基于国家安全的知识产权调查相关问题研究*
——以华为、中兴为例

■ 王淇**
国家知识产权局知识产权发展研究中心 北京 100088

摘 要：近年来，美国政府对华为和中兴开展了一系列调查，这些调查回溯到2012年，早在一份有关国家安全的报告中已有端倪。因此，重读这份报告，审视调查的复杂背景，厘清调查的来龙去脉，把握调查的醉翁之意，预判未来的调查动向，有助于从国家层面应对国家安全调查，防范知识产权风险，维护企业和国家的合法权益。

关键词：国家安全 知识产权 调查
DOI:10.11842/chips.2019.01.004

近日，经加拿大司法部确认，华为首席财务官在温哥华遭逮捕。美国政府也在寻求引渡，保释听证会业已安排。此次事件，华为的回应是“不实报道”，但是从此前美国政府对华为和中兴启动的一系列调查来看，基于国家安全的知识产权调查是重中之重[1]。追溯起来，早在2012年10月8日，美国众议院常设情报委员会（以下简称“委员会”）就公布了《中国通信公司华为和中兴通讯涉及的美国国家安全调查报告》（以下简称“报告”），认定一直试图在美国扩张的华为与中兴通讯的设备对美国核心基础设施构成威胁，建议美国政府基于国家安全利益的考虑，封锁涉及上述两家公司的并购以及其他市场行为，避免使用这两家公司的设备，美国企业也应寻找可替代华为与中兴通讯的设备供应商。当时，报告一经问世，2012年12月18日，欧盟就表示将继续搜集相关证据，就是否对华为和中兴通讯涉嫌不公平贸易行为展开调查做出决定。自这一报告开始，美国政府即开始对华为与中兴通讯投出不信任票，志在必得要将其驱逐出美国市场。时至今日，美国对于中兴和华为的调查仍在继续。

因此，仔细研读2012年的这份报告非常有必要，透过这份报告，可以看出美国实际上是以这些议题作为攻防武器，将国家安全战略列入了全球经济战略的视野，以国家安全的名义，在通信产业竭尽所能地保障本国的信息垄断利益，其中最为关键的就是维护知识产权的优势地位；同时，由于跨国公司的并购已经成为直接投资的重要方式，而知识产权又日益成为并购的核心资产，因此，美国在全球经济战略的安排上，逐渐将知识产权与投资进行关联，通过国内法的设计，在国家安全的旗号之下，不断扩大对外国投资的审查范围，将产业、财经、知识产权、外国控制等考虑因素统统纳入调控之中，形成外国企业在美国市场准入的壁垒。

1 调查的缘由

委员会在报告中介绍了发起调查的原委，主要是应

* 国家知识产权局2018年度软科学研究项目“国际知识产权热点问题研究”的部分研究成果，负责人：韩秀成。
** 王淇，博士，国家知识产权局知识产权发展研究中心发展处副处长，副研究员，研究方向：知识产权法律与政策研究。

华为的请求而起。2011年2月，在一封写给美国国会的公开信中，华为公司请求这些曾质疑过华为战略意图的议员们，全面调查该公司在美国的经营业务。这封长信的作者是华为公司副董事长胡厚崑，他在信中引用了亚伯拉罕·林肯和奥巴马总统的话，来为华为公司在美国的业务实践、公司治理以及扩大在美投资等方面做出辩护。他最后称，这些毫无根据的指控严重损害了华为公司在美国这样一个全球最大的通信设备市场的声誉，他要求美国政府能够对此开展全面的调查。在公开信的结尾，他表达了对美国监管调查公平公正的信心：

> “美国政府部门在管理上高效以及公平和公正，给华为投资美国10年过程中，留下了深刻的印象。我们相信，如果能够通过美国的公平与正义的调查流程，能证明我们是一家真正的商业公司。”***

但是，即便调查是应华为的请求而启动，但是负责调查的委员会所秉持的可能是另一套逻辑。委员会在报告的开篇，即说明美国国家安全利益因为通信设备链的脆弱而备受威胁，而这一风险来自4个方面：国家受制于相互依存的核心基础设施系统；这些系统面临的不同程度的风险；网络间谍行为的风起云涌；消费者越来越依赖少数几个设备商。

首先，国家对基础设施的倚重不仅仅只是消费者对电脑系统的使用，更重要的是多重核心基础设施建立在通过通信系统进行信息传输的基础上。这些现代化的多重核心基础设施涉及国计民生的一系列环节，包括电力系统、银行金融系统、能源和水资源系统、运输系统等等，每个都离不开计算机控制系统。而且系统之间的相互依赖又使整个系统格外脆弱，因为其中一个环节失控都会导致整体的严重后果，从而影响美国社会正常运作的方方面面。

其次，伴随着这种依存度的国家安全的脆弱程度相当广泛，威胁从系统内部打击到有预谋的政治国家的网络间谍和攻击行为都有可能。联邦调查局确信网络对供应环节的攻击主要来自政治国家和犯罪分子。同样，国家反间谍执法机构也认为“外国企图搜集美国技术和经济信息将会持续高发，并将对美国的经济安全持续不断构成巨大威胁”。

再次，美国政府必须高度关注与其政府关系密切的公司的产品，它们给美国带来了最高级别和最严重的间谍威胁，例如中国。最近的黑客攻击很多来自中国，而且通过他们恶意的网络操作，这些黑客寻求经济和国家安全信息的行为很难探测到。

最后，华为和中兴通讯这些中国通信企业在全球通信市场上，迅速成长为举足轻重的棋手。如果是其他的产业，这一进步也许不会引来特别关注。但是这些企业试图控制用于间谍和其他恶意用途的敏感设备和基础设施，而其一股独大的市场份额引起了美国和其他国家的关注。除了美国，澳大利亚在国家宽带基础设施项目上驱逐华为时也表达了同样的担忧。英国则启动了一项评估机制以限制华为进入市场，他们将在华为销售每一件设备和软件之前一一予以评估。

2 调查的逻辑

2011年11月，情报委员会开始调查在美经营的中国通信企业。在正式调查之前，委员会已经进行了初步的调查，证实了中国通信产业、在美经营的特定企业的历史和操作以及这些企业与中国政府的潜在联系。初步调查最重要的是查明了中国通信企业因为与中国政府之间存在的千丝万缕的关系，给美国国家安全带来隐患。这些企业不同程度受到政府的影响，或者为情报机构提供了通信渠道，由外国政府采取的进一步的经济和外国间谍已成为网络间谍行为的显著形式。这一初步调查与正式调查的结论一致，都认为华为和中兴提供给美国核心基础设施的设备所带来的风险会削弱美国国家安全利益；采取的思维方式也一致，都认为中国是网络间谍高发国家，而华为和中兴通讯是中国支持的龙头企业，掌握了供应链的优势地位，会在通信设备上设置“后门”，帮助中国搜集情报，从而威胁国家安全，从中不难窥见这一调查的背后逻辑。

2.1 为什么调查中国企业

委员会在报告中称是因为“最近的研究都表明中国是最大的网络攻击国”，这主要是指美国国家反间谍执法机构2011年11月3日发布的一份报告：《外国间谍在

*** 摘自《中国通信公司华为和中兴通讯涉及的美国国家安全调查报告》。

网络空间窃取美国经济机密》。因为委员会与该执法机构在工作职能上需要互相配合，先由委员会负责评估国外情报活动的威胁，然后由反间谍机构有效锁定并且消除这些威胁。

该报告搜集了美国中央情报局、联邦调查局等13个机构2009年到2011年的相关数据，宣称中国和俄罗斯将自己视作美国的战略竞争者，它们也是美国经济信息及技术的最积极收集者。这两个国家在实施对美国企业、政府机构及大学的经济间谍行为时，经常使用网络。由于人们都习惯将商业记录、研究成果及经济数据以数码形式存储，外国黑客们很容易就能迅速并风险极小地收集极大量的信息。该报告还称，外国情报收集者们最感兴趣的领域包括医药品、信息技术、军事设备、高端材料及制造工艺等。该报告援引美国国家科学基金会的数据称，2008年美国各行业、政府部门、高校及非盈利性组织花在科研上的经费为3980亿美元，因此，经济间谍犯使美国科研投入的效益“大大受损”。由于智能手机和云计算的使用，黑客们将有更多可趁之机，外国经济间谍的步伐在接下来几年里将“步步升级”。而面对这些外国间谍威胁美国企业对此一直不够重视：“只有5%的企业财政主管们会操心网络安全问题，仅13%的企业拥有跨部门的网络风险小组。”

反观委员会报告的理论基础，即国家安全利益的4个风险来源：国家受制于相互依存的核心基础设施系统、这些系统面临的不同程度的风险、网络间谍行为的风起云涌以及消费者越来越依赖少数几个设备商，不难看出这两个报告的一脉相承。出于对这样的担心，对中国的调查似乎是势在必行，那么，为什么仅针对中国而不加上俄罗斯的企业呢？报告引用了国家反间谍执法机构的说法，即“中国企业从事着全世界最活跃也最持久的经济间谍犯罪行为”。相形之下，虽然莫斯科情报机构实施了一系列搜集美国经济和科技信息的行，但是俄罗斯的攻击行为比中国少。

而且，委员会认为：在全球通信产业的供应链上，美国是中国最大的目标国。中国可以通过通信设备，从美国政府和私有企业那里修改或者窃取信息，获得昂贵费时的研究成果来确保中国的经济地位。将恶意硬件或者软件植入中国生产的通讯零件或者产品中卖到美国，在危机或者战争期间会因中国的远程操作，而将美国的国家安全系统的开关置于他国之手。而且，合同中有帮助条款，服务商以此为借口会利用授权以合法目的掩饰不法行为。

报告由此将捕风捉影的网络间谍风险具体体现到了供应链的现实风险之中，而美国政府对此的关注已有数年。2009年，白宫发布的《国家网络安全综合倡议》中将“供应链风险管理”列入了12大核心基础设施保护之一，正式成为国家关注的重点。美国的执行分支也将根据2012年1月发布的《全球供应链安全国家战略》的要求，跟踪评估供应链问题。这一战略认为供应链风险管理的重要方面就是要正确“认清并识别供应链上的薄弱环节，不论是运用了可能植入有害产品或者材料的系统还是受到有意识的攻击、事故或者自然灾害的干扰”。报告明显将中国企业视为供应链上的薄弱环节，因此对中国企业的调查就事关国家安全了，即便这一连续推导的链条中存在很多跳跃环节，但是委员会直言不讳的“中国的经济地位”成为了很好的思维帮手。

2.2 为什么调查通信产业

按照委员会的逻辑，在供应链复杂的构成之中，只对通信产业进行调查，是因为其在美国国家安全中扮演了关键角色，而美国的通信产业越来越依赖全球设备和服务供应链的生产和交付。这一依赖具有重大的风险，即其他个人或团体，包括那些外国政府支持的，有可能也将会利用和破坏网络的可靠性。中国政府可以通过对通信产业的控制，授意其在产品流水线上将元器件和系统做手脚，作为情报组织刺探信息的工具。即便产业界不予合作，情报机构也可以买通企业内部的技术人员或者管理人员。而且根据中国法律，中国政府可以国家安全为名，责令通信企业予以配合，运用其系统或者途径从事不法行为。

如果要保护网络的安全和功能，要防止国家安全和经济威胁祸及网络，就要客观全面地评估供应链的风险。英国政府率先采取了行动，与华为协议成立了独立运作的网络安全评估中心。该中心对华为安装到英国通信基础设施中的设备和软件进行独立的审核，并将审核的结论通报给相关的英国运营商和政府。英国政府借助设立这一中心来控制华为的产品用于基础设施可能带来的网络安全风险。

华为中兴在进入美国市场之时也提出了相类似的

动议，但是建议由私营企业例如电子福利社，而不是由美国政府来管理。美国考虑到中国政府利用华为或者中兴的产品来间谍或者网络攻击行为，而且美国市场的规模和程度之大，并未采纳这一建议，因为现代科技发展的步伐已使独立第三方无论在事前还是事后都无法全面评估，标准的程序如信息技术安全评估一般准则也难以适用。评估需要设备商的配合和资助，最终，英国政府否决了评估报告，并且得到了运营商的支持。

报告对英国经验的介绍，实际上否定了这一评估的可行性，认为网络安全评估中心无法保障供应链的风险控制。委员会认为有效的评估需要通过完善的工程设计和制造流程，能检查产品的整个生命周期，并审核产品方方面面的信息，包括零部件、整个产品和环境，这样得出的结论才是真实可信的，这就涉及到了对具体企业的调查。

2.3 为什么是华为和中兴通讯

华为是主动请缨要求调查的，而委员会为何又加上了中兴通讯呢？根据报告的解释，华为和中兴通讯是中国通讯设备的两家龙头企业，都与政府来往过密；两家企业都在美国成立了子公司，致力于在美国扩大市场份额。虽然华为的知名度更高，但这两家企业在政府支持和开拓市场方面很相似，所以委员会同时调查了华为和中兴通讯。

既然可以增加调查对象，为什么其他可能对美国供应链造成威胁的通信企业没有调查呢？华为和中兴通讯也认为，委员会不应只调查这两家公司而排除在中国制造通信设备的所有其他公司。委员会给出的解释是虽然非中国籍企业，包括美国的科技公司，也在中国生产通信产品，但是，除了制造地点，公司所有权、经营史和产品的目标市场对风险计算也很重要。报告称："这两家可能不是唯一存在风险的公司，但它们是进军美国核心网络设备市场中的通信设备公司中，在中国创立的、国有的最大的两家。委员会为了评估供应链的风险，决定首先把重点放在已知最大的漏洞上，并期望这项调查的结论为如何看待中国和其他国家运营的其他公司或制造商对供应链的潜在威胁而提供依据。"

如果说调查通信产业是委员会行使自由裁量权的话，那么委员会对于调查华为与中兴通讯的解释则耐人寻味，这一调查在开始之际即预设是已知最大的漏洞，而且将这两家企业视为国有企业，同时默认对供应链构成了威胁，而接下来的流程则是为上述假设寻找证据提供证明而已，最终的调查结论也就不难想象了。

3 调查的过程

委员会的调查主要是评估这些企业意图在美扩展会给美国带来的风险指数，调查包括两个独立但有相互关联的部分：一是对企业历史、运作、财务信息以及和中国政府和政党的潜在联系的公开信息的评估；二是保密信息的评估，包括美国情报协会的项目和分析。前者体现在了公布的这份报告之中，而后者则被写入了未经公开的另一份保密报告之中。

委员会的调查方式包括约见公司和政府官员，要求提供详尽的文件，并举行了听证会。2012年2月23日，委员会副主席鲁斯伯格与成员努涅斯议员、巴赫曼议员访问了华为深圳总部，参观了华为产品线以及制造工厂，包括华为副董事长胡厚崑在内的7名华为高管与其进行了讨论和面谈。2012年4月12日，委员会成员又访问了深圳中兴总部，包括中兴高级副总裁朱进云在内的8名中兴高管带其参观了公司并进行了会谈。2012年5月，委员会由达切·鲁伯斯伯格和其他3名委员，飞到香港再次会见了华为和中兴高管，并见到了华为总裁任正非。会见之后，委员会又进一步要求提供书面文件，但两家企业都没提交内部文件。因此，2012年9月13日，委员会又举行了一场公开的听证会，华为资深副总裁、美国公司法人代表丁少华和中兴北美及欧洲区高级副总裁朱进云与会作证，每人发言20分钟，委员会提供翻译帮助将问答译成英文。

对于这些调查方式，委员会都不甚满意，认为证人们的回答比较含糊不清：不了解通用的术语；不回答内部党组织的组成状况；拒绝提供在美运作的情况；并且回避知识产权保护历史的问题。正是这两家公司在调查中的不予配合，使得委员会的这种关注上升到了国家安全的高度。因此，除了与当事企业的谈话之外，委员会还约谈了业内专家以及企业的在职和离职员工以及在美相关企业的职员，但是这些人员都以会受到打击报复为由，未能公开作证，而委员会称他们都说华为或者中兴的产品存在瑕疵，管理层也有其他不道德或者非法行为。

委员会称这一调查很难明确华为和中兴的企业性质、企业内部党组织的职能和在美运作的细节，因为遇到了很多挑战，包括：欠缺透明度的中国企业；公信力不足的官僚体制；私有企业对提供真实可信资料的顾虑，以及对讨论这些顾虑的后果的担忧；来源不明的网络攻击。最终，委员会将调查的重点放在两家公司与中国政府的联系上面，这其中包括来自政府和国有银行的支持、两家公司高层与中国共产党的人际关系、两家公司为中国军方和情报部门所做的工作。特别是，华为和中兴通讯是否获得了中国政府在方方面面的资助和支持。

委员会调查的目的是为了确定华为与中兴通讯对美国通信供应链是否构成威胁，对于美国国内网络攻击确切来源方面，美国无法确认这些攻击与中国产业界、政府和黑客群体直接相关。尽管如此，因为委员会预设中国通信企业帮助中国政府危害美国通信供应链的安全，所以即便两家公司积极配合调查的各个环节，出示各种各样的内部文件，回答并不友好的问题，但是委员会的关注始终集中在其与政府和军方的关系上以及是否在美合法经营之上，且对保密信息的调查又不公开，这一调查自始至终很难说保证了公平公正公开。

4 调查的结论

委员会的职责是研究并审查各国的情报活动对美国核心基础设施的威胁，在此次专门调查之中，关于华为和中兴通讯所涉及的国家安全事项，委员会的调查将这两家公司是否对美国通信供应链构成威胁转换为其与中国政府之间是什么关系，预设的问题是如下5个：

（1）华为和中兴通讯的公司历史和治理模式，包括与中国政府、军方或者党的初始关系是什么？

（2）中国政府或者党用什么方式、在何种程度上控制或者影响了华为中兴的决策、操作和企业战略？

（3）华为和中兴通讯作为龙头企业，中国政府是否为其提供了不正当的特殊待遇或者财政资助？

（4）华为和中兴通讯深圳母公司对在美国的子公司有多大的影响力？

（5）华为和中兴通讯是否遵守了法律义务，包括知识产权保护和国际制裁（例如对伊朗的制裁）规则？

基于委员会既定的调查逻辑和假设，调查的结论是华为和中兴通讯提供给美国核心基础设施的设备所带来的风险可能会损害美国国家安全利益。

在报告中，委员会称：保护知识产权和遵守美国出口管制法律，是美国利益的核心关注点。公司遵守这些法律的能力，是检验其遵从国际商业行为准则和避免政府过度影响能力的有效方式。因此，能否保护知识产权是遵守美国法律的重要判断标准，所以特别说明一下委员会对华为和中兴通讯在知识产权保护上的调查，结论是这两家公司漠视知识产权保护，并可能存在侵权行为。

值得注意的是，在对华为的调查结论中，委员会提及了华为与思科的诉讼[2]，以此证明华为侵犯了美国公司的知识产权：首先，在华为与思科的那起诉讼中，华为的高管承诺公司将移除侵权产品；其次，思科在和解协议中要求华为“更新并且更换所有被控侵犯了版权或者其他知识产权的产品”；最后，在2012年9月13日的听证会上，丁少华拒绝回答华为设备中是否存在思科代码这一明确的问题。因此，委员会认定：华为对知识产权侵权的否认，并没有可靠的证据支持。由于华为未能出示任何内部文件或证据来支持其说法，委员会认定华为的所作所为至少是漠视了其他实体的知识产权。

5 调查的建议

在报告的最后，委员会提出了5大建议：

（1）美国应当审慎盘查中国通信企业持续打开的美国通信市场：美国情报协会必须始终警惕并关注这一威胁，尽可能积极主动告知私有部门企业这些可能的威胁；国外投资委员会基于国家安全利益的考虑，必须封锁涉及华为和中兴通讯的并购、合并和接管。立法建议扩大国外投资委员会的权力，建议收购协议应受相关委员会的全面审查；美国政府部门，尤其是敏感部门，不应采用华为或者中兴通讯的设备，包括零部件。与此类似的是，政府承包商，尤其是承接美国敏感项目的，应当在履行合同时排除华为和中兴通讯的产品。

（2）强烈建议购买华为和中兴通讯的设备或者服务的美国私人经营企业考虑安全方面的长期风险，同时还建议美国网络服务商和系统维护者另觅其他的卖家。委员会根据获取的公开和不公开的信息，认定华为和中兴通讯受中国政府的影响，因此对美国及网络系统构成了安全的威胁。

（3）美国国会所辖的委员会和行政分支管辖的执法

机构应当调查中国通信产业的不当交易行为，密切关注中国对其龙头企业的持续不断的财政资助。

（4）敦促中国公司更加开放与透明，包括履行严格的透明义务在西方证券交易所上市，提供前后一致的由独立第三方审核的财务信息和网络安全程序，符合美国法定的信息和证据提交标准，遵守一切知识产权法律和标准。特别是华为，必须更为透明并且履行美国法律义务。

（5）美国国会所辖的委员会应当考虑立法动议，以深入挖掘具有政府背景的或者其他明显不应被信任的电信企业来构筑关键基础设施所带来的风险。这样的立法应当包括增加私有企业之间的信息风向，加强国外投资委员会审查购买协议的职能。

从这5个建议来看，委员会关注的重点看似与供应链有关，但是从建议的对象来看，主要面向国外投资委员会和私营企业，涉及的更多的是美国通信市场的管制；从所涉的美国法律来看，主要是指知识产权法律和标准。至此，这一公之于众的报告表明：对华为和中兴通讯的调查，虽然因国家安全的缘由而起，但是醉翁之意并不在此，而在于华为和中兴通讯在与美国公司的竞争中表现出的实力，尤其是知识产权上的进步，以及在美国的通信市场上独步天下的潜力，构成了委员会的真正关注，这才是他们认为美国国家安全真正受到威胁之处。

在这一推理之中，知识产权与企业或者投资的关系不难理解，知识产权在通信产业中的重要性也不言而喻，那么，这些问题又是如何与国家安全联系到一起的呢？这就需要超越报告的文本，从美国的国家安全战略与全球经济战略的融合上来品评。

6　应对美国国家安全战略的建议

结合这份报告的调查思路与结论，我们可以看到：进入信息时代以来，美国将国家安全战略与全球经济战略合二为一，在主体上将企业和产业一并纳入，在内容上将企业性质、知识产权、投资等与国家安全紧密相连，在实施上令情报部门、投资主管部门以及执法机构相互分工与配合，以维持美国在价值观、企业与产业上的至上地位。但是，新兴经济体在全球化的作用增强，改变了发达国家主宰一切的局面。发达国家与新兴经济体都需要调整姿态，寻求新的全球治理模式，这会带来更多的谈判与协商，也会带来更多的调查与纷争。

早在2012年委员会的调查对象虽然只是华为和中兴通讯，但是提出的建议则对我国的知识产权等国际谈判、通信产业以及跨国公司都有一定的影响，而且这一建议还具有示范效应，可能给其他领域的产业和企业造成连带的后果。时隔6年之后，我国在经历了“301调查”、华为中兴等企业在接受了一系列调查之后，再回过头来看当时的调查，我们看到了美国政府思路的连续不断与调查的锲而不舍。基于此，针对相关国家安全的知识产权调查，建议如下：

（1）确立国家安全战略

基辛格认为：美国辩论中经常涉及的问题——国际法、多边解决、民众的同意——在中国的战略分析中常告阙如，除非是作为达到既定目标的工具[3]。

美国有着明确的国家安全战略。国家国家利益分成关键利益、重要利益和人道主义等3类。其中第一类是指那些关乎国家的生存、安全的生命力，具有广泛的和压倒性利益，包括物质安全、公民安全、经济福祉、基础设施的安全等。美国国家安全审查重点在这一类。而我国强调经济建设为中心、用发展战略代安全战略，强调公共利益而忽视安全上的国家利益，存在着国家利益不明晰、国家安全战略不明确、出了问题只能被动应付的局面[4]。

我国应借鉴西方国家纷纷出台的为维护本国国家安全专门立法的经验，结合我国政府体制现状，尽快构建出台我国关于外国投资影响我国国家安全的专门立法。

具体而言，在相关立法中应明确以下几点：

第一，应当明确国家安全审查的机构。我国应设立外国投资国家安全审查委员会，专门负责国家安全审查工作。

第二，应当明确国家安全审查的对象。国家安全审查的对象应针对特定的外国投资，这些投资应是涉及我国核心技术的行业（如国防军事核心技术行业）、关系国民经济命脉的关键敏感行业（如战略物资储备行业、重要装备制造行业）、关系重要资产的行业（如知识产权资产、重要能源资产、有关公共安全的核心基础设施资产），包括但不限于军工、能源、交通、通讯、金融、文化等产业。

国家安全审查机构进行国家安全审查还应当考虑该外国投资数额、占投资企业股权比例、所投资企业的市场份额以及对我国劳动力就业的影响等。

国家安全审查机构可以确定一定数量的需要特别保护的企业名单，可以随时对它认为的任何可能影响我国国家独立、国家统一，影响我国政治、军事、经济等领域安全的外国投资进行审查。

第三，应当明确全国人大及其常委会有权对国家安全审查委员会的工作进行监督检查。

第四，所有以“国家安全”为由的政策和规定应与WTO《与贸易有关的投资措施协定》所提倡的“便利跨国投资、保证自由竞争”保持一致，并且不应对中国企业对外投资构成明显的歧视。否则，中国可以利用WTO平台的纠纷解决机制提出申诉[5]。

第五，根据世贸组织的基本原则，在我国外资并购国家安全审查过程中，增加立法透明度，提高公众立法的参与程度，采取听证程序，广泛听取意见。对于国家安全的审查目的、审查机构和审查程序，特别是国家安全审查的内容具有稳定性和可预测性[6]。

（2）培育通信优势企业

针对我国企业开展的境外投资并购，我国政府应当提供以下支持：

第一，我国政府应在宏观层面进一步加强与相关东道国在政治、经济、文化等领域的沟通交流。我国政府应向相关东道国阐明：中国企业的境外资源能源类、高新技术类投资合作将为实现全球资源能源、高新技术的合理分配和使用、发展世界经济和提高各国人民福利水平做出贡献，最终实现“双赢”乃至“多赢”；中国企业的投资有助于发挥各自的优势，实现资源能源（或技术）和市场互补。通过政府层面的来往和宣传，增强政治经济上的相互信任，消除减缓相关国家政府和民众过于敏感的国家安全顾虑及激烈的民族情绪。

第二，由国家商务部牵头，加快与有关发达国家谈判，解决相互间的自由投资问题，适当时机签署双边自由投资协定，化解欧美发达国家利用国家安全名义实施投资保护主义的趋势。

（3）开展双边谈判与合作

从以往的经验来看，美国在大张旗鼓的一轮调查之后，紧接着就是新的一轮谈判的启动。而从报告的调查结论来看，可能会涉及两个方面的议题：

第一，知识产权与投资。

在前Trips时代，美国以打开美国市场或者进行贸易制裁的方式，先通过双边谈判，然后在多边谈判机制中将知识产权与贸易联系到了一起，关于投资只涉及与贸易有关的一小部分：根据Trims协议第1条的规定，协议仅适用于“与货物贸易有关”的投资。到了后Trips时代，发达国家与发展中国家相互的投资、生产、消费，已经改变了原来的全球化面貌。以下图为例，我国从2000年到现在海外投资的额度大幅度攀升，都表明投资成为我国新的关注点。

而美国则通过对投资设立知识产权等标准的审查，来控制国外投资进入美国市场，因此，将与知识产权有关的投资措施排除在外，必是未来国际投资立法的重要课题。

第二，供应链风险与网络安全合作

供应链的风险是各国共同勉励和关心的问题，美国联邦政府和军方成立了专门的组织。目前，自2012年调查之后，已经有4个工作组开始运转：高级指导组、采购

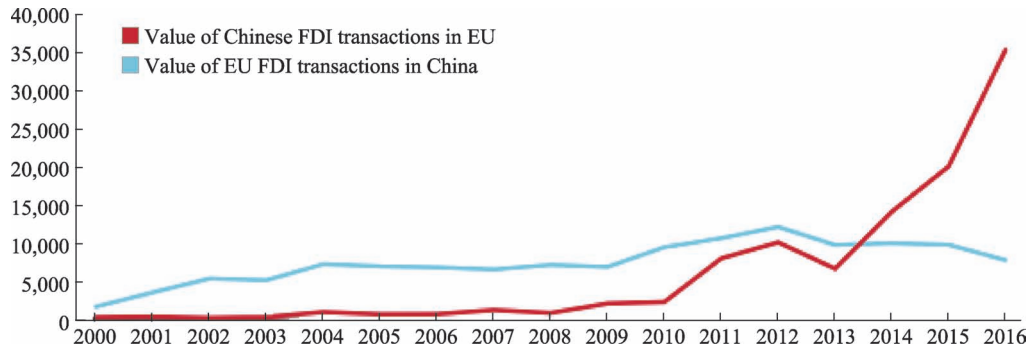

图1

政策和法律分析工作组、生命周期过程和标准工作组、威胁信息共享工作组。其中，高级指导组起组织协调作用，具体由国土安全部（DHS）和国防部（DOD）负责；采购政策和法律分析工作组旨在通过政策和法律手段加强IT采购安全，该工作组将在政策和法律层面评估是否可以利用情报部门提供供应链安全风险信息，以及利用非情报部门（包括销售商）提供重要信息，具体由管理和预算办公室（OMB）以及总务管理局（GSA）负责；生命周期过程和标准工作组旨在制定供应链安全风险管理标准和有关指导性文件，具体由NIST和国防部（DOD）负责；威胁信息共享工作组负责在整个联邦范围内共享供应商威胁分析信息，具体由国家情报总监办公室（ODNI/ONCIX）负责[7]。

目前，工作组中的很多活动都已开展。例如，在生命周期过程和标准工作组，NIST提出了“广度防御（Defense-in-Breadth）”的战略，这是对美国国家安全局在《信息保障技术框架》中提出的“纵深防御（Defense-in-Depth）”战略思想的发展。NIST认为，纵深防御战略侧重于通过分层的防御体系对网络和系统进行保护，其关注的是产品在运行中的安全，因而完全不能解决供应链安全问题。而广度防御战略的核心是在系统的完整生命周期内减少风险。在这一领域，我国可以与美国展开合作，并加强我国IT供应链的管理，应对网络安全的供应链风险。

参考文献：

[1] 玉品琨. 美国司法部调查华为是否违反对伊制裁规定[N]. 金融时报, 2018-04-26.
[2] 卫晓. 思科与华为十年争锋[J]. 中国中小企业, 2012(12): 54−57.
[3] 亨利·基辛格. 论中国[M]. 北京: 中信出版社, 2017.
[4] 周建明, 王海良. 国家大战略、国家安全战略与国家利益[J]. 世界经济与政治, 2002(4): 21−26.
[5] 石军. 通信企业“走出去”的政策风险及应对策略[J]. 通信管理与技术, 2010(1): 1−3.
[6] 杨迅雷. 论美国外资并购国家安全审查制度[D]. 对外经济贸易大学, 2006.
[7] 左晓栋. 美国政府IT供应链安全政策和措施分析[J]. 信息网络安全, 2010(5): 10−12.

Research on Related Issues of Intellectual Property Investigation Based on National Security

——Take Huawei and ZTE as Examples

WANG Qi

Intellectual Property Development &Research Center State Intellectual Property Office of China, Beijing 100088

Abstract: In recent years, the U.S. government has launched a series of investigations into Huawei and ZTE, which dated back to 2012 where there was a well-documented report on national security. Therefore, by re-reading the report, examining the complex background of the investigation, clarifying the origin and development of the investigation, grasping the meaning of the investigation and predicting the future trend of the investigation will definitely help to deal with the national security investigation at the national level, guard against intellectual property risks, and safeguard the legitimate rights and interests of both enterprises and countries.

Keywords: national security; intellectual property; investigation

（责任编辑：黄洪天；　责任译审：毛子英）