主题研讨

国家网络安全审查制度的保障功能及其实现路径

马　宁

内容提要:国家网络安全审查制度是我国提升国家网络安全保障能力的创新制度,但现有政策立法对于该制度的规定存在诸多争议。其中需要首先明确网络安全审查的制度功能,片面的“反制”定位并不能解决我们面临的安全问题,反而会将审查制度降格为纯粹的“政策工具”。在保障功能视域下审视网络安全审查制度,也有利于澄清制度的独立性问题,及其与外商投资国家安全审查在审查重点、审查对象和审查内容方面所存在的区别。为保证国家网络安全审查制度保障功能的实现,我国应当逐步建立基于风险的威胁态势感知审查理念,解决“风险残余”的棘手问题;细化信息系统分级,限定网络安全审查的实施范围;实施供应链安全审查,强调背景审查和技术审查相结合;完善信息安全标准体系,为审查机构和供应商提供明确的遵从指引。

关键词:国家网络安全审查　信息技术产品采购　制度塑造

马宁,西安交通大学法学院信息安全法律研究中心博士研究生。

2014 年 5 月 22 日国家互联网信息办公室宣布我国将建立网络安全审查制度,〔1〕我国《国家安全法》、〔2〕《网络安全法(草案)》〔3〕一审稿和二审稿也均对网络安全审查制度进行了明确规定,特别是在作为规划我国未来信息化发展方向的《国家信息化发展战略纲要》〔4〕中,亦明确提出了建立网络安全审查制度的具体要求。与有些学者的理解

〔1〕 该公告称,我国将实行网络安全审查制度,将针对关系国家安全和公共利益系统使用的重要技术产品和服务实行安全性和可控性审查,防止产品提供者非法控制、干扰、中断用户系统,非法收集、存储、处理和利用用户有关信息。

〔2〕 2015 年 7 月 1 日,第十二届全国人民代表大会常务委员会第十五次会议通过的新《国家安全法》第五十九条规定,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,进行国家安全审查,有效预防和化解国家安全风险。

〔3〕 2016 年 6 月,第十二届全国人大常委会第二十一次会议对草案二次审议稿进行了审议。其中,第三十三条规定,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,应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

〔4〕 2016 年 7 月,中共中央办公厅、国务院办公厅印发了《国家信息化发展战略纲要》,该纲要第五十五条规定,应建立实施网络安全审查制度,对关键信息基础设施中使用的重要信息技术产品和服务开展安全审查。

不同,[5]本文认为,目前各国并不存在真正法律意义上的国家网络安全审查制度,该制度是我国在国家网络安全保障领域的创新尝试。限于目前我国相关政策立法的模糊性,各方对于网络安全审查的理解并不一致,其中不乏偏见与误读。[6] 特别是在国家网络安全审查制度的功能定位和实现方面,非理性的制度设定极有可能削弱国家网络安全审查的正当性基础,有悖于制度设立的初衷。应当意识到,网络安全审查制度同样是一柄双刃剑,其既可以作为一种有效手段提升国家网络安全的保障能力,也可以沦为一种贸易壁垒令国家丧失利用先进技术的机会。

一 国家网络安全审查制度的功能定位

我国选择在美英针对我国信息技术企业实施安全审查之后公布网络安全审查政策,在客观上给人一种"反制措施"的感觉。但本文认为,将国家网络安全审查制度的功能定位于片面的"反制措施"并不能解决我们面临的安全问题,反而会将审查制度降格为纯粹意义上的"政策工具"。鉴于日益严峻的网络安全态势,国家网络安全审查制度的功能应在于"保障",是基于风险考虑的制度安排。

(一)美英安全审查对我国"反制"思维形成的影响

在2012年前后,我国信息技术企业在全球范围内频繁遭受安全审查,而其中以美国尤甚。2011年美国众议院情报委员会专门针对华为和中兴展开审查,直到今天对我国信息技术企业产生的负面影响仍然没有完全消除。2013年英国国家安全委员会对华为位于英国的网络安全中心进行了安全审查,其审查结论包含额外的持续性审查要求,并对华为网络安全中心设立了专门的监管委员会。随后,美国在《合并与持续拨款法案》中对我国采取了歧视性规定,限制四个联邦政府机构采购源自我国的信息技术。上述一系列事件引发了我国各界的强烈不满,并催生了"反制"思维的形成。

1. 美国众议院情报委员会针对华为和中兴的审查

2011年11月,作为对华为公开信的回应,[7]美国众议院情报委员会启动了对华为的调查,主要针对中国电信企业在美业务产生的反间谍和安全威胁,该调查同时将中兴纳入

〔5〕 目前,很多学者认为国外已有完备的网络安全审查制度,并提出据此我国也应当建立相应的安全审查制度。参见张莉:《网络安全审查的国际经验及借鉴》,《信息安全与通信保密》2014年第8期,第65-67页;周定平、胡鹏:《国外网络安全审查制度的经验及启示》,《湖南警察学院学报》2015年第6期,第106-111页;尹丽波:《美国安全审查概况》,《中国信息安全》2014年第8期,第78-81页;汪杨等:《印度开展网络安全审查的主要做法及启示》,《信息安全与通信保密》2014年第8期,第60-64页。

〔6〕 中国信息安全研究院的左晓栋副院长对此进行过详细的澄清,其指出,网络安全审查制度是国家一项具体的网络安全政策,不是战略;网络安全审查制度的目标是单一的,不是解决网络安全问题的"万能药";网络安全审查制度有明确的重点,不是"事无巨细"的监管手段;网络安全审查制度针对的是IT产品与服务,不涉及信息内容;网络安全审查制度对内外一视同仁,不是为了获得产业上的竞争优势。参见左晓栋:《以务实态度对待网络安全审查制度》,《中国信息安全》2015年第5期,第88-89页。

〔7〕 2011年2月25日,华为向美国政府提交了一份公开信。在信中,华为对美国政府认为华为"利用技术窃取美国机密信息,针对美国发动网络攻击"的种种误解进行了澄清,表明没有证据显示华为违反了安全规则,并"诚恳地希望美国政府对华为展开针对任何问题的正式调查"。

其中。[8] 在经历了 11 个月的调查之后,美国众议院情报委员会于 2012 年 10 月 8 日发布了调查报告,详细阐述了调查过程和结果。然而该份调查报告一经发布便饱受质疑,因为其并未提出任何有力的证据表明华为和中兴实施了针对美国的网络攻击或间谍行为,反而充斥着无端的猜测与臆断。[9] 该报告将大量调查集中于分析华为和中兴与中国政府和军队的关系,实质上等同于"背景审查",认为两公司的运作不具备"独立性"。在调查基础上,美国众议院情报委员会提出了措辞非常严厉的五点建议。[10] 如果美国各联邦机构和私营部门选择遵从该建议,那么华为和中兴毫无疑问将被排除在美国市场之外。

2. 英国国家安全委员会针对华为网络安全评估中心的审查

在美国众议院情报委员会的调查报告发布不久,英国情报安全委员会于 2013 年即发布了名为《外国参与关键国家基础设施:国家安全的影响》的报告,该报告直指华为位于班伯里的网络安全评估中心,认为华为进入英国通信市场,特别是涉足关键国家基础设施将严重影响国家安全,建议国家安全委员会尽快组织对华为网络安全评估中心的审查活动。[11] 随后,英国国家安全委员会于 2013 年 7 月对华为的网络安全中心进行了审查,[12] 形成了《华为网络安全中心:国家安全委员会审查》的报告,并向英国首相进行了汇报。尽管英国国家安全委员会的审查结论认为,华为网络安全评估中心能够有效进行运营,现有的管理制度保证了华为网络安全评估中心充足的独立性,但仍然要求设立专门的监管委员会,对华为网络安全评估中心进行年度审查。[13]

3. 美国《合并与持续拨款法案》的歧视性规定

如果上述两个案例仍然可以被视为特例,那么美国 2013 年实施的《合并与持续拨款法案》则在立法层面确立了针对中国信息技术的限制态度。[14] 作为美国联邦政府财年预

〔8〕 参见 The House Permanent Select Committee on Intelligence, Investigative Report on the U. S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, US, 2012, p. 1。

〔9〕 例如该报告认为,"美国的国家安全利益正在受到源自电信供应链脆弱性的威胁,而中国有机会和动机利用电信公司实现恶意目的,缓解措施并不能完全应对中国电信公司向美国关键基础设施提供设备和服务过程中产生的威胁。"而这一论断显然放之四海皆准,根据这一标准,任何国家均应被美国视为潜在的威胁对象。

〔10〕 该五点建议包括:(1)美国应当以怀疑的态度审视中国电信企业向美国市场的渗透。同时要求美国情报委员会(IC)对这种威胁保持警惕;要求美国外国投资委员会(CFIUS)阻止涉及华为和中兴的、可能威胁美国国家安全利益的采购、收购和并购活动;要求美国政府系统,特别是敏感系统,不得使用华为和中兴的设备。(2)鼓励美国的私营企业正视与华为和中兴商业合作中存在的长期安全风险,鼓励美国的网络提供商和系统开发商寻求其他合作伙伴。(3)美国国会司法委员会和执法机构应该对中国电信企业的不公平贸易行为进行调查,尤其应当关注中国对关键公司的持续财务支持。(4)中国公司应该迅速变得更加开放和透明,包括提供独立第三方评估机构对于他们财务信息和网络安全进程的评估,遵从美国的信息安全和知识产权立法及标准。(5)美国国会司法委员会应该促进立法,以更好应对与其他国家政府相关的电信公司所带来的风险,否则就不要充分信任他们来建造关键基础设施。这些立法包括增进私营部门的信息共享,将 CFIUS 的审查程序扩展至采购合同。

〔11〕 参见 Intelligence and Security Committee, Foreign Involvement in the Critical National Infrastructure: The Implications for National Security, UK, 2013, p. 8。

〔12〕 英国国家安全委员会针对华为的审查重点在于华为网络安全中心运行的独立性问题,包括审查华为的员工、华为的计划和预算监管、华为网络安全中心是如何运作的、以及华为设备的安全环境等主要内容。审查方式包括实地考察、主要利益相关者约谈、审查成文证据等。

〔13〕 参见 National Security Adviser, *Huawei Cyber Security Evaluation Centre: Review by the National Security Adviser*, UK, 2013, p. 3。

〔14〕 讽刺的是,2012 年 6 月,欧美日的信息通信技术行业组织刚刚联合发布了《政府网络安全推荐准则》,呼吁各国政府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。

算和拨款法案,历年的《合并与持续拨款法案》对于美国政府的政策制定和业务开展起到举足轻重的引导和规范作用。[15] 2013 年的《合并与持续拨款法案》第 516 条款赤裸裸地抛弃了各国立法所恪守的"非歧视原则",史无前例地直接限制四个政府机构采购源自中国的信息技术。[16] 该条款引起了信息技术产业的强烈不满,认为其开创了非常糟糕的审查先例。[17] 尽管第 516 条款受到了强烈质疑,但"中国依据 WTO 非歧视原则否定该法案效力的努力会相当艰难,除非有极具说服力的理由,否则该限制条款被修订的可能性很小"。[18] 在 2014 年的《合并与持续拨款法案》中,第 515 条款对中国信息技术管制的态度有所放松,开始强调 IT 供应链风险控制的具体要求,但仍然保留了对中国的歧视性规定。[19] 该规定虽然并未禁止采购源自中国的信息技术,但要求机构负责人决定采购活动符合国家利益,并向国会报告,这实质上完全排除了采购活动的可能性,"因为机构负责人不会愿意对采购活动是否符合国家利益自行作出判断"。[20]

为此,在很多情况下,我国建立网络安全审查制度被或多或少地理解为一种"反制手段"。[21]在实践中,很多学者强调美国对我国信息技术企业实施了不公正待遇,我们也应当"以牙还牙"地采取对等策略。但片面或单纯将"反制"作为制度功能,会导致该制度沦为纯粹的"政策工具",甚至是"贸易壁垒",这对于我国网络安全的实现并无裨益。

---

〔15〕 美国宪法规定联邦政府的财政支出必须经过法律的授权,联邦机构的业务运行和相关计划需要由相关法律进行拨款,合并与持续拨款法案规定了联邦机构在特定财年内的资金水平,并对拨款的使用 进行授权和限制。

〔16〕 该条第 a 款规定,美国商务部、司法部、国家宇航局和国家科学基金会不得利用任何拨款采购信息技术系统,除非上述联邦机构负责人与联邦调查局或其他适当机构对网络间谍或破坏行为进行了风险评估,该风险包括与由中国拥有、管理或资助的一个或多个机构所生产、制造或组装的信息技术系统有关的任何风险。该条第 b 款规定,上述联邦机构不得利用任何拨款采购根据第 a 款规定需要进行评估的信息技术系统,不得采购由中国拥有、管理或资助的一个或多个机构所生产、制造或组装的信息技术系统,除非第 a 款规定的评估机构的负责人决定,并向众议院和参议院的拨款委员会报告,该系统采购符合美国的国家利益。

〔17〕 2013 年 4 月 4 日,美国主要行业协会共同致信美国国会,请求国会审查该规定对网络安全和市场竞争产生的影响,并就解决这一问题考虑更具有建设性的方法,主张类似条款不再出现在任何其他法律文件中。2013 年 4 月 8 日,美中贸易全国委员会致信美国国会,认为国家安全是美国的基础,但其不应被用于保护主义,限制采购任何源自中国的信息技术已经超越了任何合理的安全考量。同日,美国信息技术产业理事会(ITI)的丹妮尔·克里兹和白石撰文称,516 条款并没有使我们更接近加强网络安全的目标,也无助于我们针对一些错综复杂的网络安全棘手问题开展理性、冷静的对话。

〔18〕 参见马民虎、马宁:《技术中立:政府 IT 采购中信息安全审查的法律理性—兼评美国〈2013 年合并与持续拨款法案〉第 516 条款》,《河北法学》2014 年第 8 期,第 13 页。

〔19〕 该法案第 a 款规定,美国商务部、司法部、国家宇航局和国家科学基金会不得利用任何拨款采购 NIST SP199 中规定的高影响(High-impact)或中度影响(Moderate-impact)的信息技术系统,除非上述联邦机构:(1)根据 NIST 制定的有关标准进行供应链风险审查;(2)通过由联邦调查局或其他相关机构提供的威胁信息审查供应链风险;(3)联邦调查局或其他机构对与系统采购相关的网络间谍或破坏行为进行了风险评估,包括由美国政府认定实施了网络威胁的一个或多个组织生产、制造或组装的信息系统,包括但不限于由中国拥有、管理或资助的组织。

〔20〕 参见 Covington & Burling LLP, *Appropriations Act Provisions on Information System Procurement for Certain Agencies, Government Contracts National Security & Defense*,2013, p. 3。

〔21〕 例如倪光南院士曾表示,2012 年美国政府以"可能威胁美国国家通信安全"为名,不允许华为、中兴的产品进入美国市场,虽然我国企业受到的待遇是不公正的,但由于当时我国没有网络安全审查制度,因而无法采取反制措施。试想,如果当时有这样的安全审查制度,我们也可以对美国企业进行类似的审查,也许可以制约美国方面对华为、中兴的制裁措施。由此可见,出台网络安全审查制度是很有必要的。参见李雪、杨晨:《对话专家 建言审查》,《信息安全与通信保密》2014 年第 8 期,第 27 页。

(二)国家网络安全审查保障功能的确立

根据国家网信办发布的公告,我国实施网络安全审查旨在"防止产品提供者非法控制、干扰、中断用户系统,非法收集、存储、处理和利用用户有关信息"。为此,我国的网络安全审查制度一定是基于安全风险的,而且仅限于信息安全风险。[22] 在这里之所以要强调信息安全风险,是因为在更为广义的国家行为范畴,遭受他国不公正安全审查同样也可以视为一种潜在的外部风险,但这显然不属于网络安全审查所意欲规避和防范的风险。

首先,"反制"注重等同效力,以对方的"在先行为"为制度启动或实施的前提,因此制度本身是以行为为基础的,这导致审查目的并不一定以网络安全为出发点——例如典型的出于报复目的的审查活动——这对于降低信息安全风险并无实际价值。其次,"反制"作为以在先行为为基础的审查活动不可能涵盖所有的网络安全风险,在出现突发事件或其他网络安全威胁时,网络安全审查并不能有效启动。例如,如果有证据表明某国信息技术产品和服务存在网络安全风险,但该国并未对我国实施网络安全审查,那么以"反制"为功能定位的网络安全审查就变得毫无意义。再次,"反制"的功能定位意味着我国的网络安全审查必然局限于针对国外信息技术企业,这不仅可能构成实质意义上的贸易壁垒而遭受国际质疑,也会造成国家丧失利用先进技术的机会。更为重要的是,受限于审查对象的范围,以"反制"为功能的网络安全审查制度一方面不可能对由国内企业引入的安全风险作出规制;另一方面,如果考虑到信息技术供应全球化的现实,在外国企业作为本国企业的次级供应商时,网络安全审查制度便被轻易地规避掉。

我们需要意识到,在过去的十几年时间里,信息技术的"泛在化"部署迫使我们开始重新审视信息技术对现代社会的支撑作用,信息技术无疑已经从单纯的通信工具转变为国家的关键信息基础设施。"信息技术的传播和发展,以及该技术的使用或应用造成网络空间和现实空间不断融合",[23] 国家和社会运行高度依赖信息技术的安全性和稳定性。然而遗憾的是,正如所有技术馈赠都有其阴暗面,信息技术滥用产生的网络风险也成为影响国家安全和社会稳定的巨大威胁。这种威胁主要体现在以下两个方面,其一是风险来源的多元化,任何信息系统内外部的环境变化都可能引入不确定的安全风险,包括恶意攻击、意外事件或自然灾害。其二是风险来源的能力化,2007 年针对爱沙尼亚政府网络的攻击,2009 年针对韩国的大规模拒绝服务攻击,2010 年针对伊朗核设施的震网病毒攻击事件,2015 年针对乌克兰电网攻击事件都一再验证了网络安全风险产生的灾难性后果。

---

〔22〕 在法学领域,信息安全并不是一个富有争议性的概念,各国均对信息安全做出了明确界定。例如,美国将信息安全定义为"确保(保护)信息和信息系统避免未经授权的访问、使用、披露、中断、修改或破坏,以实现完整性、保密性和可用性。H. R. 2458, *Federal Information Security Management Act of 2002*, Sec. 3542。美国 NIST2013 年 5 月发布的《重要信息安全词汇表》(*Glossary of Key Information Security Terms*, NISTIR 7298Revision 2)中沿用了这一概念,并且 NIST 开发的信息安全标准均采用了这一概念。欧盟将信息安全定义为"网络和信息系统抵御意外事件或非法和恶意行为的能力,这些意外事件或非法和恶意行为会损害通过网络和信息系统存储和传输的数据的可用性、认证性、完整性和保密性,或损害网络和信息系统提供或经由其访问的服务。Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency。为此,所有能够造成信息完整性、保密性和可用性减损的风险都将被视为信息安全风险。

〔23〕 参见 *Information Security Policy Council*, *Cybersecurity Strategy-Towards a World-leading*, *Resilient and Vigorous Cyberspace*, Japan, 2013, p. 5。

特别是在“棱镜事件”后,“国家”作为风险来源的可能性已经引起了各国的警醒。[24] 在这种情况下,被动式的“反制”措施能够起到的风险控制效果是令人存疑的,只有确立积极的保障功能才能充分发挥网络安全审查的制度作用,提升国家网络安全的保障能力。为此,国家网络安全审查应当是基于风险控制的保障制度,旨在防范和弱化信息或信息资源可能遭遇的保密性、可用性和完整性减损。

二 保障功能视域下国家网络安全审查的制度独立性

在信息技术领域,关键部门或行业的技术利用活动通常会引发与国家安全相关的立法思考,产生国家安全审查的客观要求,这也是国家安全审查制度保障功能的最直接体现。[25]

我们目前面临的研究困境是,建立在成熟法律制度基础上的国家安全审查目前以外商投资国家安全审查制度为主。在很多情况下,国家安全审查与外商投资国家安全审查被同等对待,认为国家安全审查专指外商投资国家安全审查,[26] 或认为国家安全审查的功能定位在于保障产业安全。[27] 为此,在论证国家网络安全审查正当性的时候,有些学者会将外商投资国家安全审查作为国家网络安全审查的制度基础,[28] 或以美国外国投资委员会(CFIUS)对我国华为并购 3COM 和 3LEAF 的否决案来印证美国存在严格的网络安全审查制度,导致目前大量的国家网络安全审查法律制度实证性研究集中于业已建立的外商投资国家安全审查立法框架。

如果从可供规制的法律行为角度分析,涉及信息技术的外商投资行为确实具有双重性,兼跨资本准入和技术准入两大国家管控领域。随着信息技术的全球化利用,外商投资国家安全审查向信息技术要素的扩展客观上模糊了其与网络安全审查的边界。[29] 在制度保障功能方面,外商投资国家安全审查和网络安全审查也具有相似性,二者均以特定领域的国家安全保障为制度功能,均以特定活动所产生的风险评估和控制为制度目的。为

〔24〕 例如,印度 2013 年的国家网络安全战略中便指出,网络空间数据的传输可能被国家或非国家主体恶意利用。

〔25〕 在我国《国家安全法》的规定中,网络安全审查被视为国家安全审查的一种。

〔26〕 例如认为“国家安全审查制度,是世界各国用于维护本国核心经济利益、有效监管涉外投资活动的一类制度安排。”参见余菁等:《国家安全审查制度与“竞争中立”原则——兼论中国国有企业如何适应国际社会的制度规范》,《中国社会科学院研究生院学报》2014 第 3 期,第 53 页。

〔27〕 例如认为“国家安全审查在产业安全保障方面的功能定位,取决于该制度在整个涉外经济管制法律体系中的地位、及其与相关制度的功能协调。”参见朱一飞:《国家安全审查与反垄断法的区别与协调——以产业安全保障为视角》,《河北法学》2009 年第 5 期,第 128 页。

〔28〕 例如认为美国在外资并购领域建立了审查机制和流程,CFIUS 拥有非常大的自由决定权和灵活度。后来的网络安全审查在很多地方都借鉴了 CFIUS 审查。参见张莉:《网络安全审查的国际经验及借鉴》,《信息安全与保密通信》2014 年第 8 期,第 65 页。

〔29〕 以 2012 年华为在美投资调查为例,华为向美国关键部门提供信息技术产品和服务被视为外国投资行为,而接受 CFIUS 的监管。从 CFIUS 近年来的审查实例来看,信息技术领域的外商投资逐渐开始关注网络安全的保障问题,美国国会众议院情报委员会在调查报告的建议中也指明,应当将 CFIUS 的审查程序扩展至采购合同阶段。也就是说,美国政府针对华为的审查尽管是以网络安全为目的和实质内容,但仍然以外国投资国家安全审查为制度基础。

此,国家网络安全审查就与外商投资国家安全审查也出现了混同或相互交叉的认知。[30] 但二者在保障方法,在审查重点、审查对象和审查内容方面均有所区别。

(一)审查重点不同

外商投资国家安全审查源于外资介入东道国市场而产生的国家安全威胁,"资本的逐利性特点导致外国投资与国家安全在突破两者之间平衡界限的情况下会发生一定的冲突。"[31] 为此,外商投资国家安全审查更侧重于保护国家经济安全,客观反映为国家对外国资本获取本国企业"控制权"的限制。[32] 而国家网络安全审查源于国家关键基础设施对信息技术依赖性而产生的国家安全"脆弱性"考虑。国家网络安全审查的目的是防止产品提供者非法控制、干扰、中断用户系统,非法收集、存储、处理和利用用户有关信息。

(二)审查对象不同

外商投资国家安全审查的保障方法是通过排除特定资本的市场准入来实现的,其审查对象是"外国人在特定领域内的投资行为"。也就是说,外商投资国家安全审查天然是以资本的来源地作为审查的核心要素。例如美国审查外国人计划实施的任何可能导致外国控制的结果的兼并、收购或接管;[33] 加拿大审查外国人在加拿大建立新商业,以任何方式取得加拿大商业的控制权和取得在加拿大经营实体的全部或部分资产。[34] 为此,外商投资国家安全审查对象包括两项基本的限制条件,即外国人和投资行为。

而根据目前我国相关政策和立法规定,国家网络安全审查的保障方法是通过验证信息技术产品和服务的安全性和可控性来实现的,其审查对象为"重要信息技术产品和服务",而且并不仅仅针对外国人,所有在我国境内使用的信息技术产品和服务都在审查范围之内。这也有助于修正目前"国别化"审查的思路,暂且不论"国别化"审查可能引发的"反歧视"争议,单从信息技术的利用角度而言,其可能造成国家丧失利用先进技术的机会,对国家安全而言并无裨益。更进一步,信息技术全球化产生的客观事实是信息技术产品和服务提供的全球化,区分国别的来源地调查就变得十分困难,在存在次级供应商的情况下,国别化审查就变得毫无意义。

(三)审查内容不同

外商投资国家安全审查的审查内容主要针对外商投资对国家安全的负面影响,例如《美国外国投资委员会国家安全审查指南》确定 CFUIS 的审查活动仅限于交易引起的"纯

〔30〕 例如将 2007 年《外国投资和国家安全法案》作为美国建立网络安全审查体系的法制基础,将 CFIUS 视为美国安全审查的组织机构。参见薛高:《网络安全审查制度研究及对我国金融业的启示》,《金融科技时代》2015 年第 1 期,第 67 页。或认为美国家安全审查制度由其外国投资委员会(CFIUS)执掌,从机构设置、法规依据、运作程序、审查内容、审查标准等方面均体现出鲜明的国家意志。伴随网络空间的蓬勃发展,网络安全审查必然成为国家安全审查的重要组成部分。参见王珞:《美国网络安全审查制度的战略效应》,《中国信息安全》2015 年第 3 期,第 52 页。

〔31〕 田文英等著:《外资并购与国家安全》,法律出版社 2011 年 4 月第 1 版,第 13 页。

〔32〕 例如《美国外国投资委员会国家安全审查指南》中列明的 CFIUS 审查过的交易主要包括两类,即"外国人取得控制权的美国企业的性质引起国家安全考虑的交易"和"取得美国企业控制权的外国人身份引起国家安全考虑的交易",其国家安全审查重点均围绕美国企业的"控制权"展开。

〔33〕 *Foreign Investment and National Security Act of* 2007.

〔34〕 *Investment Canada Act* (R. S. C., 1985, c. 28 (1st Supp.))

粹的国家安全问题”,而不涉及其他的国家利益,主要包括美国《外国投资与国家安全法》规定的 11 项审查内容。而国家网络安全审查的审查内容主要针对信息技术产品和服务的安全性和可控性,其中主要审查是否存在供应链安全风险,集中于信息安全控制部署和完成情况的检验和认定,其中应当特别关注网络间谍和网络破坏行为的潜在威胁。

这也导致二者在制度的透明度方面存在极大差别。由于外商投资国家安全审查以“国家安全”为审查内容,这意味着本身即存在模糊性的“国家安全”概念和标准并不能为供应商提供明确的指引,审查结果不存在任何意义上的“可期待性”,审查程序和审查标准均不透明。而国家网络安全审查是以防范信息安全风险为保障功能的,目前存在大量的安全标准可以验证信息技术产品、服务、乃至供应链整体的安全性。鉴于网络安全审查的专业性和技术性,审查机构通常也会发布保障政策,强制要求供应商予以遵从,而且对于信息技术产品和服务安全性的验证通常由独立的第三方予以完成。全部满足国家信息安全保障标准的供应商,在理论上均有进入本国信息技术领域的可能性。为此,国家网络安全审查的透明度要远远高于外资并购国家安全审查。

三　国家网络安全审查保障功能的制度支撑:以美国信息技术采购保障制度为蓝本

根据我国《网络安全法》(草案)的规定,我国实施的国家网络安全审查制度将主要适用于关键信息基础设施的采购阶段,这意味着我国的国家网络安全审查至少将包含政府采购和认证认可两大法律制度,但我国目前在政府采购和认证认可领域的规定几乎没有关注网络安全审查的相关内容,对国家网络安全审查制度的支撑作用有限。

在美国广泛推行电子政务的过程中,面临着与我国目前相同的境遇,由国家研发或批准使用的信息技术远远不能满足信息系统的安全建设需求,大量的商业现货信息技术产品和服务被部署在包括国家安全系统在内的政务系统中。考虑到商业现货信息技术很可能包含对国家信息安全产生威胁的潜在风险,美国在很早就重视在政府信息技术采购阶段强制采取安全保障措施,其在政府信息技术采购和认证认可制度建设中的有益经验可以为我国所借鉴。

(一)美国信息技术采购保障的基础性立法

美国涉及政府采购的立法非常庞杂,相关立法大概有 4000 多部,[35]不乏关注信息安全的重要条款,其中与国家网络安全审查这一议题直接相关的立法主要包括以下几部。

1.《联邦信息安全管理法》

2002 年,美国《联邦信息安全管理法》(FISMA)的出台标志着美国政府正式建立了政府信息安全要求,FISMA 被公认为美国信息安全保障的统领性和基础性立法。与美国其他国家战略所阐述的宣誓性规定不同,FISMA 规定了非常详细和具有可操作性的联邦政

〔35〕 参见肖志宏、杨倩雯:《美国联邦政府采购的信息安全保障机制及其启示》,《北京电子科技学院学报》2009 年第 9 期,第 15 页。

府信息安全保障规定,成为联邦政府信息安全遵从中重要的指引性立法。

FISMA 规定各联邦机构(包括国家安全系统)必须在本机构范围内开发、文档化、实施信息安全项目,以实现支持该机构运行的信息系统的信息安全,[36] 鉴于信息安全保障的复杂性,为了避免各联邦机构在项目实施中的差异,FISMA 对联邦机构实施的信息安全项目提供了参考性的指引。[37]

其中需要格外注意的是,FISMA 要求各联邦机构每年开发、维持和更新主要的信息系统。根据这项规定,各联邦机构每年需要对信息安全项目和实践进行独立性评估,包括控制测试和遵从性评估。对于非国家安全系统的评估可以由独立的第三方机构完成,而针对国家安全系统的评估只能由机构主管指定的机构进行评估。该项规定事实上构成了对联邦机构信息系统进行定期网络安全审查的基本要求,[38] 只不过这种审查是扩展到包含采购阶段在内的整个信息和信息系统生命周期的安全审查。[39]

2.《克林格 - 科恩法》

1996 年的《克林格 - 科恩》法[40] 是美国政府部门制定和实施信息技术采购政策和程序最直接的法律依据,在该部法案中,D 部分规定了联邦采购改革的相关要求,E 部分规定了信息技术管理改革的相关要求。根据该法案的规定,由 1949 年《联邦资产与管理服务法》[41] 所确立的通用服务管理局(The Administrator of general servics)集中授权采购的方式被废除,[42] 而由各联邦机构具体负责信息技术的采购事项。但这种去中心化的改革方案并没有放松信息技术政府采购的自由度,因为在联邦层面的信息技术采购资金计划和投资控制仍然归于联邦预算管理办公室(OMB),OMB 的负责人被赋予广泛的信息技术采购监管职责,[43] 其中有两项规定引起了本文关注,其一是 OMB 的负责人制定分析、追踪和评估联邦机构信息系统投资风险的程序。[44] 根据该规定,美国事实上建立了通过

〔36〕 这些信息系统同时包括由其他机构、合同方、或其他人员提供和管理的信息系统。

〔37〕 这些规定包括:定期对针对信息或信息系统进行的未经授权访问、使用、披露、破坏、变更、中断等风险和伤害进行评估;建立符合成本效益的以风险为基础的政策和程序,将信息安全风险降低到可以接受的程度,在信息系统生命周期的各个阶段保证信息安全。为网络、设备、系统及信息系统设计从属计划,以提供充足的信息安全保障;对各机构成员进行安全意识培训;定期对信息安全政策、程序、实践和效果进行基于风险的测试和评估,包括对主要系统的管理、运行和技术控制措施进行测试,该期间不得长于一年;针对信息安全政策、实践和程序中的缺陷,建立计划、实施、评估和文档化补救措施的程序;针对安全事件建立检测、报告和相应程序;建立保障信息系统持续性运行的计划和程序等。

〔38〕 很多学者坚持认为风险评估和安全审查是两个不同的制度,但本文认为风险评估是一种信息安全保障手段,其可以运用在各类不同的安全保障制度中。事实上,基于信息安全保障而构建的任何法律制度都不可能脱离风险评估这一保障方法的支撑。为此,风险评估并不是一类特定的法律制度,而是在法律制度中具体的保障方法,网络安全审查也需要包含风险评估的具体要求。

〔39〕 本文认为,针对整体国家网络态势的安全审查应当纳入到国家网络安全审查的整体框架内,而不是局限于目前的采购阶段,例如美国和澳大利亚已经开始实施类似审查。

〔40〕 克林格 - 科恩法案是一部合并性法案,由 1996 年的信息技术管理改革法案(ITMRA)和联邦采购改革法案(FARA)合并组成,经美国 104 届国会批准成为立法。

〔41〕 40 U. S. C. 759.

〔42〕 SEC. 5101.

〔43〕 包括促进联邦项目采购和使用信息技术,开发和实施信息技术标准,制定政府信息技术采购中的管理机构,在政府信息技术采购中使用最佳实践,持续性的评估和比较各联邦机构信息技术采购的实践经验,强化信息资源管理的人员培训等。

〔44〕 该程序被定义为预算程序的一部分。

预算管理限制或排除信息技术政府采购的制度安排;[45]其二是开发和实施信息技术采购政策,[46]这也成为各联邦机构广泛通过灵活的采购政策审查和保障信息技术采购安全性的法律基础。

3. OMB A-130

1985 年,OMB 正式发布 A-130 通告(Circular No. A-130),又称《联邦信息资源管理》(The Management of Federal Information Resources),该通告分别于 1994 年、1996 年、2000 年和 2016 年进行了四次修订。根据 FISMA 的规定,OMB 作为美国联邦信息保障监管的重要机构,其颁布的 A-130 号通告也被作为美国政府信息技术采购的核心遵从要求。

在 2016 年最新版的 A-130 中,OMB 专门针对联邦机构提出在风险管理中需要审查和解决与程序、人员和技术相关的风险。在采购信息技术和服务时,联邦机构需要分析与潜在供应商及其提供的产品和服务相关的安全风险,包括供应链风险,并在政府和供应商之前分配风险责任。同时,A-130 特别强调 OMB 监管责任,要求 OMB 实施信息技术计划审查、财年预算审查、信息收集审查、管理审查和其他 OMB 认为评估联邦机构信息资源管理遵从性的必要审查。要求各联邦机构实施供应链安全审查,在整个信息系统开发生命周期中防止假冒、恶意和未经授权的产品安装,防止破坏和盗窃行为,防止不可靠的生产和开发实践在信息系统中予以适用。

此外,美国的《联邦政府采购法》和《联邦信息技术采购改革法》也对美国政府信息技术采购的程序和实体要件进行了规定,其中的信息安全保障要求在政府信息技术采购活动中同样构成对供应商进行安全审查的具体要求。

(二)美国政府信息技术采购中的"安全审查"

在美国政府信息技术采购的相关政策立法中,很少出现有关"安全审查(security review)"的直接表述,而通常以"风险评估"或"风险控制"等术语来诠释安全保障要求。这些安全保障要求尽管并不以纯粹的"审查制度"方式予以体现,但在实践中一方面构成了联邦机构选择和采购信息技术的基线要求,另一方面也构成了供应商可靠性的验证标准,与国家网络安全审查的保障功能基本一致,主要包括强制性评估和认证认可两个部分。

1. 国家安全系统信息技术采购的强制性评估

早在 2000 年 7 月,美国国家安全通信和信息系统安全委员会(NSTISSC)[47]就发布了名为《国家信息保障采购政策》[48]的第 11 号政策。该政策认为,信息技术的发展和威胁彻底改变了通信和通信系统的保护方式,NSTISSC 清醒地意识到,在国家安全系统中使用

---

〔45〕 例如美国 2013 和 2014 年《合并与持续拨款法案》即是通过预算管理的方式限制四个联邦机构采购我国的信息技术产品。

〔46〕 SEC. 5112(K).

〔47〕 美国国家安全通信和信息系统安全委员会是根据美国 1990 年的第 42 号国家安全指令建立的国家安全通信和信息系统安全管理机构,主要负责制定和颁布适用于国家安全通信和信息系统的国家安全政策。

〔48〕 NSTISSP (National Security Telecommunications and Information Systems Security Policy) No. 11: National Information Assurance Acquisition Policy,有学者将译为"国家信息安全采购政策",但本文认为,information assurance 在美国信息安全相关标准中有明确定义,应为信息保障(IA)。根据 NSTISSC 2009 发布的第 4009 号指令《国家信息系统安全术语》,信息保障是指"通过实现可用性、完整性、认证性、保密性和抗抵赖性保护信息和信息系统的信息操作,包括提供结合保护、检测和反应的信息系统恢复能力。"

商业产品已经不可避免,其引入的安全风险必须得到重视,美国政府采购商业产品必须使用标准化的评估流程来确保信息技术产品的安全性。

为此,国家信息保障采购政策对进入国家安全信息系统的信息技术产品要求非常严格,强制要求在所有能够访问、处理、存储、显示或传输国家安全信息的系统中建立信息保障程序,并在政府和商业信息技术产品现货供应的采购和评估过程中实现信息保障。采购的信息技术产品必须保障信息的完整性、可用性和保密性,实现电子交易中各方主体的认证性和抗抵赖性。

该政策规定,自 2001 年 7 月 1 日起,所有国家安全信息系统中采购的信息技术产品必须满足评估和验证要求,首先必须满足互认的国际信息安全技术评估通用标准的安全要求;其次必须满足 NSA、NIST 和国家信息保障合作组织(NIAP)的评估认证程序;或满足 NIST 联邦信息处理标准(FIPS)的认证程序。相关的评估认证工作由可信的商业实验室或 NIST 进行实施。自 2002 年 6 月 1 日起,所有国家安全信息系统采购的信息技术产品只能限于通过上述评估认证的产品,同时必须接受 NSA 的评估或符合 NSA 批准的流程。关键基础设施保护第 63 号总统令规定的非国家安全系统也可以考虑适用上述评估和认证要求,这些信息系统尽管仅涉及非保密性信息,但其对于实现特定功能意义重大。

2013 年 6 月 10 日,美国国家安全系统委员会(CNSS)发布了第 11 号政策《管理信息保障和实现信息保障的信息技术产品采购的国家政策》,[49] 该政策重申了 NSTISSP 第 11 号政策的采购要求,强调所有国家安全系统采购的信息保障或实现信息保障的信息技术商业现货产品必须满足 NIAP 和 NSA 的评估和认证要求,加密产品必须满足 FIPS 中涉及密码的验证项目要求。CNSS 的采购政策更进一步明确了国家安全系统信息技术产品采购中各方主体的责任,使得信息技术产品的安全评估和认证工作更具实践性和可操作性。从 NSTISSP No. 11 到 CNSS NO. 11 的十年间,美国针对国家安全系统,同时包含关键信息基础设施的信息技术采购过程中建立了逐渐完备的安全保障要求,[50] 这些保障要求可以被视为美国在政府信息技术采购中的安全审查框架。

2. 国家安全系统的认证认可

1994 年 4 月 8 日,美国国家安全通信和信息系统安全委员会(NSTISSC)颁布了第 6 号国家政策《国家安全通信和信息系统认证认可的国家政策》,该政策强制要求所有联邦政府机构在其运营的国家安全系统中建立和实施认证认可程序,其所建立的认证认可程序应当能够有效保证国家安全系统中的信息处理、存储和传输的保密性、完整性和可用性。美国将认证认可视为两个相互独立的信息安全保障阶段,其中认证是指针对系统和其他保障措施的技术和非技术安全特性进行的综合性评估,判断其是否满足特定的安全需求,并支持认可程序的实施,这一过程非常类似网络安全审查活动中对信息技术安全性和可信性的验证过程。认可是指由指定的批准机构对在特定安全模式中使用相关信息技

〔49〕 CNSS Policy No. 11: National policy governing the acquisition of information assurance (IA) and IA-Enabled information technology products.

〔50〕 例如,NIPA 已经建立起信息技术产品清单,国家安全系统的信息技术采购只能选择清单中的产品;形成了以 SP 800 - 53 和 SP800 - 37 为基础的风险安全管理框架,将信息技术产品可能引入的安全风险由采购阶段延展至整个信息技术产品生命周期中;NSA 同样公布了在保护涉密信息的信息系统中使用信息保障和实现信息保障的信息技术商业现货产品的相关指南。

术进行批准的书面声明。[51]

2000 年 4 月，NSTISSC 在《国家安全通信和信息系统认证认可的国家政策》的基础上颁布实施了第 1000 号指令《国家信息保障认证认可程序》，该指令建立了国家安全系统认证认可中的最低安全标准，要求所有运营国家安全系统的联邦机构建立统一的国家安全系统信息保障认证认可程序（NIACAP）。NIACAP 旨在保障国家安全信息系统符合文件化的认可要求，并保障在整个系统生命周期中保有经过认可的安全特性。NSTISSC 设计整套 NIACAP 的关键是在信息系统管理者、[52]指定的批准机构、[53]认证机构[54]和用户之间建立安全协议，该协议通常被称为“系统安全授权协议”（SSAA），SSAA 被用于指导和文档化国家安全信息系统的认证认可过程，并在系统开发和变更之前建立安全要求，在信息系统经过认可之后，SSAA 将被作为信息系统安全配置的基础性文件。[55] NSTISSC 规定所有国家安全系统中每一个信息系统均必须由相关 SSAA 覆盖，SSAA 的复杂程度取决于认证的复杂性和安全需求的差异性。

（三）美国内政部信息技术采购安全审查实证分析

美国在联邦层面的政府信息技术采购要求具有一般性，但仍然不能充分指引联邦机构在采购实务中完成信息技术的安全性审查活动。为此，很多美国联邦机构，特别是那些处理国家秘密或敏感信息的主要部门，均在立法授权的范围内制定了本部门的信息技术采购要求。以美国内政部（DOI）为例，其在信息技术采购活动中规定了大量的安全审查要求，主要包括人员背景审查和技术安全审查。

在人员背景审查方面，DOI 对所有可能访问自身信息资源的供应商雇员开展审查，其审查强度和水平与处于类似工作职位的联邦政府雇员相一致。根据 DM441 第 3 章[56]的规定，DOI 将联邦政府的职位分为国家安全职位和公共可信或非敏感职位两类。而在国家安全职位中，根据政府雇员能够访问的信息敏感度，DOI 又将其分为如下四类，包括特别敏感职位（SS）、[57]关键敏感 1 类职位（CS）、[58]关键敏感 2 类职位（CS）、[59]非敏感职位

---

〔51〕 参见 NSTISSC, *National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems*, us, 1994, p. 1。

〔52〕 根据 NSTISSC 的规定，信息系统管理者负责在整个系统生命周期中实现安全利益，包括采购、生命周期管理、资金、系统运行和维持。

〔53〕 指定的批准机构负责信息系统的授权工作，从安全风险的角度评估任务目标、商业案例、预算需求，决定可被接受的风险残留水平。

〔54〕 认证机构根据 SSAA 中确定的安全要求进行信息系统的技术审查，确定认证结果。认证机构必须独立于提供信息系统的组织。

〔55〕 为此，SSAA 在整个 NIACAP 流程中处于核心地位，国家安全系统的认证认可过程完全基于 SSAA 中确定的安全水平。NSTISSC 规定 SSAA 属于正式的官方协议，其中必须包括足够指导 NIACAP 有效实施的安全要求，具体包括：（1）操作环境和威胁；（2）系统安全架构；（3）建立认证认可的系统范围；（4）明确批准机构、认证机构、系统管理者和用户责任；（5）系统被认可的必要条件；（6）认证认可方案；（7）记录测试计划、认证结果和残余风险等。

〔56〕 Part 441: Personnel Security and Suitability Program; Chapter 3: Position Risk and Sensitivity Level Designation.

〔57〕 特别敏感职位（Special-Sensitive）包括能够访问敏感隔离信息（Sensitive Compartmented Information（SCI））的联邦机构负责人。

〔58〕 关键敏感（Critical-Sensitive）1 类职位包括给国家安全可能造成极其严重损害的职位，包括能够访问属于最高机密国家安全信息的；能够制定和批准战争计划的；具备涉及人员安全的调查权限的；具备执法管理职责的；与国家安全相关的其他职位。

〔59〕 关键敏感 2 类职位包括可能访问到国家安全秘密信息的非管理委托类执法活动职位。

(NCS)。[60] 同时,根据 DM441 第 4 章[61]的规定,背景调查会根据职位的不同分别适用背景调查(BI)、有限制的背景调查(LBI)、最低限度的背景调查(MBI)和独立范围背景调查(SSBI)等,审查内容涵盖供应商雇员的工作、教育、居住、执法、法庭记录、公共记录、信用记录等众多内容。根据实际情况,DOI 可附加国家机构检查和问询的要求。

在技术安全审查方面,DOI 对于不同类别的供应商有不同的审查要求,对商业现货(COTS)软硬件供应商仅要求其陈述质量控制内容,而对于开发或提供客户端应用服务、IT 服务外包或在线支持服务的供应商则具有广泛的审查要求,包括保密审查、[62]培训审查、[63]位置审查、[64]服务标准审查、[65]独立认证审查(IV&V)、[66]认证认可审查(C&A)、[67]质量控制审查、[68]脆弱性分析、[69]安全控制审查[70]和业务连续性审查[71]等内容。

四 我国网络安全审查制度保障功能的实现路径

国家网络安全审查保障功能需要依托完备的规范体系,鉴于制度目的的一致性,我国可以参照美国政府信息技术采购保障的相关政策法律框架来塑造国家网络安全审查的制度体系,特别是在政府信息技术采购和认证认可制度中附加对网络安全审查的特殊要求。同时必须考虑我国目前的政策立法现状和面临的现实需求。

(一)建立威胁态势感知的审查理念

风险的"泛在化"是网络社会的固有特点,技术的不确定性则客观上增加了风险产生的概率。与传统风险相比,网络风险正在越来越具有非对称性,例如,网络攻击愈发便捷而高效,攻击者借助信息技术几乎可以在世界任何地方发起攻击,而且很难被追踪和溯源。通常攻击行为都是即时性的,不会给防御者留下充足的反应时间部署安全措施。更为严重的是,网络攻击付出的成本与网络安全防护的成本不成比例,攻击者可以利用简单的漏洞或后门攻破采取复杂保护措施的信息系统。

在这种情况下,基于"风险排除"或"绝对安全"的传统保障理念将毫无意义,网络安全审查也不例外。随着网络安全态势的恶化,各国针对信息技术产品和服务的审查力度

〔60〕 非关键敏感职位(Non-Critical Sensitive)包括可能对国家安全造成损害的职位,包括能够访问国家安全秘密或保密信息的;可能直接或间接影响国家安全机构职责的。

〔61〕 Part 441: Personnel Security and Suitability Program;Chapter 3: Personal security and Suitability Program

〔62〕 任何能够访问 DOI 信息系统的供应商雇员在提供相关服务之前均须与 DOI 签署保密协议。

〔63〕 在提供服务之前,DOI 会审查供应商雇员是否通过了 DOI 终端用户计算机安全意识培训,培训内容定期更新。

〔64〕 DOI 要求软件开发及其外包活动必须位于美国境内,如果该服务需要在境外予以提供,供应商必须提交可行的安全计划,用以降低跨境通信、控制和数据保护的风险。

〔65〕 供应商必须满足 DOI 系统开发生命周期(SDLC)安全指南(DOI SDLC Security Integration Guide)和 NIST SP800 - 64 的具体要求。

〔66〕 DOI 要求所有的软件更新在部署到产品中之前必须通过独立的认证审查。

〔67〕 DOI 要求主要应用和通用性支持系统在投入使用前必须经过认证认可,并且每三年需要重新进行认证,在安全环境发生变化时也需要进行重新认证。DOI 要求供应商必须遵从 NIST SP800 - 37,800 - 18,800 - 30,800 - 53,800 - 60,FIP199,FIP200 以及 DOI 安全测试与评估指南和 DOI 隐私影响评估指南的具体要求。

〔68〕 供应商应当保证所有软硬件不带有恶意代码。

〔69〕 所有系统每月应当进行脆弱性分析,高风险系统和可以接入互联网的系统必须进行独立的渗透测试。

〔70〕 供应商应遵从 NIST SP800 - 53, FIP199,FIP200 有关安全控制的具体要求。

〔71〕 供应商应遵从 NIST SP800 - 34 和 DOI 持续性计划指南的具体要求。

在逐年增强,但效果却不容乐观。例如 2015 年美国人事管理办公室(OPM)因遭受入侵而泄露了包括联邦政府雇员在内的 2570 万个人信息,而讽刺的是,美国很多人员安全审查的政策均由 OPM 制定和实施。再如 2015 年,本身即为黑客公司的“Hacking Team”遭黑客攻击泄露了 400G 的内部资料,披露出该公司向多国政府出售零日漏洞进行监控或入侵,安全审查很难对未经披露的漏洞进行识别。

为此,将风险降低到可接受的程度就成为唯一可行的选择,那么,对风险进行及时的感知和应对就变得格外重要。威胁态势感知即是这样一种理念,其以承认风险的广泛存在性为前提,而以风险识别的“实时性”为内容,强调通过环境要素变化提供可预期的风险发生概率。

威胁态势感知强调风险发现与应对的实时性,有助于解决网络安全风险残余的棘手问题,但同时也要求网络安全审查改变目前“节点控制”的审查方式。国家信息技术安全研究中心总工李京春曾经认为,“我们以前所做的许多测评认证工作,只是集中在信息安全产品本身是否达到标准,达标后的信息安全产品是否还存在安全风险,存在多少、何等程度的安全风险,谁也不知道,也很少有人关心。”[72] 为此,有效的网络安全审查应当是始于信息技术采购的动态风险感知过程,涵盖信息技术的整个生命周期。例如,2009 年和 2014 年,美国和澳大利亚分别在全国范围内开展网络安全审查,评估网络安全保护水平。

(二)细化信息系统分级规则

国家网络安全审查制度的保障功能在于实现特定信息或信息资源的安全,这就需要明确相关制度意欲涵盖的信息系统边界。通常这类信息系统对于信息保密性、完整性和可用性的要求较高,在遭受信息安全减损时,对国家安全和社会公共利益造成的危害也更为严重。美国政府信息技术采购保障建立在成熟的信息系统分级基础之上,用于明确实施采购保障边界,信息保障主要针对国家安全系统,同时也适用于关键基础设施,这与我国《网络安全法(草案)》确定的安全审查对象基本一致。

但这样的审查对象仍然过于广泛,特别是越来越多的信息系统被划入关键基础设施的范围,国家是否有能力对如此庞大的信息系统实施有效审查就成为疑问。为此,美国在 2015 年《合并与持续拨款法案》中明确提出供应链审查的对象仅限于高影响或中度影响的信息系统。根据美国 NIST FIPS PUB 199[73] 的规定,中度影响级的信息和信息系统在遭受完整性、保密性和可用性减损后会对组织运行、组织资产和人员造成严重[74] 的不利影响。高影响级的信息和信息系统在遭受完整性、保密性和可用性减损后会对组织运行、组织资产和人员造成严重或灾难性[75] 的不利影响。

---

〔72〕 参见李雪、杨晨:《对话专家,建言审查》,《信息安全与通信保密》2014 年第 8 期,第 27 - 33 页。

〔73〕 联邦信息和信息系统安全分类标准,为联邦信息和信息系统建立了通用性的安全框架,帮助联邦机构提升信息安全项目管理和监管的有效性。

〔74〕 其中“严重”是指(1)会严重削弱组织完成任务的能力,但组织仍然能够实现主要目标和功能;(2)对组织的资产造成重大损失;(3)造成重大的财产损失;(4)对人员造成重大伤害。

〔75〕 其中“严重或灾难性”是指(1)会严重削弱组织完成任务的能力,以至于组织不能实现主要目标和功能;(2)对组织的资产造成重大损失;(3)造成重大的财产损失;(4)对人员造成严重或灾难性伤害,包括丧失生命或使生命遭受重大威胁。

同时 FIPS PUB 199 定义了信息系统的安全类型基本表达式,即信息系统的安全类别 = {(保密性, 影响度),(完整性,影响度),(可用性,影响度)},由此确定了多达 27 类的信息系统安全类型,用以指导联邦机构划分和确定其信息系统的安全等级。我国目前的信息系统分类分级依赖于等级保护制度,根据 2007 年《信息安全等级保护管理办法》的规定,我国的信息系统安全保护等级分为五级,尽管各级均给出了相应的判断标准,但其标准过于模糊,〔76〕无论对于信息系统的运营机构还是网络安全审查的实施机构而言,起到的指导意义非常有限,对于审查对象的确定往往需要基于个案分析,无疑会降低审查效率,也会增加审查机构的负担。为此,我国需要在现有信息安全等级保护制度的框架下,进一步细化信息系统的分级标准。

(三)实施供应链安全审查

美国政府信息技术采购保障的一大特点是根据风险来源不断适时调整和扩展审查范围。随着信息技术供应的全球化,IT 供应链的复杂程度大大提升,大量的信息技术产品和服务提供存在全球范围内的业务外包的情况,安全风险将具有更多的渗透渠道。为此,早在 2012 年美国审计局就明确指出联邦政府在政府采购中具有信息安全脆弱性,〔77〕认为"通过全球供应链提供的 IT 产品和服务存在威胁,要求联邦机构识别和防范 IT 供应链风险。"〔78〕2015 年,美国更是在全球范围内率先明确了供应链审查的具体要求,规定美国商务部、司法部、国家宇航局和国家科学基金会根据 NIST 制定的有关标准进行供应链风险审查,而上述机构也正在逐步落实该法案的审查要求。

反观我国,《国家安全法》和《网络安全法(草案)》均未明确网络安全审查的范围,如果根据 2014 年网信办的公告,我国的网络安全审查限定于"关系国家安全和公共利益系统使用的重要技术产品和服务",属于典型的"终端产品和服务"审查。这样会产生一个明显的弊端,即信息技术产品和服务生产或提供环节的安全状态不可见,无法判断供应商是否在信息技术供应中采取了适当的安全保障措施,而任何"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。"〔79〕并且"攻击者可能在产品开发、制造、生产或交付过程中篡改产品。"〔80〕

同时,"终端产品和服务"审查主要采取技术审查,即审查产品和服务是否存在潜在的安全风险,而欠缺对人员安全的考虑,无法解决供应商可信性的问题。大量的实践经验表明,恶意的内部人员往往比产品或服务缺陷导致的危害更为严重,网络间谍即属典型。在供应商雇员可以访问采购方信息系统的情况下,缺乏对人员安全的必要审查将会大大增加信息泄露或网络破坏行为发生的可能性。为此,基于终端产品和服务的安全审查并不能有效控制风险的渗透的过程,需要将我国网络安全审查范围扩展至整个供应链。

---

〔76〕 例如,我国目前的等级保护制度是以损害为划分标准的,但对损害的严重程度并没有给出相应说明。

〔77〕 包括联邦信息系统被嵌入恶意程序,使用不合格产品组件,存在非恶意漏洞,关键产品生产的中断等威胁。

〔78〕 参见 GAO, *IT Supply Chain National Security-Related Agencies Need to Better Address Risks*, *USA*, 2012, p. 6。

〔79〕 参见 Helen Peck, *Drivers of Supply Chain Vulnerability: an Integrated Framework*, *International Journal of Physical Distribution & Logistics Management*, 2005, pp. 210 - 232。

〔80〕 参见 Scott Charney, Eric T. Werner, *Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust*, Microsoft, 2011, p. 1。

（四）完善信息安全标准体系

从美国 DOI 的安全审查过程可以发现，供应链的网络安全审查会非常复杂，需要依靠大量的安全标准。有一种观点认为，美国针对我国华为和中兴的审查并没有依据安全标准，而是充斥着怀疑和主观臆断，我国的网络安全审查制度也应当“审查过程、标准、机制完全不公开，也不需要披露原因和理由”，[81]或认为“信息网络安全审查决策是在对相关产品、技术、服务、系统等安全性能和提供人背景等情况进行判断基础上，依据国家经济社会发展情况、对外经贸和外交形势做出，不需要有具体的审查标准”。[82]这种考虑有一定合理性，因为明确而固化的审查标准会弱化审查机关的自由裁量权，容易产生被动局面。然而，如果从审查活动的有效性分析，缺乏审查标准的审查制度仍然只能称为“政策工具”或“贸易壁垒”。因为这样的审查制度无论对于供应商而言，还是审查机构而言，均无法提供明确的审查指引，也就无法形成所谓的“可期待规范”。特别是考虑到我国的网络安全审查制度并不专门针对外国供应商，而是针对国家网络安全风险设立的保障制度，如果缺乏审查标准的支撑，那么制度整体的有效性和正当性都会存疑。因此，在国家网络安全审查向供应链审查进行扩展时，信息安全标准化建设也需要同步加快。

五　结　语

鉴于英美针对我国信息技术企业实施安全审查的现实影响，国家网络安全审查制度存在一种错误的功能认知，以“反制”为定位的网络安全审查并不能解决我们面临的安全问题，反而会将审查制度降格为纯粹的“政策工具”，甚至在某些情况下并不能起到应有的制度规范效果。我们必须意识到目前网络安全风险的“泛在化”态势，明确国家网络安全审查制度的保障功能，将其作为一项积极的保障手段，而非被动的防御措施。将国家网络安全审查的制度功能定位于保障，同样也能澄清制度独立性问题，其与外商投资国家安全审查在审查重点、审查对象和审查内容均有所区别，网络安全审查旨在保障国家网络安全，通过对信息技术产品、服务乃至供应链的安全审查，防止产品提供者非法控制、干扰、中断用户系统，非法收集、存储、处理和利用用户有关信息。在此基础上，国家网络安全审查保障功能的实现需要依托完备的制度支撑，在此方面可以参照美国政府信息技术采购保障制度的有益经验。为保证国家网络安全审查制度保障功能的实现，应当建立基于风险的威胁态势感知审查理念，细化信息系统分级，实施供应链安全审查和完善信息安全标准体系。

［本文为 2015 年国家社会科学基金重大项目“网络社会创新治理研究”（15ZDA047）的研究成果。］

〔81〕 参见张莉：《网络安全审查的国际经验及借鉴》，《信息安全与通信保密》2014 年第 8 期，第 67 页

〔82〕 参见许长帅：《从国家行为角度探讨构建信息网络安全审查制度》，《现代电信科技》2014 年第 10 期，第 13 页。

[**Abstract**] National cyber security review system is an innovative system aimed at enhancing the state's ability to safeguard national cyber security. However, there are many controversies over and doubts about the existing legislation and policy on this system. The first issue needs to be clarified is the institutional function of the system. The one-sided "counter" function can not solve the cyber security problems faced by China, but will degrade the system into a pure "policy tool". Examining the system from the perspective of the safeguarding function is conducive to clarifying the questions relating to the independence of the system and its differences from national security review of foreign investment in the emphasis, target, and content of review. In order to ensure the realization of the function of this system, China should gradually establish the risk-based "review of threat situational awareness" to solve the difficult problem of risk residual, further elaborate the grading of information systems, define the scope of implementation of the system, carry out review on security of supply chain, emphasize the combination of background review and technical review, improve the system of information security standards, and provide clear compliance guidelines for the review agencies and suppliers.

(责任编辑:支振锋)