部可以评估进口产品对国家安全造成的破坏或影响，并由此提起调查。《国防授权法案》授权国防部长以及陆、海、空司令可排除存在重大供应链风险的合同商。

②2012年6月，欧美日三国的ICT行业组织联合发布了《政府网络安全推荐准则》，呼吁各国政府应当确保网络安全相关的所有法律、法规及其他政策的制定均在公开透明的决策过程中进行，确保网络安全要求的技术中立性，不限制技术采购来源国或者技术供应商的国籍。

③非传统安全是相对于传统安全而言的，指除军事、政治和外交冲突以外的对主权国家安全及发展构成威胁的安全要素，包括经济安全、科技安全、生态安全、信息安全等。

与货币安全、战略资源保障、对外贸易与投资安全等经济安全要素，环境与生态保护、重大自然灾害控制等国土与生态安全要素，重大犯罪的防范与控制、重大事故和人为灾害的防范与控制、突发性事件的应急处置等社会安全要素，以及生物安全、信息安全、核安全等科技安全要素等，都成为影响国家根本利益的因素，因而都属于国家安全的范畴。”[14]“ 可以把全球化时代的国家安全概括为政治安全、军事安全、经济安全、文化安全、科技安全、社会安全等诸多方面的有机结合。”[15]

IT 供应链国家安全审查应当以综合国家安全观为指导思想，体现传统安全和非传统安全相互融合，相互影响的特点，特别是当技术利用和经济发展成为国家进步的核心动力时，不同的安全领域具有了相当程度的同质性，其实质都体现为实现国家的稳定状态，保证国家生产生活的正常运行。在这样的语境下，综合国家安全观更符合全球化背景下的国家利益。

（二）IT 供应链国家安全审查的范围

IT 供应链国家安全的审查范围是解决“ 审查什么 ”的问题，至少在“ 广度 ”和“ 深度 ”的维度上存在加以明确的必要。长期以来，由于技术的局限性和审查思路的片面性，各国基于国家安全的审查活动通常围绕“ 核心企业 ”和“ 最终产品 ”开展审查，没有对 IT 供应链的层次进行区分，这无益于国家安全审查基本目的的实现。

首先，围绕“ 核心企业 ”和“ 最终产品 ”进行国家安全审查不符合 IT 供应链的特点。随着技术流动和经济合作的加强，IT 产品和服务的提供更加依赖广泛的全球化市场，供应商自身的采购行为、业务外包行为、系统集成行为产生了区分间接供应商的客观需要，由“ 核心企业 ”向“ 多级供应商 ”分散的风险控制很难进行‘ 模块化 ’的处理，利用 IT 供应链进行的渗透和攻击可能出现在任何参与主体或供应流程中，仅针对‘ 核心企业 ’和‘ 最终产品 ”实施的彼此拆分的审查过程无法满足保障国家安全的需要。IT 供应链国家安全审查的范围应当扩大审查半径，包含 IT 产品和服务的整个生命周期，涵盖供应商的采购、研发、生产和提供过程，特别是需要将供应商与第三方（如次级供应商、外包方、采购商）之间的关系纳入审查范围①，这是 IT 供应链国家安全审查在“ 广度 ”层面上的横向延伸。

其次，需要根据 IT 产品和服务的部署领域进行 IT 供应链的分类审查。在 IT 供应链中，涉及军事和国防建设的 IT 产品和服务直接关系国家军事安全，各国的政府采购法或进出口管制法通常规定只能采购或部署本国供应商的 IT 产品或服务，由于与国家的生死存亡密切相关，应当尊重国家在该领域的基本态度，严格适用该国的国内安全标准 ；涉及商业或民用用途的 IT 产品和服务关系国家经济发展和技术利用，除属于国家禁止或限制进出口的 IT 产品和服务（如商用密码产品）以外，各国通常对该领域实行原则上的自由贸易，该领域的审查应当适用国际安全标准② ；涉及关键基础设施的 IT 供应链较为特殊，既涉及商业民用的用途，又与军事国防密切相关，鉴于在国家运行中日益重要的支撑作用，关键基础设施 IT 供应链的国家安全审查需要考虑其“ 军民两用 ”的性质，平衡国家安全与技术利用和贸易自由之间的权重，可以提倡适用国际安全标准，并将国内安全标准作为参照。这是 IT 供应链国家安全审查范围在“ 深度 ”层面上纵向扩展。

三、IT 供应链国家安全审查的中国应对

为了应对日益严峻的 IT 供应链风险，并改善我国供应商海外频频遭遇国家安全审查而被否决的现状，避免因 IT 技术控制的不对等性而对我国科技创新自主能力造成的损害，弱化技术依赖性带来的国家安全威胁，我国需要建立 IT 供应链国家安全审查制度，并对现行法律体系进行适时调整。

（一）建立 IT 供应链国家安全审查制度

我国的信息技术发展水平与发达国家存在差距，而所面临的安全风险却是与国际同步的，美国已经为应对供应链风险实施了战略部署，而我国仍未对此做好准备，建立 IT 供应链国家安全审查制度是目前亟待推进的重要任务。

我国 IT 供应链国家安全审查制度应当确立“ 合作包容 ”的理念。该理念的精髓在于以国家综合性安全为基点，实现技术共同进步、经济共同繁荣。[17] 在技术领域，这一理念体现为始终保持技术中立原则，不带有任何政治经济色彩。在法律领域，这一理念体现为法律制度不应当成为技术进步和经济发展的阻碍。IT 供应链是 IT 技术流

①如供应商与第三方之间是否存在产品安全协议，供应商是否对第三方提供的产品或服务实施了安全保障措施，等等。

②如《信息和通信技术供应链风险管理》（ISO/IEC 27036-3）提供了 IT 软件、硬件和服务的供应链安全指南。

转的重要途径，当技术与国家利益之间存在越来越密切的联系时，国家安全的保护并不意味着技术自由的绝对牺牲。“技术自身也已经成为影响国家安全的一个直接的、独立的要素。”[18] 在平衡国家利益与技术利用的冲突中，合作包容的战略理念为国家安全审查确立了应当恪守的基本原则。该理念并不是强调妥协，在经济的全球化合作必须建立在平等的基础上，对于将国家安全审查作为政治工具，通过附加不公正条件而限制我国IT技术自由贸易的国家，我国应当在维护国家利益和产业发展中坚守对等原则，在更广泛的利益框架下促进综合国家安全的实现。

我国IT供应链国家安全审查制度应当通过立法进行确立，这一立法可以是专门的审查法，也可以在相关立法中进行制度构建。[①]审查过程可以考虑改变目前分散的审查方式，设立统一的审查机构，这一审查机构可以是现有的与IT供应链安全相关的主管机构，如工信部、商务部或公安部，也可以建立类似美国外资审查委员会（CFIUS）这类的专门机构。根据前述确立的IT供应链国家安全审查范围，审查机构负责统一部署和分配IT供应链的国家安全审查工作，实现IT供应链国家安全审查的基本目标：一是通过加强信息安全以保护IT供应链和关键节点的完整性，保证IT产品和服务的安全，并有能力核实和检验其是否存在被禁止的情况；二是利用事前响应机制在潜在威胁之前降低IT供应链中断的风险，建立弹性的IT供应链系统；三是制定与完善国家政策、法律和标准，明确各方在IT供应链安全中应当承担的责任和义务。

（二）调整涉及IT供应链国家安全审查的法律规范

IT供应链国家安全审查涉及多项法律的适用和协调，技术进出口管制、商用密码专控和认证认可是与审查活动最为密切相关的法律制度，为了与国家安全审查的目的更加契合，需要进行适度调整。

（1）技术进出口管制的法律调整。IT技术的发展必然超越立法的增补速率，我国在现行的技术进出口管制立法中仍然对“技术”“技术产品”缺乏清晰的定义，仅依靠列举限制或禁止的类别表明受管制的技术范围，极易在国家安全审查范围中对存在风险威胁的新技术产生疏漏。而且，我国在技术进出口管制方面确立了分别管制的原则，即货物进口和技术进口需要适用不同的法律。但在实践中，某一项具体的IT进口项目经常是货物、技术密不可分的，甚至IT产品本身也包含技术的要素，这就造成对同一项目可能依据不同的法律规范进行管控。容易造成在法律适用方面产生冲突，有必要协调技术和物品进出口法规之间的衔接。

（2）商用密码专控的法律调整。我国《商用密码管理条例》第二条将商用密码定义为不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。对介于国家秘密和商用信息之间的政府非涉密敏感信息如何适用未作规定，这一“灰色地带”可能导致进口密码或其基础上的二次开发密码直接适用于电子政务，在政府信息逐步向电子政务迁移的过程中产生大量的信息聚合，原本分散的、非敏感信息通过聚合可以形成完整的、敏感的整体信息，我国应当尽快将政府非涉密敏感信息纳入密码专控的范畴，防止该部分信息泄露对国家安全产生的威胁。同时，我国目前在商用密码进出口控制方面没有对密码位数的具体要求，在密码技术进出口的国家安全审查中，需要对所有密码技术和含有密码技术的产品进行审查，这与国际社会向“重点可控”发展的密码管制趋势相悖。

（3）认证认可的法律调整。认证认可法律制度是IT供应链国家安全审查中最为核心的内容。我国多种许可制度与认证认可制度同时运行，在国家安全审查过程中可能存在重复测评认证的问题。涉及政府采购的IT产品和服务在国家安全审查中，至少需要销售许可和强制认证的双重检测，若产品或服务包含密码技术，则还需经过密码主管机构的测评许可。过于繁琐的认证认可程序会加重IT供应商的负担，增加向我国提供IT产品和服务的时间与成本，IT供应商很可能会将其解读为我国希望通过严厉的审查达到排斥特定供应商的目的，而对我国失去技术输入的信心。IT供应商的这种顾虑还可能源自对我国第三方认证机构独立性的怀疑。在我国目前的认证认可法律体系中，第三方认证机构及实验室目前仍未完全脱离国家政府部门，在独立性和公信力方面存在瑕疵，IT供应商完全有理由怀疑我国的审查结果可能出于纯粹的政治需要。我国虽然已经对《信息技术安全评估通用准则》（CC）进行了转化，但在认证过程中仍然主要依靠国内标准，而且没有参与国

①如我国的外资并购国家安全审查是在反垄断法中进行的制度构建。

际标准的国家间互认。认证认可国际互认有助于减少技术性贸易壁垒。[19]在国家安全审查中，对于已经通过CC认证的IT供应商仍然需要开展大范围的安全及风险控制评估与测试，将导致不必要的二次审查。

结语

立法的确定性和稳定性是规制国家安全审查“工具性倾向”的有效途径，在立法上怠于明确审查范围，会减损国家安全审查的正当性。对IT供应链的安全审查源自供应链风险对国家安全的潜在威胁，审查过程本身即是对风险的识别和控制过程，以弱化因技术脆弱性产生的IT产品或服务缺陷及IT供应链中断等风险，规制IT供应链渗透、入侵或间谍活动等恶意行为，达到保障国家安全的目的。尽管IT供应链处于不断发展之中，但立法完全可以对普遍性的风险做出法制安排。① 我国应当在“合作包容”理念的指导下坚守对等原则，全面理解综合国家安全观的要义，尽快建立符合国家发展目标的IT供应链国家安全审查制度，平衡国家安全与技术利用之间的冲突，提高在全球供应链中的参与程度并切实保障国家利益。

①比如次级供应商，特别是远程技术支持和业务开发流程是IT供应链的主要环节，其风险对国家安全的威胁已经取得了国际社会的普遍共识，立法应当对此做出反应。

参考文献

[1] Zachary Williams. Supply chain security：an overview and research agenda [J]. The International Journal of Logistics Management，2008，(2).

[2] Jon Oltsik，John McKnight，Jennifer Gahm. Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure [R]. Enterprise Strategy Group，2010.

[3] Sander Boyson，Thomas Corsi，Hart Rossman. Building A Cyber Supply Chain Assurance Reference Model [R]. SAIC and the Supply Chain Management Center (SCMC)，Robert H. Smith School of Business，2009.

[4] Helen Peck. Drivers of supply chain vulnerability：an integrated framework [J]. International Journal of Physical Distribution & Logistics Management，2005 (4).

[5] 肯尼思·沃尔兹.国际政治理论[M].胡少华，等，译.北京：中国人民公安大学出版社，2004.

[6] Homeland Security. National Infrastructure Protection Plan [R]. USA，2009.

[7] John Rollins，Anna C. Henning，Comprehensive National Cyber Security Initiative：Legal Authorities and policy Considerations [R]. Congressional Research Service，2009.

[8] The White House. National Strategy for Global Supply Chain Security [R]. USA，2012.

[9] GAO. IT Supply Chain National Security-Related Agencies Need to Better Address Risks [R]. USA，2012.

[10] Scott Cadzow，Georgios Giannopoulos，Alain Merle，et al. Supply Chain Integrity：An overview of the ICT supply chain risks and challenges，and vision for the way forward [R]. Enisa，2012.

[11] International code of conduct for information security [R/OL]. [2012-12-21] http：//cs.brown.edu/courses/csci1800/sources/2012_UN_Russia_and_China_Code_o_Conduct.pdf

[12] 巴瑞·布赞，奥利·维夫，迪·怀尔德.新安全论[M].朱宁，译.杭州：浙江人民出版社，2003.

[13] 吴庆荣.法律上国家安全概念探析[J].中国法学，2006，(4).

[14] 刘卫东，等.论国家安全的概念及其特点[J].世界地理研究，2002，(6).

[15] 谢雪屏.国家安全及若干相关概念的学术梳理[J].福建师范大学学报(哲学社会科学版)，2007，(5).

[16] Scott Charney，Eric T. Werner. Cyber Supply Chain Risk Management：Toward a Global Vision of Transparency and Trust [R]. Trustworthy Computing Microsoft Corporation，2011.

[17] 马民虎，等.商用密码管制：从对立到包容之趋势分析[J].海外资讯，2009，(2).

[18] 杨春平，刘则渊.技术安全：国家安全的重要内容[J].大连理工大学学报(社会科学版)，2005，(4).

[19] 姜茹娇.技术性贸易壁垒与认证认可国际互认制度[J].重庆大学学报(社会科学版)，2006，(5).

[责任编辑：康敬奎]

The Second Enlightenment Calls for a Postmodern Rural Civilization with Roots

WANG Zhi-he

Abstract: Modern civilization has suppressed rural civilization in the name of "urbanization" and "development" and therefore jeopardized the latter. This suppression in turn has caused the rootlessness and unsustainability of the former. The underlying causes lie in the Enlightenment as the philosophical foundation of modern civilization and its suppression of the rural way of life, especially in its imperialistic attitude toward nature, its nihilism toward tradition, its contempt toward peasants, its worship of development, and the modern mechanical worldview underpinning all these. The second Enlightenment aims at transcending the first and calls for a postmodern rural civilization with roots, which reveres nature, values tradition and farmers, and appreciates community prosperity. This transcendence would result in a rooted ecological civilization which espouses common prosperity of the city and the country, industry and agriculture.

Keywords: Second Enlightenment; Constructive Postmodernism; Urbanization; Rural Civilization; Ecological Civilization

IT Supply Chain Security: the Scope of National Security Review and China's Countermeasures

MA Min-hu MA Ning

Abstract: The globalization of IT products and services supply increases the complexity of the IT supply chain, which means that unsafe or malicious IT products and services will have more penetration channels, particularly in national critical infrastructure because of its increasing dependence on IT products and services. The establishment of national security review of the IT supply chain is inevitable. The current national security review system should be clarified in scope and procedure, and its legitimacy established through legislation. In response, China needs to take counter-measures to reduce the national security threat brought about by technology, and to avoid the damage that IT technology asymmetry does to China's ability in scientific and technological innovation. In the spirit of cooperation and inclusiveness, China should redefine national security from a comprehensive point of view, promote law regarding national security review, and expand the scope and the depth of national security review.

Keywords: IT Supply Chain Security; National Security Review; Scope; China's Countermeasures

Reform and Evolution of Economy of Collective Ownership in the South of Jiangsu Pattern: A Case Study of Suzhou

XIA Yong-xiang

Abstract: As a case study of Suzhou, the paper, based on an analysis of the reform and evolution of economy of collective ownership in the South of Jiangsu province, including its shift from people's commune to township enterprises and then to shareholding cooperatives, argues that economy of collective ownership is the inevitable result of marketized production and the dispersion of means of production, and that it undertakes an important historical mission. The role of economy of collective ownership should be given full play in the urban-rural integrated development and the construction of the "new country", while, at the same time, reformed for effective realizations of which the shareholding cooperative is one. Property ownership should be clearly defined and quantified on a personal basis, and democratic management administered in these shareholding cooperatives.

Keywords: South of Jiangsu Pattern; Suzhou; Economy of Collective Ownership; Reform and Evolution; Shareholding Cooperative