彎曲評論

科技 · 人物 · 潮流

美国众议院情报委员会对华为和中兴公司引发的美国国家安全问题的调查报告

Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE

A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence
U.S. House of Representatives. 112th Congress. October 8, 2012

翻译: 陈怀临等
弯曲评论创办人, 北极光创投投资顾问
2013年4月20日

目录

美国众议院特别情报委员会主席和高级成员

对中国电信公司华为与中兴对美国国家安全引发的问题的调查报告

概述

2011年2月，中国领先的电信设备制造商华为公司对美国政府发表了一封公开信，信中否认针对其公司或设备的安全担忧，并申请美国政府对其公司运作进行全面调查[1]。华为公司显然正确的意识到，和相信，不经过美国政府对其公司的全面调查，美国不会放心华为的设备及相应的服务应用于美国电信网络中[2]。

众议院特别情报委员会（以下简称“委员会”）于2011年11月发起了本次对在美国有商业活动的中国电信公司对美国造成的情报和安全威胁的调查。在发起正式调查之前，委员会对这个议题进行了初步的评估，结果证实，（我们）对中国电信业本身、对在美国本土有商业活动的（中国）电信公司的历史背景和运营方式、以及那些与中国政府当局有着潜在关联的公司的了解方面，存在着严重的信息缺乏和不对称。更为重要的是，那次初步的调查评估结果使得我们加深了对与中国政府和军队有着潜在关联的中国电信公司对美国国家安全带来威胁的担忧。特别是，从某些程度上而言，这些公司受着中国政府的影响或者在为中国情报机构提供电信网络的数据存取，（因此，我们有理由相信），一个大家都已经知道的从事着许多网络间谍活动的民族主义国家，在上述情况下，对（美国）经济和外事间谍活动的机会是的确存在的。

正如许多其他国家通过他们的行动表达出的，本委员会相信电信行业在国家的安全问题上扮演着关键角色，因此该行业常常是外国情报工作的目标。委员会的正式调查聚焦在中国最大的两家电信设备生产商华为与中兴身上。这两家公司都在试图将他们的设备销售给美国的电信基础设施。由于他们希望在美国拓展他们的业务，本委员会的主要目标是更好地了解这两个公司对美国国家安全造成危险的程度。为了评估这种威胁，调查分为两个不同而又相关的部分：（1）通过公开信息来源来综合评估该两家公司的历史、经营、财务信息、以及与中国政府和中国共产党存在的潜在联系。（2）通过对密级信息的评估，其中包括对美国情报部门的项目和工作的评估，以查明情报部门是否在对供应链的危险评估工作中采取了正确的优先顺序划分和资源配置[3]。

尽管经历了许多小时的面谈，很多次的要求提供相关文件资料，对公开信息的综合汇聚，以及

对两个公司证人的公开听证，委员会仍然对这两家公司的合作以及坦率程度感到不满意。两家公司均没有情愿的提供充足的证据来化解委员会的对美国国家安全的顾虑。没有一个公司乐意提供他们与中国当局之间的正式关系或在监管上互动的详细信息。两家公司没有提供各自公司内部中国共产党党组织在公司内部准确职能的具体信息。此外，两家公司也均没有提供他们在美国经营的具体信息。特别指出的是，华为公司未能提供公司的组织结构、历史、所有权、经营状况、财务安排、以及管理方面的详尽信息。更重要的是，两家公司均未能提供详尽的公司内部文件或其他证据来支持其之前向委员会调查组所提问题的有限答案。

在调查过程中，委员会从工业界专家，当前和过去华为员工了解到，华为公司可能正在违法美国法律。这些指控描述的是一个未能遵守美国法律或者国际商业行为准则的公司。委员会将会把这些指控提交给执法机构进行更深得审议，包括进一步的调查。

总而言之，调查委员会认为两家公司未能提供证据以使本次调查成为公正全面的调查。虽然这本身并不能证明他们有什么过错，但确实影响了调查委员会下面的结论。另外，本报告包含了一个机密附属部分，该部分的内容增加了委员会对该两公司对美国造成国家利益风险的担忧。本次调查的结论是，华为和中兴通讯公司提供通信设备给美国关键基础设施所带来的相关风险，可能会消弱或危害美国的核心国家安全利益。

基于本次调查，委员会提出下列建议：

建议一： 美国应当对中国电信公司对美国市场的持续渗透持有怀疑的态度。

* 美国情报界必须对此威胁保持关注与警惕。情报界应当积极接触私有企业和部门，尽量使之了解面临的威胁以保持安全无虞。
* 鉴于华为和中兴通讯公司对美国国家安全利益造成的威胁，美国外国投资委员会(CFIUS)必须阻止这两家公司介入的收购与并购行为。立法上，建议扩大美国外国投资委员会的职能，使之权限包括在国会相关委员会接手的购买协议审议过程中。

* 美国政府系统，特别是敏感系统，应当排除使用华为和中兴通讯公司的设备以及零部件。同样的，政府项目承包商，特别是为敏感项目工作的承包商，应当排除在系统中使用中兴或华为的设备。

建议二： 强烈建议美国私营部门实体，在与中兴或华为公司做设备或服务生意时，考虑所面临的长期安全风险。强烈建议美国网络供应商和系统开发商在其项目中使用非中兴与华为的其他供货商。基于我们掌握的密级和非密级的关于该两公司的信息，华为与中兴通讯公司由于受到其国家的影响，对美国国家乃至我们的系统构成安全威胁，因此不能予以信任。

建议三： 美国国会司法委员会和执法机构的相应仲裁委员会，应当对中国电信行业从事的不公正贸易行为进行调查，需要对中国国家给予相关关键公司所提供的金融支持予以特别关注。

建议四： 中国公司应当迅速改变为更加开放和透明，包括在西方国家证券交易所上市的公司必须符合全面的透明要求，由独立第三方评估人对其金融信息和网络安全流程提供更加一致的评估，达到符合美国法律规定的信息披露和生产许可标准，并遵守知识产权保护的法律和标准。特别需要指出的是，华为公司必须变得更加透明，并对其在美国所负有的法律义务要积极相应和反映迅速。

建议五： 美国国会司法委员会应当考虑进行立法，从而更好的处理与（极端）民族主义国家有紧密关系的通信公司带来的国家利益风险，否则无法对其从事关键设施建设予以完全信任。这项法律可以要求增强有关安全风险信息在私营实体之间的分享，以及加强美国外国投资委员会在并购协议审批过程中所起的作用。

调查报告

I. 电信设备供应链中存在的漏洞对美国国家安全利益带来的威胁已越来越重要，其原因包括：国家（越来越）依赖于互联的重要基础设施系统；这些重要系统面临的威胁的范围（在变大）；网络间谍活动的兴起; 所有客户更多的依赖于少数的几个设备供应商。

美国的重要基础设施，特别是电信网络，需要建立在可信和可靠的基础之上。电信网络系统对来自恶意的，持续的网络入侵和毁坏性行为是很脆弱的。因此，设备供应商和提供管理服务的供应商必须在任何时候都具备足够的信任程度。一个提供设备的公司，特别是任何能够接触到或者有这些电信网络详细结构规划信息的公司，必须要遵守美国的法律，法规和标准。如果一个公司不能被信任，美国和相关机构应该质问是否该公司可以在我们的重要基础设施的网络系统里运营。

网络（攻击）威胁带给美国国家安全和经济利益的风险是一个不可否认的重要事宜。首先，（我们）国家对电信基础设施的依赖不仅仅是大家可以使用计算机而已。事实上是（我们）多个重要的国家基础设施系统都需要通过电信网络来进行互联和信息传输交换。这些现代化的重要的基础设施包括电力系统，银行和金融系统，天然气，石油和水利系统， 铁路和航运通道等等。每一个这样的系统都是高度计算机控制化的。另外，这些系统之间的互相依赖性极大的增加了一个系统出故障会导致其他系统也出现故障或崩溃的风险[4]。因此，电信网络的崩溃会导致对现代美国人民的生活出现灾难般的影响，导致影响整个社会（日程生活所需）的短缺和中断。

第二，这种系统之间的互相依赖性带来的安全薄弱是很广泛的，从来自内部的威胁攻击[5]，网络间谍和来自有国家为幕后力量的攻击。事实上，关于电信系统供应链中的漏洞，越来越多的认同都汇聚在是（我们）选购了来自外国的电信设备并用在了美国国家安全的应用上。例如，联邦调查局（FBI）经过充足的评估调查认为，来自个体犯罪人员和幕后民族主义国家力量操控对基础设备供应链的威胁是居高不下的网络攻击的重要组成部分[6]。 同样，美国国家反情报执行机构的评估是“外国试图收集美国的技术和经济信息，将继续保持在一个较高的水平，并且将是一个持续增长的事情，并将一直威胁到美国的经济安全。[7]”

第三，美国政府必须要特别关注那些最有可能针对美国开展高级间谍活动的国家制造的通信设备，例如，中国。最近的许多网络攻击往往源于中国。虽然精确的定位分析是一个长期的挑战，但从攻击的数量，规模和复杂性来看，这种攻击通常意味着有一个国家力量在后面参与。美国中国事务委员会曾经在一份关于对中国进行网络战和计算机网络情报收集方面的能力的非机密文件中谈到， 来自中国的，通过恶意网络行为来收集敏感的（外国的）经济和国家安全的信息的动作往往很难被其锁定的目标所察觉[8]。

最后，这个问题变得复杂的是，中国的电信公司，如华为，中兴通讯正在迅速成为占主导地位的，全球性的电信市场设备提供商。在其他的行业，这种趋势可能不是特别有关系。但是当这些公司试图控制敏感的设备和基础设施并可用于间谍和其他恶意目的的市场，这个市场缺乏多样性就成为美国和其他国家的担心了[9]。 值得注意的是，美国并不是唯一对这些问题担忧的国家。 澳大利亚在决定禁止

华为进入其国家宽带电信业务的时候其实是表达了同样的担忧[10]。英国方面试图通过建立评价制度限制华为获得对基础设施的接触的程度，并且在华为设备和软件在电信基础系统上线之前进行充分评估[11]。

A. 中国拥有相应的手段，机会和动机去利用电信公司以实现起恶意的目的。

中国对美国政府的情报收集工作，在“规模，强度和复杂性”[12]方面一直在持续加强。中国具备世界上最活跃的和长期经营的经济谍报工作人员[13]。 美国私人企业公司和网络安全专家的调查报告认为，一些规模迅猛的计算机网络入侵起源于中国，而且几乎可以肯定的认为这个网络攻击有中国政府参与或在幕后提供支持[14]。 此外，中国的情报机构，以及私营公司和其他实体，经常招募那些能够直接访问（美国）企业网络的人员来窃取商业秘密和其他敏感的私有数据[15]。

这些通过网络和人工参与的间谍活动往往具备非常复杂的技术能力，这些技术能力可以转化为在来自中国制造的电信设备部件中植入恶意的硬件或软件，并销售给美国。在电信设备整个产品的过程中，更改电信设备部件和系统的机会点是到处都存在的，垂直领域的产业巨头华为和中兴通讯为中国的情报机构提供了许多这样的机会，可以使得他们在关键的电信网络的器件和系统中植入恶意的硬件或软件[16]。为了这些恶意攻击的目的，中国（当局）可能会寻求和华为或中兴等公司的领导层面的合作。即使公司的领导层拒绝这样的要求，中国情报部门只需要在这些公司招聘相应的管理人员或者蓝领的技术人员，（就可以达到目的）。此外，从中国法律来看，中兴通讯和华为有义务和中国政府无条件的合作，（政府）可以使用他们的系统，或者在国家安全的幌子下怀着恶意的目的访问这些系统的数据。[17]

中国，这样一个复杂的民族主义的国家，有着损害干扰全球电信供应链的动机，其中美国是（他们）一个非常重要的高优先级的目标。具备拒绝服务或破坏整体系统的能力可以使得一个外国国家可以给另外一个国家所依赖的关键基础设施设备施加压力或者完全控制。通过从政府和企业恶意修改或者窃取信息的能力，中国可以获得昂贵和需要花费大量时间的研发成果。这些成果可以促进和加速中国在世界上的经济地位。能够访问美国电信基础设施，可以使得中国对美国政府和私营部门从事无法被检测到的间谍活动[18]。 充分认识到美国军方的先进技术优势的中国军事和情报机构，正积极寻找将来如果与美国发生冲突的时候能被使用的非对称优势[19]。在为美国客户生产的，来自中国制造的电信设备器件和系统里植入恶意的硬件或软件可以让北京在危机或战争的时候关闭或者削弱（我们的）国家安全系统。在关键的基础设施环节中恶意植入的东西，例如，在电网或金融网络里，也将是中国弹药库里的一个巨大的武器。

恶意植入的硬件和软件也是一个可被用在侵入美国国家安全系统的强大间谍工具。也包括那些封闭的美国公司内部网络。这些内网中通常含有敏感的商业秘密，先进的研发数据， 谈判或诉讼立法条款。这些信息的获得可以使得中国在和美国打交道的时候，获得不公平的外交或商业优势。

除了硬件和软件相关的供应链的风险，管理服务软件也构成了威胁。管理服务，通常是销售合同中系统维护的一部分，允许远程网络访问，做每天软件的更新和打补丁。不幸的是，这样的合同也可以让管理服务承包商在合法的幌子下，使用被授权的访问做恶意活动。这样的系统存取访问也提供了许多

机会给更多密谋好的经济或有国家背景的间谍活动。 而 华为这样的电信公司目前正在寻求扩大其服务业务的部分[20]。

美国政府数年前已经认识到这些电信供应链的风险问题 。事实上，在白宫的2009年综合国家网络安全倡议（CNCI）中，供应链风险管理（SCRM）就被确定为国家关注的12个关键基础设施保护的优先事项之一。同样，行政部门一直持续在按照2012年1月发布的整体供应链安全国家战略下的方针指导下审查供应链的风险问题。在2012年1月份的报告中阐述的供应链风险管理的一个重要组成部分就是“正确理解和识别那些来自有害的设备物资，来自有意的攻击，事故和自然灾害带来的系统崩溃等供应链的脆弱性。”[21]

B. (目前所）建议的“缓解措施”不能完全解决提供设备和服务给美国关键基础设施的中国电信公司所带来的（国家安全）威胁。

许多国家对来自不可信任的电信公司所带来的潜在威胁所困惑。为了解决这些问题，英国政府采取了一些初步措施（作为其总体缓解战略的一部分）并和华为签署了一项协议，与华为建立一个独立管理的网络安全评估中心（CSEC）。 CSEC，（作为一个第三方机构），对要进入到英国电信系统的华为的软件和设备进行独立的审查，并将相应的结果提供给英国相关运营商和政府。英国政府的目标是试图减轻部署在英国关键的电信基础设施上的华为的产品所带来的对英国整体网络系统的可靠性所带来的威胁。

为了其产品进入美国市场，华为和中兴通讯提出了类似的计划。这个计划中没有美国政府的参与，而是由电子冲突协会或其他私营部门来管理[22]。（他们试图通过）这些合作关系来解决对这两家公司可能会允许中国政府植入一些能够帮助（中国政府）间谍活动或者网络战的功能到他们的产品中所引起的担忧。 遗憾的是，因为美国电信市场的广度和巨大，我们担心，华为和中兴的这个方案不能完全解决（我们对）美国安全隐患的担忧。

设备产品化后的评估过程通常是通过一个标准的方法来确定一个复杂软件密集型系统的安全属性。信息技术安全评估和各种私人认证服务等流程通常被评估者用来针对一系列标准来衡量一个产品，并为其分配一个安全等级。该评级是为了帮助客户了解其将使用的设备或者软件包的安全功能的信心度。（在评估流程里），厂商对其系统实现和研发的流程都需要文档化，并通常用作安全等级评估中的重要依据。此外，这样的流程并不一定能够发现恶意代码，而是鼓励在有安全功能的产品中必须具备一个基本的安全框架。

由于一系列的技术和经济原因，华为和中兴提出的评估方案不太有用，不是（我们）所期望的。事实上，（他们的）评估方案可能由于评估不完全，有漏洞或者错误的评估，而导致产品被赋予错误的安全等级。由于一个局外的专家可能以某种方式“赞”一个产品，所以一个细心的客户应该选择放弃这样的含有威胁的和不客观的风险评估，同时省下这样的评估所需要的花费。

通过标准化的第三方安全性评估不能解决的一个关键问题是产品和部署的多样性。取决于如何以及在哪里配置，安装和维护，设备或系统的行为变化很大。出于时间和成本方面的原因，（第三方的）评估通常会局限在针对一个产品型号配置在一个特定的，往往是不是真正现场实用的，很局限的方式。

现在科技发展的步伐非常快，速度远远超过任何第三方的综合评估过程所能跟踪。第三方测试评估中使用的小范围的配置规范，无疑的让人确信一个被评估过的设备在部署的时候的运行模式是和在被评估的时候是不一样的。如果一个设备在现场部署时和测试的时候规格是不一样的，那么对一个复杂的设备的安全性评价是没有意义的。

在现场部署之前的对产品的评估，只是针对了网络生命周期中的产品部分。另外，要重要的认识到，网络运营商如何控制设备的补丁管理，故障排除和维护，升级，管理服务的方面，以及如何选择提供这些服务的厂商，都会影响到电信网络的目前的安全程度。

由于设备厂商资助自己产品的安全评估产生了商业利益冲突，导致（美国政府）对评估结果的独立性和严谨持有怀疑态度。设备制造商会自然的去追求自己商业利益的最大化，其利益是和客户的利益不一致的。在通用标准认证方面，（我们）已经发现存在着一些不同的但相关的（为了利益）挑战底线的行为[23]。厂商提供金钱资助给安全评估方。 通用标准系统认证的设计充分了解这种危险然后规定了评估者必须拥有政府资格证书。但这种预防措施看起来基本上是装门面的，没有意义的。因为（目前为止），尽管（我们发现）认证评估的效果很差，也没有发现任何认证被取消 。基于同样的考虑和担心利益冲突，华为设备在英国的评估机构必须通过英国政府的审查，获得政府的安全等级许可。这个流程获得了英国各个运营商的支持。 但是，尚不清楚的是，英国这样的方式能否会迅速的被借鉴到美国市场，也不清楚这种运作方式是否能真正的成功地克服人的私欲从而导致真正的独立评估调查。

在一个复杂的产品中发现和消除每一个重大漏洞的任务是巨大的。当一个产品漏洞是一个内部的人故意放入的时候，查找任务变得几乎不可能[24]。虽然许多技术文章里谈到如何在硬件和软件系统中自动查找潜在的漏洞，但是没有一个技术声称能找到一个已存在的系统中的所有的漏洞。能够证明一个系统实现符合一个形式设计规范的技术确实存在[25]。但是这样的形式方法技术必须贯穿整个系统的设计和实现的过程中才能起到作用，而不能用在一个已经完成的规模巨大或者相当复杂的系统中。即使能够用在系统的研发过程中，这种形式方法也还是不能还好的扩展到完全的商业电信系统中。（所以，）通过华为或中兴提出的系统安全评估合作，即使不说其评估的完全性和动机，（在技术上，）都无法确定规模和复杂性都很巨大的核心网络基础设施设备中的所以相关缺陷。如果在已经被广泛应用的产品中和已经被潜在对手都了解的评估流程还存在重大的漏洞 ，这种评估过程的作用就微乎其微了。

可能看起来对一个将被部署在关键基础设施的的可疑设备做安全评估似乎是对其可能带来的安全问题是一个好的解决方法。但遗憾的是，由于电信网络系统的复杂性，目前的安全性评价技术的局限性和设备供应商提供经济资助的认证过程提供的只是一种安全感，而不是实际的安全性。高度系统安全的保障只能通过完整的设计和工程流程 ，考虑完整的系统的系统设计方法，要跨越完整的产品生命周期，从设计研发到产品做旧下架。这样的设计流程也包括考虑系统分离的技术模块，模块之间的交互，人在使用设备中的环境因素和来自各种对手的威胁。 这样的一个评估处理过程才是令人信服的，具有多样证据的。这才是可以使得我们信任的安全评估[26]。

II. 调查

A. 调查的范围

众议院特别情报委员会是负责美国的各项情报工作的部门，监督情报事务的各项活动并确保其合法，有效和是否获得了适当的资源，以达到保护美国国家安全利益的目的。具体来说，该委员会负责不间断的审查和学习研究情报工作各部门单位，各种项目和活动，并且非常严格的审查和研究的情报界的来源和方法[27]。伴随着这个责任的是学习和了解美国所面临的来自国外的威胁，其中包括那些直接针对我们国家关键基础设施的威胁。同样，委员会必须评估来自外国情报活动的威胁，并确保美国的反间谍机构能聚焦并得到相应的资源，从而打败那些入侵活动[28]。

情报委员会对于这次调查的目标是调查中国最好的两家通信企业给美国带来的潜在的安全风险，并检讨我们的政府是否已正确定位，理解和应对这一威胁。另外一个目的是要搞清楚和决定，在一个公开的形式下，需要提供什么样的信息来回答这两家公司在美国的电信市场里是否会构成国家安全风险。这种风险是可能带来美国关键设施的失控的。

美国的电信业显然越来越依赖于全球供应链提高设备和服务。这种依赖性存在着明显的风险，一些个人或团体 – 包括那些由外国政府支持 的- 能够和将会利用和破坏网络的可靠性。如果我们要保护网络的安全性和功能正常，如果要保护国家安全和防止针对这些电信网络的经济威胁，我们需要更好地理解供应链所面临的风险是至关重要的。（基于这个目的），这次调查的范围覆盖了使用风险控制的方法来管理整体供应链体系的基本需求。

最近的研究强调指出，中国发起的网络攻击比任何其他国家都更多。在一个针对网络间谍方面的公开报告中（美国）国家反情报机构的高层人士曾经解释过，“中国拥有世界上最活跃的和持久的经济间谍活动的人员。”[29]。因此，这就是为什么情报委员会聚焦在对最有可能和中国（政府）有内部关联的（例如，华为和中兴）和那些寻求扩大在美国市场的中国公司。华为和中兴都是中国本土企业，在渊源上都和中国政府有关系。华为和中兴在美国都已经成立子公司，并都正在寻求扩大其在美国市场的份额。从目前来看，华为受到分析师和媒体的关注最大。由于这两家公司的性质相似，例如，和中国政府的潜在关联，来自中国政府的支持和都在推动其在美国扩大市场，委员会决定对华为和中兴一起做相应的调查。

华为和中兴通讯都坚称委员会不应只注重他们这两家公司，而不调查位于中国的生产和制造排除设备和部件的其他公司。委员会（确实）意识到，许多非中国企业，包括美国的科技公司，在中国生产制造他们的产品。但是，需要注意的是，产品在哪里生产对风险评估重要但不仅仅。一个公司的所有权，历史背景和正在销售的产品也非常重要。确实，华为和中兴不是唯一两个能对美国产生国家安全风险的公司，但华为和中兴是两个最大的由中国人创办的，中国人拥有的电信设备公司。而且并在积极寻求在美国网络设备市场的销售。因此，为了评估要（通

讯设备）供应链的风险，委员会决定先把重点放在我们能看得见的漏洞上，并希望这次调查的结果对将来如何审查其他来自中国或者别的国家的公司对美国电信设备供应量的风险评估方面提供信息和依据。

B. 调查过程

委员会的调查过程包括对相应公司和政府官员的大量交谈，调阅许多相关文件，和来自华为和中兴的高级官员的公开听证会。委员会的工作人员审阅了相关公司的资料，会见了华为和中兴的官员并进行了长时间和深入的面谈。调查委员会工作人员还参观了公司的设施和工厂。

具体的细节是，2012年2月23日，委员会的工作人员在华为公司总部深圳，会见并采访了华为的高管。代表团参观了华为公司的总部，审查了公司的产品线，并参观了一个华为的大的设备生产工厂。参与讨论的华为官员为华为公司常务副董事长胡厚崑、财务管理办公室副总裁白熠、主管美国的华为公司高级副总裁陈巍、董事会秘书江西生、全球安全总监约翰·萨福克（John Suffolk0、出口管理部郝艺等。

在四月十二日，委员会的工作人员在深圳中兴的总部拜访了其高管。除了会议之外，代表团也简单的参观了中兴的总部大楼和其设备生产工厂。参与会谈的中兴高管包括中兴的朱进云（美国与北美国市场高级副总裁），范庆丰（执行副总裁和全球营销和销售副总裁），郭家俊（法务总监），独立董事石义德（Timothy Steinert），马学英（法务总监），曹伟（信息发布办公室安全与投资部），钱宇（信息发布办公室安全与投资部）和John Merrigan（DLA Piper律师）等。

2012年5月，情报委员会高级成员Ruppersberger，和委员会成员众议员Nunes，Bachmann，Schiff去香港会见了华为和中兴的高级官员。在这次会见中，调查委员会成员会见了华为的创办人任正非。

在这次会议后，调查委员会通过致函华为和中兴要求公司澄清一些书面问题和要求调阅一些文件，以补缺委员会对华为和中兴了解的信息不完整，公司一些前后不一致或不完整的答案，和需要一些公司确认的关于公司历史和现状的书面证据。遗憾的是，这两家公司都没有完全或充分响应委员会的文件请求。事实上，华为和中兴都没有提供委员会致函所要调阅的内部文件[30]。为了回答剩余的问题，委员会要求每家公司来众议院出席公开听证会。

2012年9月13日，情报委员会举行了一次公开听证，华为和中兴的代表都有出席。其中包括华为公司高级副总裁和华为的美国代表丁耘和来自中兴的负责北美和欧洲的高级副总裁朱进云。这次听证会是很公平透明的。每个证人有20分钟的致词，然后在回答问题和听证的过程中，每位证人都有一个翻译的帮助以确保他们能最大程度上的完整的了解和真实的回答问题[31]。

(我们）再次发现，（来自华为和中兴公司的）证人回答问题往往是模糊和不完整的。例如，他们声称不理解或不知道一些基本术语，无法回答公司内部的中国共产党委员会的组成问题，拒绝直接回答公司在美国的运作问题，试图避免回答他们过去在知识产权保护上的问题，并声称不理解或不了解中国政府可以强迫他们允许政府机构接触和检查他们的（电信）设备的法律，公司在听证会之后对委员会提出的问题记录的回答是同样的回避。

C. 调查面临的挑战

这份非机密报告包括了委员会在试图了解这些公司的性质，中国政府和中国共产党在公司内部的角色，和他们目前业务在美国运营时所获得的非保密信息。在这个过程中，委员会遇到了许多挑战，其中一些挑战对于许多试图理解中国政府和企业的关系，理解中国对我们的基础设施构成的威胁之间的关系时，是一模一样的。这些挑战包括：在中国，企业和官僚结构缺乏透明度从而导致缺乏信任；一般私营部门不愿意提高私有的或保密信息;如果私营部门公司或个人谈论他们的忧虑对被政府报复的担忧；和网络攻击的不确定的属性。

属于保密部分的附件提供了更多的信息，这些信息加重了委员会对国家安全威胁的担心。但为了避免危及美国的国家安全，这些密级的信息不会公开。但是，不保密的报告部分已经很明显的显示了华为和中兴都未能缓和委员会对他们持续的扩大在美国市场扩展而带来的重大安全问题的担忧。事实上，由于他们屡次未能彻底和明确的回答关键问题也没有对其答复提供可靠的内部证据，委员会对华为和中兴公司在美国其运营带来的国家安全担忧没有得到任何减轻。事实上，由于他们的阻挠行为，委员会认为，对华为和中兴带来的美国国家安全问题的考量是当务之急的。

除了委员会与公司的讨论，委员会的调查人员还采访了工业界的行业专家和两个公司的前任和现任员工。美国各地的公司都经历过当使用华为或中兴通讯的设备时发生一些奇怪的或者报警事件。这些（使用华为和中兴公司设备的）公司的官员总是担心公开承认这些事故将会有损于他们的内部调查和事故定位，损害他们防卫他们目前系统的努力，当然，也危及他们的工作。

类似的，华为或中兴前任或现任员工也都表述了公司设备存在漏洞，和有来自华为官员的不道德或非法行为。这些来自前任或者现任员工的言词由于担心受到公司的惩罚或报复而不敢公开[32]。

此外，由于定位在美国境内的一个网络攻击是来自个人还是一个实体本身是一个非常有难度的技术，这对调查人员来说很难确定一个攻击是或者与中国的工业界，政府或者还是中国的黑客

社区自己的行为[33]。

III. 调查发现总结

中国通信企业为中国政府干扰美国电信供应链提供了一个机会。虽然意识到了这个问题，但认识和理解中国国家对经济实体的控制和影响的程度和手段依然是(很）困难的。就像中国问题专家解释的那样，国家对那些据称是私营企业的控制和影响是既不明确也不对外泄露[34]。中国问题专家认为，中国政府和中国共产党可以对公司的董事会和私营机构的管理层施加影响，这种影响可以是通过人事变更，或者一些更微妙的手段[35]。就像中兴提交委员会的材料中写道："政府可能影响的程度确实在各个方面都存在。"[36]

委员会因此把重点放在审查华为公司和中兴通讯关余中国国家的关系，包括来自政府和国有银行的支持，和中国共产党的关系，和他们为中国军事和情报部门所做的工作。委员会还审查了华为和中兴是否遵守美国的法律，如保护知识产权，以确定华为和中兴是否是可以信任的良好企业。委员会并没有试图审查华为和中兴产品或部件的所有的技术漏洞。当然，委员会认真的对待了之前和调查过程中该两家公司最近被指征的后门程序，或其他一些他们产品中的意想不到的东西。但是，由于委员会的专业知识的局限性，委员会没有对设备的特点部分做全面审查。

调查试图回答关于华为和中兴公司的几个关键问题，其中包括：

公司的历史和管理结构，包括最开始与中国政府，军队，共产党是的关系是什么？

中国政府或中国共产党是如何和在何种程度上对华为和中兴的决定，运营和战略施加控制或影响的？
华为和中兴是中国的国有央企，或者是中国政府提供了他们一些（相对于其他企业，）不公平的，特别的（竞争）优势或财政资助？

华为和中兴每家公司在美国市场上的定位是什么，在深圳的母公司对其在美国的业务运营的影响有多大？

华为和中兴公司是否遵守法律，包括保护知识产权和国际制裁条约（例如，关于伊朗）？

委员会发现，华为和中兴公司对上述咨询的反应不足和回答的不明确。此外，尽管一再要求，公司一直提供非常少的内部文件来支持他们自己的说法。另外，因为华为和中兴都没有遵循委员会提供的标准的文档，他们所提供的这些很少的文件基本上无法做验证检查。此外，由于中

国政府明显在控制这些相应的信息，导致委员会对华为和中兴的彻底调查充满了障碍。其中一家公司口头和书面形式清楚的告诉我们，如果没有中国政府的批准，这些相关的文件是无法调阅给调查委员会的[37]。 中国企业认为其内部的文件或信息仍然是“国家机密”的这个现实只能加剧我们对中国政府控制这些公司和他们的业务的担忧。

委员会对华为和中兴通讯充分既不充分回答问题，也不选择提供支持他们说法的文件感到失望，特别要指出的是，是华为主动要求彻底和完整的这次调查的。委员会无法信赖华为和中兴公司负责人的发言所声明的，他们在美国关键基础设施的设备不会造成（美国国家安全的）威胁，也无法信任他们不会屈从于中国政府的压力作出不利于美国利益的事情。

下面是委员会根据了解到的信息作出的一些总结，并对后续的调查作出相关建议。

A. 委员会调查发现，华为没有完全配合这次调查，并不愿多讲公司与中国政府和中国共产党的关系。但是从可信的证据表明（我们认为）华为未能遵守美国相关法律。

在整个调查中，华为官员试图将华为公司描绘为一个透明开放的公司。但是，华为一直拒绝以书面形式提供调查委员会质询问题的详细答案，也没有提供相应的内部文件来支持他们调查核心问题中他们的解释。特别的是，华为不愿意完整解释华为公司及其附属子公司的历史，结构和管理体制。没有满足调查委员会调查的要求。委员会几乎没有得到关于中国共产党党委在华为内部所起的作用的任何信息，也不知道任何华为是如何与中国政府通过正式渠道交互的详细信息。华为拒绝提供其在北美的业务运营信息细节，也没有透露与中国军方或情报部门如何合作的细节。我们因此对华为公司决策过程的问题得不到一个清楚得答案。华为公司对于调查委员会的书面文件的请求也没有反馈任何内部文件。这都妨碍了委员会对公司反馈的答案或者一些声明的评估。

除了与华为（总部）官员进行讨论，调查委员会也采访了几个现任和前任华为美国分部的员工。这些员工声称，华为美国分部几乎完全在华为总公司的控制之下。这些说法削弱了华为所声称的其在美国的运营基本上是独立于其（在中国的）母公司的说法。这些现任或者曾经任职于华为美国的员工，还有曾经与华为有生意业务往来的人提供的证词和透露的证据，揭示了华为几个非常严重的违法违规行为。这些都需要进一步的调查。调查委员会将把这些事项转移给相关行政部门。

这些指控并不是我们开始调查时的焦点和突击部分，是在调查过程中发现的。委员会相信这些指控揭示华为公司一些干部潜在的不道德和非法的商业行为模式。

华为员工对自己雇主公司的指控使我们对华为是否在美国按照美国的法律要求和国际商业行为规范的来运行产生了严重的怀疑。

(一）华为没有提供在其公司结构和决策过程的清晰和完整的信息，（其原因）很可能仍然依赖于中国政府的支持。

华为宣传自己是“全球领先的信息和通信技术”解决方案供应商，“致力于提供可靠，安全的网络销”[38]。但在整个调查过程中，华为始终否认与中国政府有任何联系，并坚持认为华为是一个私有的，员工持股的公司[39]。然后许多业界分析家不这样认为。例如，许多人认为华为的创始人任正非，曾经是中国人民解放军信息工程学院的一个部门负责人。信息工程大学同中国军方负责情报的总参三部关系密切，所以分析家认为任正非同中国军方还保持着某种程度的联系[40]。此外，许多分析师认为中国政府和军方把华为当作一个具有国家战略意义的企业来对待，并为华为提供了政府干预下的扰乱市场的金融支持[41]。

在试图理解中国政府对中国电信公司的影响或控制的过程中，委员会着重于华为的企业结构和决策过程。更多关于华为企业结构的资料有助于回答那些业界质询的挥之不去的问题。这些问题都是由于华为一直缺乏运作透明性而造成的[42]。多年来，业界分析家一直挣扎着试图了解华为的员工所有权模式是如何能够落地实践的，了解这种员工所有权模式是如何转化为企业领导和决策过程的[43]。华为一再声称公司是一家私营企业，是有员工拥有和控股的公司，不会受到中国政府和中国共产党的影响[44]。华为的高级管理人员还声称华为这种独特的员工持股和报酬制度是华为公司的崛起并取得成功的根基。

(我们掌握的）信息与华为描述的其公司结构不吻合。许多分析师认为华为实际上并不是所谓员工控股，而是由其管理阶层中的一个精英团队所控制[45]。因此调查委员会向华为公司要求提供更多的公司所有权的结构信息。 例如，委员会要求华为列出其前十大股东的细节。华为拒绝了这个要求[46]。在2012年9月13日在听证会上，华为公司承认，其股东协议赋予该公司的创始人任正非拥有对公司事务的一票否决权[47]。其他的一些公开材料也证明华为6万持有股份的员工在管理着整个公司的说法是不精确的。

例如，在2011年华为的年度报告中，任正非强调，华为的董事的目标不是其股份持有者的利益最大化（包括员工，政府和供应商）。而是以客户的利益为中心的企业核心价值观，并鼓励员工成为奋斗者，为公司作出持续的贡献[48]。

这样的陈述报告负面影响了华为一再声称的其员工控制和管理公司的的说法。因此，要探讨这些互相矛盾的说法，调查委员会非常重视华为的内部股份分配方案。值得注意的是，在调查过程中华为向委员会唯一提供的是一份据称是内部的，没有签名的股票协议文件。遗憾的是，因为该文件是没有签名和非官方的，委员会无法核实这些文件的合法性。

（另外，）华为官员解释说，中国法律禁止外国人在中国公司持有股份，除非通过一个特殊的

批准[49]。但是现任和之前华为（美国）的员工确认只有是中国公民的华为美国员工才能参加持股计划。非中国公民的华为员工无法持有华为公司的股份进一步削弱了华为宣称自己是一个员工控股的公司的说法。整个一批（美国）员工不仅仅是利益处于不利地位，也被自动排除参与到公司的（各种决策）流程中，没有任何机会。

华为一直坚称中国政府没有对其企业施加影响，公司是通过华为的员工持股计划（ESOP）为基础的员工拥有和管理的实体。（华为）官员解释说，持股计划是不是一个福利计划，相反，它是給高绩效员工购买选择权可以购买由每年分红的股份，从而分享公司的价值。由资格的员工可以以公司确定的价格下购买股票，并且只能他们离开公司，或者通过批准的时候出售其相应的股票[50]。

华为还让调查人员查看其员工选举股东代表和董事会的投票。这些似乎不是表面的纸上的欺骗，但（我们）无法进行验证，尤其是调查人员不允许从华为拿走相关文件去給第三方做验证。文件显示员工股东有选择股东代表的权利，但没有选择董事会的权利。相反的是，华为官员表示董事会被提名人选在先前的董事会投票之前就确定了。目前还不清楚华为最初的董事会是如何成立的，华为一直未能提供以前什么人在董事会的任何答案。

华为进一步解释说，中国第一个“公司法”是1994年正式制定的，该法律规范有限责任公司的的建立和运行机制[51]。在该法中，一个有限责任公司的股东人数最多为50人。因此，华为声称在1997年改变了其公司法律结构为有限责任公司，并开始实施其员工持股计划。华为称，1997年深圳市也出台了相关公司员工持股的政策。华为认为其股份结构的设计是符合中国的“公司法”，和深圳市的相关法律和政策的[52]。

华为的投资控股有限公司负责员工持股计划的实施。该机构是一个合法注册的协会。华为官员表示，“华为的成功可以直接归功于华为独特的薪酬结构。”[53]。华为称目前，该机构持有98.7%的员工股份，其中任正非持有1.3%。在2011年12月31日，华为的员工持股计划ESOP在大约有65,596的参与者，涵盖所有华为员工（现任和已经退休的），华为声称，其中没有第三方机构持股，其中包括没有政府机构持有任何公司的股份。

（尽管这样，）调查委员会的工作人员在与华为官员的会议之后还是存在疑问。最重要的是，委员会不是很清楚董事会的董事成员是如何选出的。这对我们而言是一个很重要的问题和充满了顾虑，因为这些董事会成员是华为公司的主要决策者，也是这些人和中国政府有着潜在的联系。。据华为官员透露，前任的董事会提名当前的董事会成员。但我们不清楚华为第一界董事会董事是如何构成的和第一届监事会是如何产生的[54]。

如上所述，华为向委员会提供了没有签名的，未经验证的如下文件，：（1）虚拟受限股条款条款（2）虚拟受限股承诺书（3）股票发行与确认书的通知（4）持股员工名单（5）员工的付

款和回购的记录，（6）员工股款及回购的收据（7）2010年华为员工持股代表选举程序，选票，结果，公告等的选举纪录 （8）2010年的ESOP代表大会的会议结果。

因为华为华为只提供了没有签名的草稿文件，调查委员会无法验证这些文件的合法性，下面是我们从这些文件中获得的一些关键信息摘要[55]：

（1）ESOP 职工虚拟受限股 – 总结
ESOP职工虚拟受限股第20条规定这些股票是发给是目前工作成绩比较好的员工。

每一年，公司会根据工作表现决定一个员工可以购买的股份数目。有资格的员工必须签署确认书和承诺书，并掏钱购买相应的股份。

员工的股票只能他（她）自己持有，不得转让或出售。当员工离开公司的时候，华为公司会回购这些股票，（除了退休条件的：在华为工作已经8年并且年龄已经45岁）。

内部股的股价是上一个年度股票的净资产值。当一个员工想购买更多的内部股份或公司回购股份的时候，是基于当前的股票价格。每年的股息分红是基于公司每年的业绩。

（2）虚拟受限股条款条款

a. (股票管理）委员会

委员会由51名常委和9名候补组成。每届任职5年。这些成员由内部股持有员工的活跃成员选出。

* 这些参与投票的人可是在深圳市华为投资控股有限公司，或任何其参股子公司和参与内部股票持股的受益人。

* 在委员会成员出现空缺的时候，候补依次填补空缺。候补委员可以参加所有的会议，但没有投票权。

* 委员会审查和批准职工虚拟受限股的发放申请，审查和批准股息分配方案，审查和批准报董事会的报告，选举和替换董事会成员，选举和替换监事会成员，评审和批准选举员工代表的流程。批准各种条案的修订。审批和批准使用的储备基金。审查和批准虚拟受限股的其他材料事宜。执行公司股东的责任和权益。负责增资扩股，利润分红，选择董事，董事会和监理会选举的各项事宜。管理委员会每年至少召开一次会议，由董事会召集，董事会主席或副主席主持。

b. 董事会

董事会负责公司日常业务的各项管理，并向管理委员会汇报。

董事会的主要职责是：准备虚拟受限股的发行配股方案。 准备股利分红方案，和对虚拟受限股详细规则，流程和实施方法的形成落实，批准和修改。对各种公司条例的修改。对使用储备基金规划的决定。对整个公司管理委员会决议的贯彻执行。 履行参股公司的具体权利和权力的行使（除了一些需要管理委员会的决议才能做主的事情）。其他一切董事会能做决定的事宜。

董事会成员由13名。有董事委员会选定。任期五年。

董事会每年至少举行一次，必须需要2/3的成员参加。会议决议应经全体董事至少1/2的过半批准。

董事会可设立一个虚拟受限股管理委员会，或者其他相关的机构，来负责贯彻落实董事会指派的工作，例如对虚拟受限股的评估，分配到回购，也包括资金帐户的管理和虚拟受限股相关联的储备基金等财务的管理。

c. 监事会

监事会是负责监督实施员工持股计划的机构，其主要职能和权力如下：

* 监督董事会决议的执行情况;
* 对公司需要处理的法律，法规和董事会制定的一些章程提出建议和提供咨询。
* 向管理委员会做工作汇报。
* 其他常规的职能和权力。

监事可以列席董事会会议，但无投票权。

监事会由5名监事组成。由管理委员会选举出来，任期五年，董事会成员不能担任公司监事。

每年至少召开一次会议，需要至少2/3成员出席，决议要求至少有2/3的全体监事批准。

d 决议的有效性

2018年12月31日之前，任正非有权否决关于员工虚拟股票和华为其他重大事宜的决定（董事会决议，委员会，以及公司的股东会议）。

2013年1月1日起，员工持股或虚拟股份的受益人，如果达到了所有内部股的15%（不含重组收购受益人所持股份和保留限制股），将有权否决关于虚拟限制股和华为的重大事项的决定（包括董事会决议，委员会和公司股东大会）。

只有当拥有否决权的人（任正非，或者超过15%的内部股持有者）不行使否决权的情况下，华为相应的各种决议才生效。

（3）员工受限内部股份的发放

受限内部股发行给有优异工作表现的公司关键员工。

在内部股发行的评估章程下，一个员工的过去一年工作的综合评价是股份管理委员的重要依据来每年决定给一个员工是否给予内部股份和多少。退休或收购重组的受益者不得购买新股。

（4）受益人的保密和非竞争责任

除非公司的书面或者相关同意协商，当前员工受益人（持有者）或重组收购股票受益人不能以任何方式直接或间接拥有第二份工作。

（二）华为未能解释其与中国政府的关系，其声称与中国政府的支持没有关联是不可靠的。

现代中国经济的本质对了解化为与中国当局的关系是有内在联系的。中国政府通常会对有战略意义的公司和相关产业提供财政支持。事实上，研究中国政治经济方面的分析师认为：

华为公司的产业业务是中国政府（北京）明确提到的七大“战略产业”之一。战略领域是被视为对国际和安全利益据报道核心价值的产业。在这些领域，中国共产党通过市场保护，低息贷款，税收和补贴等方案确保“央企”的主导地位，当涉及海外市场的时候还提供相应的外交支持。事实上，如果没有当局的背书，中国的战略领域是不可能发展起来的[56]。

类似的，美中事务委员会曾经解释，对于中国公司，“中国政府的作用是一种很隐晦的，不直接也不披露。”尽管已经有了一些改革，“中国经济体许多部分的所有权或控制权依然在中国政府的手里。[57]”美中事务委员认为华为是一种得到了中国政府广泛指出的一种中国企业 - 处在一个相对较新的市场从而得到政府许多政策的扶持，在国外类似企业竞争的时候，由政府出面施加壁垒。[58]

因此，委员会询问了中国政府和华为之间的准确关系。委员会与华为高管会议期间，和在

2012年9月13日的公开聆讯中，华为官员坚持否认除了正常的政策法规之外，和中国政府有任何深度关连[59]。华为在其书面答复委员会的具体解释中写道，“华为保持着与中国政府监管机构正常（一般）的商业交流与互动，包括工信部和商务部。[60]” 华为公司声称，华为“不与不相关的政府机构包括国防部，国家安全部，中央军事委员会有联系。”[61] 但是华为没有向该委员会提高可以评估确认这些声称的信息，华为拒绝回答委员会具体询问有关该公司如何与这些 政府机构的互动确切方式。

委员会并没有期望华为证明和中国政府“没有任何关系”。相反，在中国问题专家们也不太了解中国国家资本主义制度的原因下，委员会试图更深入地了解华为与中国政府的实际关系。委员会要求华为提供详细资料和证据解释证明其声明中的与中国政府的保持着正常的政策监管互动的性质。任何在美国有运营的公司都可以很容易地描述和出示证据显示其和联邦政府部门的互动，包括相关对口接触的政府官员。

在华为书面回答委员会的材料中，华为简单地声称其“与相关（中国）政府监管机构维持着正常的，一般的商业沟通和互动，包括工信部和商务部。[62]” 华为没有提供进一步的资料解释说明华为是如何被中国政府监管，控制，或以其他方式管理的。这些材料都不利于华为声称的其没有受中国政府的不恰当的干预或影响。华为似乎很不愿意提供更多的细节来解释其和中国政府的关联，从而减轻（我们）对华为对美国构成安全隐患的顾虑。

同样，华为官员没有提供华为之前的董事会成员的背景的详细资料。相反，委员会只收到了先前已经披露的当前董事会成员和监事会成员的个人资料[63]。（委员会认为，）华为前董事会成员可能和共产党，中国军队和政府有很深的联系。因为当前董事会成员是由之前董事会负责提名的，所以上一届董事会成员的信息对了解了解华为公司的历史是很重要的。由于之前的董事会成员的个人资料可能会显示公司于中国政府的军事或情报部门的关联，华为一直不提供相关信息让委员会感到很警觉。

（三）华为承认，在公司内部存在着一个中国共产党党委，但未能解释党委的职能和党委成员细节。

华为公司与中国共产党的联系是调查委员会的一个重要的顾虑。因为这表示中国政府有机会在一个寻求进入美国关键基础设施市场的中国公司的决策经营中发挥影响力。（我们的）这些顾虑建立在中国共产党在中国的机构和实体事务中无处不在的现象上。这种顾虑也建立在大家一致认为中国共产党对中国的经济事务起着主导和施加各种压力的作用[64]。

尽管（我们给了华为）许多机会来回答其和中国共产党的关系，华为表示华为公司和中国共产党没有内在联系。例如，在回答委员会关于共产党在公司的事务中扮演的角色的问题时，华为只是说，“在其商务活动中与中国共产党没有关系。”[65]

但是华为承认其内部存在着一个共产党党委。华为简单的解释为中国法律要求在所有的公司里都需要有党委机构。然而，这个委员会的存在具有特殊意义。华为在其答辩中解释中国所有的经济结构中内部都有一个党的机构[66]。但这不是一个正在为美国建设基础通讯设施的公司所能给出的令人接受的解释。事实上，中国的政治经济专家认为，（中国）共产党正是通过 这些（公司内部的）党委，对公司施加影响，压力和监察企业的各种活动。从本质上讲，这些党委会以一种很微妙的方式，扮演和提供着（公司内部的）权利和影响力，对中国的经济方向起着指导的作用[67]。因此，华为拒绝讨论或提供华为党委员会成员名单是很可疑的。华为也同样拒绝说明华为党委参与审查公司的何种业务决定，和拒绝透露个人是如何被挑选进入党委的。

同样，华为官方没有提供任正非在党委所扮演的角色或地位的信息。在他的官方简历介绍中，任正非承认，他是1982年的第12届中国共产党的全国代表大会的的代表。全国代表大会是一个十年一次的大会，选举未来中国国家领导人。党代表通常被认为是共产党员的积极分子[68]。任正非骄傲地承认他被选举为代表并参加了党代会，但他没有解释其作为党代表的职责。在参加了党代表大会不久，任正非成功地创办了华为公司，虽然他声称他没有得到政府和共产党的任何支持[69]。华为同样拒绝回答任先生是否是后续的全国代表大会的成员，和在共产党系统内部所起的作用[70]。

从现有获得的资料来看，华为可能有着不愿意透露的和中国高层的联系。 由于华为拒绝透露其公司内部党委的细节， 因此委员会对华为在任何其他可能与中国政府，军队，共产党是否有关联的问题的回答上的坦率程度抱有质疑。

（四）华为公司的历史表明其与中国军方存在着关系，但华为未能提供针对这些问题的详细的答案。

华为试图通过阐述华为创办人任正非的生平来解释公司的成立和发展。据华为官员透露，任先生曾经是中国军队的工兵部队的一个军人，参与建立辽阳化纤厂，并晋升为副主任，这是一个技术兵种，相当于一个副团级干部，但没有军衔[71]。 任先生1983年在工程兵解散后从部队退役后。之后任职于一家国有企业（SOE）。根据这个解释，任先生是“不满意”他在国有企业的低工资和职业发展道路，所以在1987年，他创立了华为公司。华为官员并没有解释他如何离开他国有企业的工作，还是他和政府有了协议。华为官员否认任先生是一位军队里的高级干部[72]。委员会要求华为出示任正非军事和专业背景的更多信息，遭到华为的拒绝。 华为拒绝描述任正非的完整军方背景。华为拒绝说明他在部队的时候谁是他的上司。 华为拒绝回答任正非为何被邀请出席第12届全国代表大会，他的职责是什么，以及他是否已被要求参加类似的党内事务。

华为同样否认了华为董事长孙亚芳女士曾经与国家安全部有来往的陈辞。丁先生说，据他所了

解的，一些中国刊物比如新京报对于孙女士的报道都是有误的[73]。丁先生没有回答这些刊登的信息来源是哪里，也没有回答是否孙女士在华为官网上的简历是错误的。他只是简单地再一次提供了孙女士在2011年华为年报上的简历[74]。

关于华为的创办人，华为引用了法律条款称新成立的公司必须有五位股东且有20000人民币的注册资本。在于委员会的会议中，华为官员称在1987年任正非通过自己的储蓄和其他五位个体投资者筹集了21000[75]。 据他们所了解的，这五个人没有一位是之前与任先生合作过的，其中只有一位有过政府背景。华为官员称，这五位投资人从没有在华为工作过，并且都在若干年后撤销了投资[76]。

调查委员会试图从华为最初的创办得到一些关于华为背景的答案，例如，任正非是如何认识其他的投资人的，他军方背景是否对华为的发展起到了重要的作用，他在共产党内的职务是否对他个人和华为公司的成功是一个重要的因素。

（五）华为没有提供关于中国政府1999年对于公司税务欺诈调查材料。委员会认为这加深了人们对华为不透明化的看法；华为很轻松的摆平了中国政府的此项调查损害了其声称的中国政府认为华为是一个不受欢迎的电信解决方案提供商的说法。

华为官员声称，在华为90年代从农村区域（的交换机市场）开始成长并取得了很大的发展后，中国政府对华为公司在1998-1999年度的税务进行了调查[77]。华为官员认为，那次调查是华为公司的竞争者在后面指使的。这些电信公司都是一些国有企业。华为的胡厚锟先生指出那次调查是华为公司的一个历史转折点。华为从此进军海外市场就是那次调查的结果[78]。华为这些官员试图通过这次调查来解释华为不是一个中国国家扶持的企业。[79]

既然那次中国政府的税务调查对华为后来的战略转变是如此的重要，委员会随后的问题和相关文件的请求就聚焦在关于事件的具体信息和记录上。委员会尤其试图得到中国政府对于华为的调查结论。当我们发现华为在深圳的一些官员对他们当时如何利用关系网来摆平政府的调查引以为豪的时候，这个调查结论对于调查委员会就显得特别重要。华为这些官员的能量让调查委员会觉得华为不是象他们所说的那样没有政治背景或者政府的影响。

尽管这个事情的来龙去脉是如此重要，华为没有针对调查委员会的问题提交书面材料[80]。华为也没有能够提供材料来证明针对华为的那次调查在法律层面已经完全结案，或者没有任何附加的条件[81]。

（六） 华为未能解释其与西方咨询公司的关系，公司的成功是得益于这些关系而不是中国政府的支持的声称缺乏信服力。

华为官员声称，公司成功的原因之一是其对西方咨询公司，如IBM、埃森哲、普华永道会计师事务所等提供的咨询服务的遵从和依赖 [82] 。华为试图说服委员会，其在最近的几年里奇迹般的增长得益于这些公司的建议，而不是中国政府的支持。 [83]

由于华为强调其对这些咨询公司给出的建议的重视，委员会试图寻求更多的信息和证据以表明过去的这些建议对公司有重要影响。委员会明确表示不会探究华为与咨询公司在商务合约方面的信息，而是会调查这些公司对华为的哪些信息进行了评审及为华为提供了何种建议。委员会承诺将对这些信息保密，以避免产生对泄露公司商务信息的担忧。

华为仅对这些公司提供的建议做出了一个比较模糊的回应。具体而言，尽管“自从1997年起，华为依靠西方管理咨询公司帮助其改善运营能力，建立流程，并根据客户需求的驱动开发了一个综合管理系统”，华为未能提供详细资料说明这些公司如何改革华为，还是这些咨询公司仅仅提供了几句提到标准商业行为的建议，包括从线索到回款的合同周期管理（LTC），集成产品开发（IPD），问题解决（ITR），以及综合金融服务（IFS）。华为“拒绝提供关于其和咨询公司关系更多的细节”，表达了对关于在这些建议中存在专(私有)有信息的担忧 [84] 。委员会解释说，其最关心的是那些华为对这些咨询公司的建议作出了什么反映的证据，特别是财务或其他证据，以用来证实华为的声明：这些改变提高了公司的效率、增长和市场成功 [85] 。华为其实可以在不透露公司机密的情况下回答这些问题 [86] . 委员会也表示愿意与各方签署保密协议，但这项提议被华为拒绝接受。 [87]

通过将其快速成功归因于由这些咨询公司提出的建议，华为认为这些咨询建议的细节与这次调查相关。那么对华为而言，对委员会隐瞒这些可以令其评估那些声明的信息就是不合情理的。如果华为拥有那些信息和文件，可以证明这些由咨询公司提供的协议对华为的成功具有关键作用，那么华为应当提供这样的信息88。委员会愿意并将继续愿意与各方讨论机密协议，以解决关于专有信息泄露的担忧。华为未能接受这一提议。华为的拒绝显示了华为在整个调查过程中缺乏合作。

（七）华为没有回答关键问题或提供证明文件以表明其在财务上独立于中国政府。

作为一家对中国具有战略重要意义的公司，华为的地位可以从其来自于中国政府和中国共产党的财政支持和接受的政策指导体现出来 [89] 。检视一家公司受国家的支持和引导的方法之一就是看该公司的资金来源。许多业内专家和电信公司都描述华为产品通过低于市场价格的方式销售 [90] 。因此，委员会试图寻求更多关于华为融资的信息，包括其客户的财务情况。这样的财务信息也能够有助于更多地了解一家在很大程度仍不透明的公司的财务结构。

在委员会的听证会上，丁先生表示他不理解或不知道“国家龙头企业”的称号. 这个称号经常在关于中国的经济文献中被用来描述受国家青睐的公司 [91] 。委员会认为丁先生说他不理解这个

称号是不可信的，华为自己在2011年11月向美国国会办公室提供了一个幻灯片，里面就多次使用了“国家龙头企业”的字眼 [92] 。在回答委员会提出的有关在那份文件中使用了该术语的问题时，华为并未否认其使用了该文档并提供了包含该术语的文档 [93] 。然而，华为声称那份包含在其他更多的文件里面的那个幻灯片是由第三方撰写的，因此不是华为的责任 [94] 。然而, 委员会认为，华为在与美国调查委员会的代表讨论时知道自己曾经使用该文档表明了足够的证据显示华为是了解这个术语的意义的。
丁先生一直坚持拒绝回答哪家公司被认为是中国电信业的“国家龙头”的问题被认为是（对调查的）蓄意阻挠。事实上，他在回答委员会这个问题时说“华为在此前没有关注过 ‘国家龙头企业’这个称号” 显然是不真实的，这与该公司之前在其幻灯片中使用了这个术语背道而驰 [95] 。此外，他的回答还表明，他并不想解释为何华为作为中国第一大电信服务提供商在中国不是一个具有战略重要意义的公司。而这是世界众所周知的。

华为官方也否认收到了来自中国政府的任何特殊的财务激励或资金支持 [96] 。华为声称，该公司只是和中国的银行的进行了正常的合作，但并没有去试图影响或协调中国发展银行和进出口银行这样的国有银行。在之前的陈述中，华为已表明，它只是作为国家金融信贷和客户之间“中介和桥梁” [97] 。然而华为拒绝提供关于这些信贷额度如何被使用的更多细节。华为也拒绝回答其与中国银行所建立的正式关系的具体情况，而只是选择回答了它与中国进出口银行只是保持着“正常商业联系”的问题 [98] 。

在2月份的会议期间提交给委员会的陈述中，华为提供了一系列谅解备忘录，关于其已为相关客户与中国银行签订了信贷额度 [99] 。华为承认它的客户有1000亿美元的可用信贷，但华为声称从2005年到2011年期间信贷金额只有58.67亿美元。此外，在书面答复中，华为声称 “这是给客户提供的融资机会，而不是华为的” [100] ，然而，在2012年2月23日的与委员会调查员的会面中，华为解释说中国的银行支持大额度的可用信贷的目标是让人觉得中国的市场是“吸引力的和印象深刻”, “华为不得不参与其中否则将不再能够”从中国的银行获得贷款101。在回应委员会重复的问题和对文件的要求时，华为未能就公司从这些融资安排所得到的利益提供进一步的书面解释，也没有提供内部文件或任何可审计的信息，来证实其对从中国的银行的贷款的范围和流程。

同样，华为也拒绝详细描述其与中国国有银行的关系。例如，在丁先生的备案声明中，他解释说华为从10家中国银行获得贷款，但丁先生拒绝回答这10家银行中有多少家是国有银行 [102] 。正如上一节所描述的那样，华为也拒绝提供额外的“咨询关系”的细节，因为它可能涉及已经签署了的含有“高度敏感的专有信息”的保密协议 [103] 。在回应委员会关于华为的成功及其是否归功于中国政府的支持的问题时，华为再次向委员会说明，它在全球的成功得益于华为与咨询公司的关系以及从这些公司得到的建议 [104] ，由于华为拒绝提供关于这些关系和所得到的咨询意见的细节信息，委员会无法评估它声称成功是源于这些关系。因此，委员会不完全相信这些咨询公司所起到的作用，并继续认为华为的成功可能在很大程度上是由于得到了

中国政府的支持。

总而言之，华为承认其客户获得了来自中国国有银行数十亿美元的支持，也承认多年来收到了中国银行的优惠贷款。华为拒绝对有关这些援助是如何被担保的问题提供直接答复，也没有提供内部文件或可审计的财务记录，以用来评估其声称的这些协议的条款符合标准程序和国际贸易协定。委员会也同样关注由公司领导层提供的声明，这些声明也都削弱了委员会对该公司所提供的财务信息的信心。例如，在2007年6月对华为英国员工发表的演讲中，任先生说，他赞赏子公司创建的财务报表，“不管数据是否准确”[105]。根据现有的资料，委员会认为华为从中国政府和中国的国有银行得到了大力支持，这至少在部分程度上帮助华为奠定了其在全球市场中的地位。

（八）华为美国分部未能提供足够的关于其在美国的运营、财务及管理方面的细节或支持文档; 这些都破坏了所谓的华为美国是一个完全独立于其在中国深圳母公司的子公司的声称。

为了理解华为的设备对美国当前脆弱的供应链带来多大的威胁，有必要了解华为的设备在多大程度上已经被放置在美国的基础设施中。因为美国的电信基础设施主要是由私营部门建造和拥有的，美国政府并不完全了解它包含了什么，因此尚未完全知情，并制定相关的政策来保护关键基础设施[106]。

委员会因此要求华为提供其在美国的产品和服务合同的信息。了解华为的设备在多大程度上已经存在于美国，对于评估目前给国家带来的风险是很必要的，同时也能核实华为提供的关于其在美国的规模和业务范围的声明。遗憾的是,华为未能提供其在美国商务交易的具体信息。华为的确向委员会提供了一份在美国的客户清单，包括： Cricket Communications、Clearwire、Cox TMI Wireless、Hibernia Atlantic、Level 3/BTW Equipment、Suddenlink; Comcast 和Bend Broadband等公司，但华为并未提供其运营规模和范围、向基础设施提供何种元件及在何地运营等信息[107]。

委员会所要求的关于华为在美国的合同信息对用来评估华为所声称的它们销售的产品和服务的价格遵守了所有法律和贸易义务也是非常有必要的[108]。到目前为止，华为未能提供任何信息，用来证实其宣称的华为产品的价格是根据市场来制定的。华为拒绝提供明确答复或文档支持其声称，迫使委员会认为华为的辩解是不可信的。委员会认为华为可能收到来自中国政府的大力支持，以使华为在美国至少有一些产品以低于成本的价格在市场销售。

同样，华为在美国的子公司在多大程度上独立于在中国深圳的母公司运营仍不清楚。这样的信息是重要的，因为在中国的母公司与中国政府的任何联系都可能影响美国分公司的运营和行为，委员会因此要求华为提供信息说明华为美国公司的决策在多大程度上受到母公司的控制、影响和审查。

华为解释说，第一个美国华为子公司成立于2005年，总部设在德克萨斯州普莱诺。华为表示其母公司不需要批准在美国的合同个案 [109] 。相反，它表示在中国的董事会并未对在美国的运营设置通用条款，并且如果子公司需要，父公司可以帮助它调动资源并制定战略。然后,委员会已从数位前华为美国员工那里得知他们不同意华为对其美国分公司运营模式的解释。来自美国各地的资料也提供了大量具体实例，表明在美国的商业决策需要通过中国母公司的审批。在一个案例中，一位具有第一手资料的知情者解释道， 没有中国的批准，美国的高级主管不能签署关于在美国的网络安全服务的合同。事实上，在一个实例中，先前由美国高级官员签订的合同后来被母公司拒绝 [110] 。在讨论华为美国来自中国母公司的政策时, 这些华为前员工提供了包括内部备忘录和电子邮件在内的文档证据。这些关于华为美国子公司的描述也与其他华为分公司和中国母公司之间关系的报告相一致 [111] 。

为解决这个矛盾，委员会试图从其给华为的书面问题质询中获得更多信息，以便理解华为深圳母公司通过何种精确机制来控制华为在美国市场进入和增长的策略。当华为官员声称,如果需要的话华为美国将从母公司得到一般性的方向指导和相应的“资源” [112] , 调查委员会对于北京对华为的支持可能影响美国市场的担忧被加重了。然而，在其书面回复中，华为未能回答委员会的细节问题，或提供更多关于华为美国子公司和其母公司之间协调层面的细节信息 [113] 。

由掌握一手资料的华为员工提供的信息和材料，再加上华为未能提供详细的内部信息，这些都削弱了华为声明的可信度。基于这些原因，委员会认为华为关于其美国子公司独立于华为深圳总部运营的声称是不可信的。

（九）有证据显示，华为对美国公司和实体的知识产权表现出一种漠视。

华为对知识产权的保护能力，是该公司是否遵守美国的法律能力的重要佐证。因此，委员会试图寻求更多关于华为在知识产权保护方面过去的记录。

委员会有理由相信，华为并未严格执行知识产权保护相关法律。调查人员从大量渠道得知，当涉及到保护其他实体的知识产权时，华为的态度一直是多变的 [114] 。特别地，一些前华为员工声称，华为有意使用其他公司拥有专利的材料是众所周知的。前任员工掌握的第一手资料表明，华为并未恰当地购买软件程序以供其员工使用 [115] 。同样，委员会从业界专家那里得知，华为曾有意使用和销售其他公司的专利产品 [116] 。 最后，委员会收到了一份华为公司提交给美国国会办公室的幻灯片，该文稿其实就未经允许使用了一家外部咨询公司的相关材料，这本身就违反了知识产权保护原则 [117] 。

华为官方一直否认曾侵犯其他公司的知识产权。即使在关于华为与思科的诉讼方面，华为已经

同意从市场上撤出某些产品，但华为仍声称，它并未侵犯思科的利益 [118] 。相反，华为认为，在那次对其设备的专家审查中没有发现任何侵犯思科的专利 [119] 。

华为的辩解是不可信的。首先，关于思科的诉讼，华为的声明与华为官员在诉讼期间的声明并不一致，当时华为表示将从市场上撤下侵权设备 [120] 。其次，当时和思科的庭外和解的协议中包含了要求华为“更新和更改所有被指控侵犯版权或知识产权的产品” [121] 。最后，在2012年9月13日的听证会期间，查尔斯•丁拒绝明确回答思科的代码是否曾被用在华为的设备上 [122] 。丁先生在听证会期间的蓄意阻挠，违背了华为关于自己并未侵犯思科专利的说法。

委员会发现，华为否认侵犯知识产权的说法是不可信的或者并没有可靠的证据支持相反的观点。由于华为未能出示任何内部文件或证据来支持其辩解的观点，委员会认为华为对其他实体的知识产权至少是表现出一种漠视的态度。

（十）华为未能提供关于其在伊朗业务的详细信息，尽管其否认与伊朗政府有商业往来，但未能提供证据证明其遵守所有的国际制裁或美国出口法律。

华为遵守国际制裁制度和美国出口管控法规的能力，是该公司独立于中国政府的影响或利益去遵守公司行为的国际标准和美国法律的一个重要指标。目前公开的报告质疑了该公司遵守这些法律的能力。
在对委员会问题的回复中，华为官员只提供了很模糊的陈述来表明他们会遵守所有相关的法律，特别地，华为声称该公司尽力遵守所有的法律法规，并在外部商业顾问的建议下转变其商业模式以便更透明地监管公司行为以确保符合国际制裁制度的要求。为了强调中国政权对华为商业决定没有影响力，华为指出，中国驻伊朗大使馆对华为决定限制公司在伊朗的业务发展感到十分惊讶。华为也声称它禁止其员工参与在伊朗任何地方的网络活动，如人口监测等。

尽管如此，华为拒绝回答关于其在伊朗或其他受制裁国家的业务的详细问题。在其提交给委员会的书面资料中，华为再次重申它限制了其将来在伊朗的业务，主要是因为国际社会进一步的制裁以及在伊朗回款的困难度增加。不过华为也强调，“华为尊重其与客户签订的合同”，因而不会终止在伊朗现有的合同 [123] 。华为声称将“遵守联合国、美国、欧盟以及其他国家和地区关于制裁的法律法规 [124] 。”同时也声称已经建立了一个关于贸易合规的内部流程，从而可用最好的去处理这些事务 [125] 。但华为拒绝提供任何有关其决定缩减在伊朗的业务，或其他有助于让我们相解华为(美国)在遵守美国法律的内部文件。

这些资料其实可以帮助华为证实其做出的公司的决策是基于遵循法规的要求，而非基于中国政府压力影响。

（十一）华为拒绝提供其研发项目细节和其他文件，这降低了华为所声称的没有为中国军方或

情报部门提供研发帮助的可信度。

为了了解华为在多大程度上为中国军方或情报部门进行研发活动，委员会要求华为提供关于其代表中国政府或军方的相关业务的信息。具体而言，委员会要求华为提供由中国政府支持或资助的任何技术，设备，资金项目的信息。在其提交给委员会的书面材料中，华为未能提供关于政府支持的研发活动的具体细节 [126] 。相反，华为只是声称它仅仅竞标公开投标项目 [127] 。

在与委员会的会谈中，华为同样声称其并未对中国军方或国家安全部门提供特殊服务 [128] 。

在回答委员会听证会后的问题时，华为又一次宣称其“从未运营过任何解放军的网络”以及“从未受到中国政府的资助去帮助军方系统进行研发项目”。然而，华为的确承认它为中国军方开发了占华为总销售额千分之一（0.1%）的“传输网络产品、数通产品、视频会议产品、数据中心和VoIP产品 [129] ”。然而, (矛盾的是), 华为也声称，它“仅仅为民用目的开发，研究和制造通信设备。 [130] ”

委员会也从前任华为员工那里收到华为内部的文档，文档显示华为曾为一个被认为是解放军内部的特种网络战部队提供特殊网络服务 [131] 。这些文档看起来是华为官方可信的文件，该前任员工声称在他还是华为员工时收到的这份材料 [132] 。这些文件再次表明，当描述该公司代表解放军所进行的研发和其他活动时，华为官员也许不是那么乐于提供信息。

委员会发现华为关于其对中国军方的销售额的陈述是内在前后矛盾的。委员会也发现华为未能完全回答关于其研发活动的细节问题，再加上它承认为中国军方提供了产品，以及从员工那里收到的文件，都削弱了华为所声称的没有为中国政府或军方进行研发活动的可信度。

（十二）前任与现任华为员工提供了关于华为官员潜在非法行为的模式与实际证据

在调查期间，一些前任和现任华为员工主动提供了关于华为在美国行动的声明和指控。出于所涉及问题的敏感性考虑以及为了保护证人不被报复或解雇，委员会决定对这些人的身份保密。委员会已从这些人那里收到关于华为官员一些潜在违规行为的大量可信的证据。这些指控包括：

* 违反移民法
* 贿赂和腐败
* 歧视行为
* 侵权问题

具体 而言，委员会从许多员工那里听说，从中国来短暂旅游签证或持会议签证的华为员工事实上在华为美国全职办公，这违反了美国的移民法。类似的，华为员工提供了可信证据表明，持特殊技术人才签证（如工程师专业）来美国的人在华为美国并未被被雇用。这些与其他违反移民法的指控将被移交国土安全部进行审理及有可能的进一步调查。

其次，员工实例指控了华为在与美国寻求商业合同时有欺诈和贿赂行为 [133] 。这些指控将被移交司法部进行审理和可能的进一步调查。

第三，委员会约谈的华为员工谈到了对华为官员普遍的歧视行为的指控。这些员工声称，对于非中国籍员工而言，在美国的华为机构获得提拔是非常困难甚至不可能的。此外，这些员工声称非中国及员工经常被解雇，工作岗位被 来自中国持短期签证的员工所取代 [134] 。这些指控将被移交行政机构的相关部门进行审理和研究。

最后，委员会从前华为员工那里得知，华为在其美国办公部门建立了一种使用盗版软件的方式并行为。如前所述，委员会收到消息称，华为公司的商标标志有意的而且公开的违反了另一家公司受版权保护的材料 [135] 。委员会因此发现，华为公司非常粗心的不顾其他机构的版权问题。由于这些员工的指控可能是可信和属实的，委员会也会将这些指控移交司法部进行调查。

B. 中兴公司未能回答关键性问题或提供相关文件来支持其声明，这些声明辩称，回答委员会关于其公司内部活动的问题有可能导致该公司触犯中国国家机密。

在整个调查期间，中兴力图表现得合作，并及时提交委员会需要的文件。然而中兴一直拒绝对一些具体问题做出明确的回应，该公司也未能提供内部文件来支持其多项声明。与对华为公司一样，委员会对中兴公司的审查重点放在其与中国政府的关系，以及该公司的历史、管理、财务、研发和企业架构上。委员会未收到关于下列问题的详细答案。中兴未能描述其与中国政府的正式往来关系。它没有提供除了已公开信息之外的财务信息，没有解释中兴内部共产党党委的正式角色，只在最近才提供了党委成员的信息。委员会没有收到关于中兴在伊朗和其他被制裁国家的经营和活动的细节。最后，中兴拒绝提供其在美国的经营和活动的详细信息。

同样重要的是，因为担心会违反中国的国家机密从而导致中兴官员在中国被起诉，中兴极力辩称它不能提供内部机密文件或对调查委员会的某些问题做出回答 [136] 。事实上，由于担心有可能涉及国家机密，中兴甚至拒绝提供在2012年4月会议期间给委员会展示的幻灯片。就某种程度而言，因为中国的法律视这些信息为国家安全机密，从而中兴不能向委员会提供详细说明或回应委员会的质询。调查委员会对中兴参与美国基础设施项目对美国国家安全的影响的担

忧更加加深了。

委员会注意到，中兴提交的许多书面材料从未配合委员会的特定问题和文件要求进行编号，而这本应作为正式法律程序所应该的。委员会相信，中兴通过这种方法试图拒绝坦诚的回答 问题。此外，中兴的回答通常是重复的，缺乏文件或其他证据支持，或者在其他方面不甚完整。

委员会还注意到，中兴并未简单地否认来自全球电信供应链的国家对国家安全的担忧。中兴一直倡导一种解决方案——一种基于信任交付模式的——通过被双方都信任的“独立的第三方评估人员”来移交“硬件、软件、固件及设备中的其他结构件到相应的评估人员” [137] 。这种被中兴所倡导的模式还包含许多其他因素，例如，一个“经过彻底审查和分析的软件代码”、“漏洞扫描和渗透压力测试”、“硬件设计的审查和审核系统框架设计示意图”、“物理设施的审查和对供应商的生产、仓储、加工及交付操作的独立综合审查”、“定期评估”等等。

中兴建议，这种之前曾也被华为及其他公司提出，很类似在英国提出的模式，可以在电信设备供应商之间广泛实施。如前所述，虽然这些缓解措施有一定帮助，委员会仍然担心这种模式未能缓解电信设备的对国家安全非常重要的本质。

（一）中兴未能缓解委员会对中国国有企业在中兴业务决策和运营的控制的担忧

与华为类似，委员会担忧中国政府对于中兴业务的影响。这种影响为中国政府提供一个现成的途径来利用包含中兴设备的电信基础设施为中国国家服务。为了评估中兴与中国政府的联系，委员会很关注该公司的历史，结构和管理。许多评论家指出，中兴的资产包含有中国国有企业的重大投资和参与，因此，委员会试图分析其目前的运作情况及股权结构，希望了解该公司是否还与中国政府保持联系。
中兴将自己描述为一个业务遍布140个国家的全球电信设备和网络解决方案供应商。公司成立于1985年，中兴声称2011年营业同比增长了24％，达到137亿美元，其海外营业收入同比增长30％，在此期间达到74.2亿美元，占公司总营业收入的54.2％ [138] 。中兴声称，其系统和设备被国际市场的顶级运营商所使用。重要的是，中兴还在其2011年报中强调，中国的第12个五年计划对中兴最近在国内市场的成功做出了重要肯定 [139] 。

在2012年4月至5月与中兴官员的访谈中，他们强调中兴是一家上市公司，于1997年在深圳证券交易所上市，2004年在香港证券交易所上市。中兴辩称，它并非靠政府援助起家，也没有来自政府的技术转让和财务上的援助。然后，中兴承认中国政府在1997年的公开发售时是其股东之一。中兴坚持认为国有企业股东对其战略方向没有任何影响 [140] 。虽然很少指名道姓，中兴经常将自己与华为进行比较，认为华为是中兴的主要竞争对手。但认为因为中兴是一家上市公司，因此更加透明公开化。

这些官员通常借助公司已经是上市公司来声称其财务是透明的，且一贯遵守符合中国大陆及香港关于上市公司的资产公开规定。他们通常仅仅引用公司年报所公开的信息来回应委员会对于详细信息的质询，例如政府贷款的金额和比例，补贴和信贷等。然而，中兴拒绝表示是否愿意达到西方股票交易市场（如纽约证券交易所）所要求的透明度 [141] ，和华为一样，当委员会试图向中兴质询更多与政府关键部门互动等问题时，中兴表示拒绝回答。

正如该公司在向委员会提交的书面材料中承认的那样，中兴的历史和结构揭示了其与中国政府和重要军事科研院所存在目前还保留的与过去的历史联系。在回应质询时，中兴官员的回应与其中兴在建立初期来自于国家航空航天部，一家政府机构的公开声明自相矛盾。事实上，从在深圳会议期间所展出的一些展品可以看到中兴早期和中国政府的691厂，以及其他国有企业之间的合作紧密。中兴拒绝向委员会提供在本次会议期间所展示幻灯片的副本。

相反地，中兴官员声称侯为贵先生于1985年与其他五个工程师一起建立了中兴公司。虽然这些人都曾在国有企业工作，中兴官员坚持认为，中兴的创立并非来自于与政府的关系。该公司在其向委员会提交的书面材料中承认，其早期与政府所创立的691厂有联系 [142] 。按照中兴的描述，691厂现在的名称是西安微电子公司，是中国航天电子技术研究院——一家国有机构的附属公司。在其提交的材料中，中兴也承认，西安微电子技术研究所拥有中兴新的34%的股份——中兴新是中兴的股东之一 [143] 。中兴从与中国政府和军队有联系的研究机构的演变其实恰恰凸显了中国信息技术(IT)产业格局的本质。事实上，即便中兴提交的关于其历史和所有权的材料全部是真实的，中兴的演变恰恰证实了研究中国IT行业的分析家的怀疑，他们认为中国的IT行业是服务于商业和军事的混合体 [144] 。
1997年，中兴首次在深圳证券交易所公开上市。中兴的高管声称，正是在那时，其他国有企业才开始投资中兴。

目前，中兴30％的股份为中兴新集团所持有，其余70％股份由分散的公众股东持有。委员会特别感兴趣的是，中兴新持有的30％的股权是否有主要控制力，否则给国有企业提供了对中兴施加影响力的机会。这个问题非常重要，因为有两家国有企业拥有了中兴新51％的股份。中兴的高管强调，公众持股的比例正在上升，因为中兴新正在出售其持有的中兴股份（例如， 2004年中兴新持股44％，而现在其持有的股份是30％）。在7月3日中兴提交给委员会的材料中，中兴表示，“了解中兴的人士很少将其视为一家国有企业（SOE）或一个被政府控制的公司。
[145] ” 但是委员会特意问到，在这种股权结构下中兴如何保持向股东负责的原则，而又不受其最大股东的影响或控制。在提交给委员会的材料中，中兴也承认，30％的股权在香港及中国的法律中均被认为是构成“控股股东”的份额 [146] 。对此质询，中兴简单的表示，该公司与大量股东的信托责任意味着控股股东事实上并不能对公司施加太多的实际控制权 [147] 。中兴并没有更详细地解释五位由国有企业选出的董事会成员，其中几位还是共产党员或公司内部党委成员，为何不能对公司的决策施加影响。

中兴新，中兴的第一大股东由两家国有企业部分所有，分别是西安微电子公司和广宇航空，这两家公司与中国政府不仅有所有权联系，据说也承担了中国政府和军队敏感技术的研发。中兴未能回答委员会关于这两家公司的历史、任务等详细信息的问题。中兴也没有回答这些公司与中兴的关键领导人，特别是侯为贵先生以及中兴的另一主要股东Zhongzing WXT之间的关系。

由于中兴未能回答其公司历史和与政府机构的关系等关键问题，因此委员会不能相信中兴未受政府干涉，特别是政府通过其主要股东和董事会成员对其产生的影响。

（二）中兴在其公司内部保留了中国共产党委员会，但并没有完全解释该委员会的职能、成员选举机制、以及与中国共产党有何关系。

与华为一样，中兴与中国共产党的关系是委员会的重点关注。这种关系使得中国共产党有机会影响公司的决策和运营，而该公司正在试图扩大在美国的关键基础设施建设。如前所述，如果不被中国共产党所控制（很大程度上是通过在个体企业中设立的党委），现代中国的国家资本主义经济将受到重大影响。

在与中兴官员的访谈中，中兴拒绝回答其高层或董事会成员是否是中国共产党党员。中兴首先淡化了公司内部党委的存在，公司代表也未能回答是否有董事会成员是中国共产党党员。随后，在应对委员会接下来的问题过程中，中兴承认在其内部确实存在党委，并指出这是由中国法律所要求的。然而，在回答委员会的书面问题时，中兴再次拒绝提供党委成员的姓名及职务。而在2012年9月13日的听证会上，中兴发言人朱先生曾宣誓，中兴将提供这些人的名字。

作为对2012年9月13日听证会上所提出的问题的应对，中兴的确向委员会提供了一份中兴内部19位党委成员的名单。这19位党委成员中，至少有两位是中兴董事会成员，其他人是中兴实体的主要股东。应中兴的要求，委员会已同意不对外公开这些人的姓名。中兴试图说法委员会这些人对公司的决策不会产生大的影响。中兴请求委员会不公布这些人的姓名，是担心公司或这些个人可能面临中国政府或中国共产党的报复。委员会已决定在公开报告中不公布这些成员的姓名，但公司由于其仅仅向委员会成员提供了中兴内部人员姓名而担心中国政府潜在报复的担忧则更加凸显了为何调查委员会认为中国政府是中兴公司的幕后决策者。 中国政府显然试图在中国经济体中保持重要角色并刻意低调。当这些受中国政府控制的公司要在美国建立关键基础设施时， 相应的公司行为及其透明程度让人担忧。
中兴也没有完全解释党委在其公司的功能。相反，中兴简单的宣传委员会由公司管理层所控制。这种说法与中兴自己的声明“中兴高管和董事会成员是中国共产党的成员并与其活动划清界限” [150] 自相矛盾。在某种程度上，这些高管和董事会成员对公司股东和国家（通过共产党的领导）都有义务，在职责上有内在的利益冲突，这份声明确认了中国共产党可能通过这些人实际地影响和参与公司业务。

在独立董事Timothy Steinert的作证声明中，旨在消除任何政府或党的影响的担忧：

“根据我的经验和据我所知，中兴董事会没有任何成员，（在公司决策时，）曾经提出要考虑代表中国政府、中国人民解放军或是中国共产党的利益。”

这份声明并没有消除委员会的担忧。首先，公司的日常运作和战略决策有一些并不是由董事会决策和审核。Steinert先生的宣誓书没有提到中国共产党在这些决策到达董事会之前所施加的影响，或对那些根本没有通过董事会的决策的影响。另外，中国共产党通过中兴党委的影响可能不会明显的表现在为董事会审核所提供的决策文件中。由于至少有两名董事会成员是中国国产党的党员，因此无法得知董事会的表决结果是否未收到中国共产党的影响。当在处理中兴的业务或在一些事务方面投票时，这些董事会成员不需要搬出共产党来去代表国家或者政府的利益。基于以上两点考虑，委员会认为中兴声称Steinert先生的作证书中“确定中兴商业决策的制定没有受到政府或共产党的影响”是不具说服力的［152］。

中兴近期声称内部党委“只执行礼仪性和社会职能”。在过去的六个月，委员会向中兴询问关于党委的作用，但直到最后时刻中兴也没有提供任何回应。由于没有更多关于党委在公司运营中起影响作用的信息和细节，委员会无法减轻对这些存在于一个正在试图铺建美国国家基础通讯设施的公司内部共产党组织的担忧。

（三）中兴未能披露与其在美国的活动相关的信息。

中兴提及其业务遍布全球140个国家，但通过暗示其在美国95%的销售额主要来自手机，来淡化了其对美国的潜在威胁。中兴官员强调，他们在美国有五个研发中心，雇用员工约300人。中兴官员试图表明，该公司在美国农村基础设施和网络的业务是在努力帮助美国的宽带业务。委员会工作人员对这种逻辑提出质疑，中兴官员也承认中兴在这些项目中所扮演的角色不是慈善机构或公共服务，就像他们最开始谈及的，是希望在美国获得一个“立足之地”，并希望在美国学到技术。中兴官员甚至承认，他们愿意在美国以低于成本价格提供设备，以达到学习美国市场的目的。特别地，在委员会与中兴官员在深圳会见期间，朱先生表示，该公司愿意在美国亏本以获得立足之地，并了解美国的技术和标准。

中兴对其当前在美国的活动的描述是一个片面和局部的描述。由于中兴没有对委员会质询文件作出应答，委员会无法确定该公司的合同或进入美国市场的程度。尽管多次质询，中兴并未提供其在美国基础设施建设项目的详细信息，也未能回答中兴是否有意以低于成本价的进行项目投标的问题，以及公司如何处理这些商务损失。此外，在9月13日的HPSCI（House Intelligence Committee，美国众议院情报委员会）听证会上，朱先生推翻了他之前的回答，并拒绝承认中兴在美国以低于成本价投标［155］。

（四）中兴未能提供任何其遵守知识产权或美国出口管制法律的证据。

对知识产权的保护和遵守美国出口管制法对维护美国利益至关重要。一个商业公司遵从这些法律的能力可以被用来有效检验其遵从国际商业行为惯例的能力和避免政府过度影响的能力。

中兴公司代表一直拒绝对近日媒体关于中兴向伊朗出售出口管制项目的报道进行评论[156]。在2012年9月13日的听证会上，中兴承认其正在进行内部审查，以确定该公司是否销毁了任何与其在伊朗的活动相关的文件或其他证据[157]。朱先生未能提供任何信息，以便让委员会评估这些销毁证据事件的程度、其是否遵守美国法律或有管理层的参与。中兴未能回答委员会关于为什么需要限制其在伊朗的业务活动；中兴是否将履行目前与伊朗的合同；这些合同是否包括培训或监控设备的维护等相关问题。此外，中兴拒绝回答其在伊朗转售何种产品的问题。中兴也拒绝提供任何关于其在伊朗的活动的文件。

（五）中兴未能向委员会提供关于其研发业务的信息，尤其是涉及到军事或政府项目的业务。

鉴于中兴的背景，委员会对中兴的研发活动，尤其是其与（或代表）中国军事和安全服务有关的研发活动很感兴趣，特别是它的研发活动或代表的中国军事或安全服务。这些信息有助于委员会评估该公司在美国建设基础设施的同时是否也在为中国政府研发项目并试图找出或利用这些系统中的漏洞。

委员会对中兴与中国政府相关研究机构的众所周知的关系尤为感兴趣。例如，中兴承认其主要股东之一中兴新，部分归属于西安微电子公司，这是国有研究机构中国航天电子技术研究院的一个下属单位[158]。中兴新的另外17%股份由航天广宇所持有，这是一家国有企业的子机构，其业务除其他之外还包括航天技术产品[159]。中兴未能回答委员会关于这些研究机构为中国政府生产的产品的范围的详细信息，因此委员会无法评估这些技术是否与军事或情报目的有关[160]。

由于中兴这些业务活动都与中国政府的研究机构和生产企业有关，委员会试图寻求更多关于中兴研发活动的细节，特别是其潜在的代表政府、军队或安全服务的工作。中兴很自豪地解释说，它已在中国、法国和印度建立了18个最先进的研发中心，并雇用超过30,000名专业研究人员。中兴还声称，该公司的年销售收入的10％投资于研发。但是中兴未能回答委员会关于其为中国政府和军队研发或出售技术的问题。在2012年4月12日委员会与公司官员的会议中，公司的独立董事会成员Steinert先生声称：中兴为那些恰好是国有企业的中国电信供应商所做的工作并不表明中兴在为中国军事或情报部门工作。当提供书面答复时，中兴拒绝为其在代表中国军事或安全部门的工作的性质和程度提供明确答案。相反，中兴声称“中兴在过去的几年里收到的来自中国政府或财团的资金与世界上其他从事研发的公司通过正常途径获得资金的方式没有区别[161]。”

既然中兴的研发活动仅仅是通过正常的政府采购程序，委员会不理解它为何不直接回答这些项目的细节问题。出于这个原因，委员会不能消除中兴与中国军事情报活动或研究机构有密切联系的担忧。

结论与建议

为了寻求长期对关于中国电信公司（华为和中兴）与中国政府之间关系的问题的答案，调查委员会发起了这次调查。在为期数月的调查中，华为和中兴都试图用不同的描述方式，解释了为何这两家公司都没有对美国的国家安全利益构成威胁。令人遗憾的是，两家公司都没有与我们的调查完全的合作，两家公司都未能提供文件或其他证据来证实他们的说法或支持他们的陈述。

尤其是华为，对委员会提出的核心安全问题提供了模棱两可、答非所问或不完整的答案。这些公司未能对关于它们与中国政府的关系及政府对它们的支持这些问题提供积极有效的答案，使得人们对其能否遵守国际规则产生了进一步的疑问。

建议

基于本次调查，委员会提供如下建议：
建议1：美国应该用怀疑的眼光检视中国电信公司对美国电信市场的不断渗透。

* 美国情报体系（IC）必须保持警惕，并专注于这一威胁。 IC应试图积极知会私营部门，并尽可能使其知晓该威胁。

* 考虑到对美国国家安全利益的威胁，美国外商投资委员会（CFIUS）必须阻止涉及华为和中兴的收购、吞并或合并。试图扩大CFIUS并使其包含采购协议的立法提案应由相关国会委员会进行详细考虑。

* 美国政府尤其是敏感系统，不应使用华为、中兴的设备，包括零部件。同样，政府的承包商，特别是工作于那些美国敏感项目的合同的，应该在系统中排除使用中兴和华为的设备。

建议2：强烈建议美国的私营部门实体考虑与中兴或华为开展设备或服务业务的长期安全风险。强烈建议美国网络运营商和系统开发商在其项目中寻求其他的供应商。基于现有的机密和公开信息，华为和中兴不能被认为未受中国国家影响，这对美国和我们的系统构成了安全威胁。

建议3：美国国会司法委员会和行政部门的执法机构应当调查中国电信行业的不公平贸易行为，尤其要注意中国对关键企业提供的持续财政支持。

建议4：中国企业应当尽快变得更加开放和透明，包括在具有更高透明度要求的西方证券交易所上市，提供更加一致的由独立的第三方评估机构进行的财务信息和网络安全的审查，遵守美国的信息和举证的法律标准，并遵守所有的知识产权法律和标准。尤其是华为，必须更加透明和响应美国的法律义务。

建议5：美国国会司法委员会应考虑立法，以更好地解决由后面存在政府支撑的电信通讯公司带来的风险，否则这些公司不能完全被信任参与美国关键基础设施建设。这种立法可以包括增加私营部门实体之间的信息共享，并在CFIUS争取包含采购协议的过程中发挥更大的作用。

参考文献

1 Ken Hu, “Huawei Open Letter.” http://online.wsj.com/public/resources/documents/Huawei20110205.pdf (accessed August 2, 2012).

2 Huawei’s letter was issued in February, 2011, when the Committee on Foreign Investment in the United States (CFIUS) issued a recommendation that Huawei voluntarily divest assets it received in a 2010 deal with 3Leaf, a United States company that developed advanced computer technologies. Shayndi Raice, “Panel Poised to Recommend Against Huawei Deal,” Wall Street Journal, February, 11, 2011. http://www.wsj.com/article/SB10001424052748704629004576136340771329706.html (accessed August 2, 2012)

3 A classified annex to this report provides both classified information relevant to the discussion, as well as information about the resources and priorities of the IC.

4 Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,” IEEE Control Systems Magazine, December 2001.

5 “The former National Counterintelligence Executive, Mr. Robert Bryant, recently noted that, ‘Insider threats remain the top counterintelligence challenge to our community.’ An insider threat arises when a person with authorized access to U.S. Government resources, to include personnel, facilities, information, equipment, networks, and systems, uses that access to harm the security of the United States. Malicious insiders can inflict incalculable damage. They enable the enemy to plant boots behind our lines and can compromise our nation's most important endeavors. Over the past century, the most damaging U.S. counterintelligence failures were perpetrated by a trusted insider with ulterior motives.” http://www.ncix.gov/issues/ithreat/index.php

6 FBI, Intelligence Bulletin, “Supply Chain Poisoning: A Threat to the Integrity of Trusted Software and Hardware,” June 27, 2011: 1.

7 Office of National Counterintelligence Executive, Report to Congress on Foreign Economic Collection and Industrial Espionage, “Foreign Spies Stealing US Economic Secrets in Cyberspace.”(October 2011, Washington, DC: 1.)

8 United States Congress, 2011 Annual Report of U.S.-China Economic and Security Review. (2011, Washington DC: 59.)

9 National Institute of Standards and Technology, Draft NISTIR 7622, “Piloting Supply Chain Risk Management for Federal Information Systems,” June 2010, 28.

10 Joint Press Conference, March, 29, 2012, Sydney, Australia. http://www.pm.gov.au/press-office/transcript-joint-press-conference-sydney-1.

11 The Economist, “Huawei: The Company that Spooked the World,” Economist, August, 4, 2012. http://www.economist.com/node/21559929 (accessed September 30, 2012).

12 United States Congress, 2011 Annual Report of U.S.-China Economic and Security Review. (2011, Washington DC: 148.)

13 Office of National Counterintelligence Executive, Report to Congress on Foreign Economic Collection and

Industrial Espionage, “Foreign Spies Stealing US Economic Secrets in Cyberspace.”(October 2011, Washington, DC: i.)

14 Ibid, 5; HPSCI staff interviews with cyber-security experts.

15 Ibid, 5.

16 Defense Science Board, Report on Mission Impact of Foreign Influence on DoD Software, September 2007: viii.

17 “Where State security requires, a State security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual.” State-Security Law of the People’s Republic of China, Article 11.

18 Defense Science Board, Report on Mission Impact of Foreign Influence on DoD Software, September 2007: viii.

19 Northrop Grumman Corp, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage, prepared for U.S.-China Economic and Security Review Commission, March 7, 2012, 6-8.

20 The Economist, “The Long March of the Invisible Mr. Ren,” the Economist, June 2, 2011. http://www.economist.com/node/18771640 (accessed on September 15, 2012).

21 FBI, Intelligence Bulletin, “Supply Chain Poisoning: A Threat to the Integrity of Trusted Software and Hardware,” June 27, 2011: 4.

22 ZTE, Submissions to HPSCI, July 3, 2012; ZTE, Submission to HPSCI, August 3, 2012; Ken Hu, “Huawei Open Letter.” http://online.wsj.com/public/resources/documents/Huawei20110205.pdf (accessed August 2, 2012). John Suffolk, Huawei’s Global Security Officer, previously served as the Chief Information Officer with the UK government at a time when the UK entered into its agreement with Huawei to set up the Cyber Security Evaluation Center (CSEC). Mr. Suffolk advocated for a cyber- security and supply-chain solution that would recognizing the issues as a global concern that must be addressed at an international level, preferably by an international standards-setting organization through which all products must pass. Mr. Suffolk also highlighted that in the present age, technology is moving faster than our ability to adapt our institutions. Key assumptions are that security requires a whole systems approach, and that all systems will be breached at some point. Thus, in Mr. Suffolk’s view, telecommunications companies and governments must manage the risk, focus on areas of most concern, instill diversity and adaptability, and learn to deal with the consequences. Mr. Suffolk acknowledged that Huawei’s desire to be an end-to-end provider for whole network solutions does not align with his proposed solutions to the supply-chain concerns, which depend on diversity of supply. HPSCI meeting with John Suffolk, February 23, 2012.

23 Anderson, R., & Fuloria, S. Certification and Evaluation: A Security Economics Perspective. Emerging Technologies and Factory Automation, (2009).

24 Ken Thompson, Reflections on Trusting Trust. Turing Award Lecture, (1984).

25 Gerwin Klein, Formal Verification of an OS Kernel. Symposium on Operating Systems Principles. Big Sky, MT, USA: Association of Computing Machinery, (2009).

26 Daniel Jackson, Martyn Thomas, and Lynette I. Millett, Eds. Software for Dependable Systems: Sufficient Evidence? Committee on Certifiably Dependable Software Systems, National Research Council. (National Academies Press, 2007.)
27 Rules of the House of Representatives, 112th Congress, Rules 10(3)(m), 11.
28 Understanding and developing a strategy to protect the country from Chinese cyber espionage in the United States is one of the obligations of U.S. counterintelligence professionals. Many reports have suggested that the Intelligence Community continues to struggle integrating and acting on its counterintelligence mission. As Michelle Van Cleave, former head of the National Counterintelligence Executive, has explained, "the U.S. government has been slow to appreciate the effects of foreign intelligence operations, much less to address the threats they pose to current U.S. foreign policy objectives or enduring national security interests." Michelle Van Cleave, "Chapter 2: The NCIX and the National Counterintelligence Mission: What Has Worked, What Has Not, and Why," in Meeting Twenty-First Century Security Challenges, 62.
29 Office of National Counterintelligence Executive, Report to Congress on Foreign Economic Collection and Industrial Espionage, "Foreign Spies Stealing US Economic Secrets in Cyberspace."(October 2011, Washington, DC)
30 In response to the Committee's June 12, 2012, document request, ZTE provided one document: a summary of its cyber-security measures. Huawei provided no documents other than materials already on the company's website or otherwise publicly released. After the September 13, 2012 hearing, Huawei provided a document labeled "Internal Compliance Program (ICP)," dated March 2012. That document summarizes Huawei's internal policy with respect to trade control policies. Huawei provided no material that would allow the Committee to evaluate their compliance with or enforcement of that policy. Huawei also provided a copy of the publicly released paper entitled "Cyber Security Perspectives" prepared by John Suffolk, and Huawei's public statement regarding its Commercial Operations in Iran.
31 House Permanent Select Committee on Intelligence, Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Congress, 2nd session (September 13, 2012).
32 Given the sensitivities involved, and to protect these witnesses from retaliation or dismissal, the Committee decided to keep the identities of these individuals confidential.
33 As the U.S.-China Commission has highlighted, even the largely circumstantial evidence that known incidents appear state sponsored is compelling -- as the actors' targeting often focuses on key defense and foreign-policy sources of information, which are of most concern to the state and not commercial entities. United States Congress, 2011 Annual Report of U.S.-China Economic and Security Review. (2011, Washington DC: 59.)
35 United States Congress, 2011 Annual Report of U.S.-China Economic and Security Review. (2011, Washington DC: 59-60.)
36 ZTE, Submission to HPSCI, July 3, 2012, 3.
37 Discussion with PLA Piper, June 2012. Huawei, in its responses to Questions for the Record after the

September 13, 2012, hearing, denied that there is any state-secret concern with their documentation. The Committee is left wondering, then, why Huawei has refused to provide internal documentation that could substantiate its claims. Moreover, Huawei's failure to provide the list of individuals on Huawei's Chinese Communist Party Committee is an example in which the Committee believes the state's concerns with state secrets is particularly relevant. Huawei's continuous failure to provide such information cannot be explained otherwise.

38 Huawei Investment & Holding Co., Ltd., 2011 Annual Report, 7.

39 Ken Hu, "Huawei Open Letter." http://online.wsj.com/public/resources/documents/Huawei20110205.pdf (accessed August 2, 2012).

40 That report suggests that Huawei "was founded in 1988 by Ren Zhengfei, a former director of the PLA General Staff Department's Information Engineering Academy, which is responsible for telecom research for the Chinese military. Huawei maintains deep ties with the Chinese military, which serves a multi- faceted role as an important customer, as well as Huawei's political patron and research and development partner. Both the government and the military tout Huawei as a national champion, and the company is currently China's largest, fastest-growing, and most impressive telecommunications-equipment manufacturer. Evan Medeiros et al., A New Direction for China's Defense Industry, Rand Corporation: 218-219. http://www.rand.org/pubs/monographs/2005/RAND_MG334.pdf.

41 Ibid, 217-219

42 The Economist, "Huawei: The Company that Spooked the World," Economist, August, 4, 2012. http://www.economist.com/node/21559929 (accessed September 30, 2012).

43 Juha Saarinen, "Analysis: Who Really Owns Huawei?," ITNews, May 28, 2012.

44 Ken Hu, "Huawei Open Letter." http://online.wsj.com/public/resources/documents/Huawei20110205.pdf (accessed August 2, 2012).

45 Richard McGregor, The Party: The Secret World of China's Communist Rulers, 2010: 204.

46 Huawei, Submission to HPSCI, July 3, 2012.

47 House Permanent Select Committee on Intelligence, Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Congress, 2nd session (September 13, 2012).

48 Huawei Investment & Holding Co., Ltd., 2011 Annual Report, 2.

49 Huawei, September 25, 2012 Response to Questions for the Record, at __. 50 Huawei, September 25, 2012 Responses to Questions for the Record, 6-7. 51 Interviews with Huawei officials, February 23, 2012.

52 Interviews with Huawei officials, February 23, 2012.

53 Interviews with Huawei officials, February 23, 2012.

54 Mike Rogers and Dutch Ruppersburg, letter to Huawei, June 12, 2012; Huawei, letter to HPSCI, "Response to June 12, 2012 Letter," July 3, 2012.

55 Huawei, Documents Provided in Advance of February 23, 2012 entitled Shareholder Agreements.

56 John Lee, "The Other Side of Huawei," Business Spectator, March 30, 2012.

57 United States Congress, 2011 Annual Report of U.S.-China Economic and Security Review. (2011, Washington DC: 59)
58 Ibid.
59 House Permanent Select Committee on Intelligence, Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Congress, 2nd session (September 13, 2012).
60 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012, 1.
61 Ibid.
62 Ibid.
63 Huawei, July 2, 2012 Submission, 7-15
64 Highlighting that as China moved from a pure control economy in the 1990s, Chinese companies experienced particular difficulties raising capital in foreign capital markets, including the "most sensitive of all, how would they explain the role of the internal party bodies, which for years had run companies, free of any of the inconvenient structuring of corporate reporting and governance rules." Richard McGregor, The Party: The Secret World of China's Communist Rulers, 2010: 47; See John Lee, "The Other Side of Huawei," Business Spectator, March 30, 2012
65 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012, 2.
66 Ibid.
67 See John Lee, "The Other Side of Huawei," Business Spectator, March 30, 2012; Richard McGregor, The Party: The Secret World of China's Communist Rulers, 2010.
68 Richard McGregor, The Party: The Secret World of China's Communist Rulers, 2010: 72.
69 Meeting with Mr. Ren, May 23, 2012.
70 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012.
71 Huawei officials stated that China had cancelled ranking system at the time. HPSCI Interviews with Huawei officials, February 23, 2012.
72 Huawei officials suggested that the rumors that Mr. Ren is a former PLA General is the result of confusion with Julong, another Chinese telecommunications company and state-owned enterprise whose President is a Major General in the PLA. HPSCI Interviews with Huawei officials, February 13, 2012.
73 Huawei, September 25, 2012 Responses to HPSCI Questions for the Record, 8.
74 Huawei, September 25, 2012 Responses to HPSCI Questions for the Record, 8.
75 Huawei asserted that Chen Jinyang, who invested 3,500 RMB, was a 26-year-old manager at the Chinese Trade Department.
76 Interviews with Huawei officials, February 23, 2012.
77 Interviews with Huawei officials, February 23, 2012.
78 Interview with Ken Hu, February 23, 2012.
79 Scholars of the Chinese political economy suggest that national champions are those chosen by China to be supported both financially and otherwise by the state because of the strategic importance of the sector and

the company to China's national interests. See John Lee, "The Other Side of Huawei," Business Spectator, March 30, 2012
80 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012, 19. 81 Ibid.
82 Interviews with Huawei officials, February 23, 2012; Huawei presentation, February 23, 2012. 83 Interviews with Huawei officials, February 23, 2012
84 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012, 19-20. 85 Mike Rogers and Dutch Ruppersburg, letter to Huawei, June 12, 2012, 6.
86 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012, 19-20. 87 Phone conversations with Huawei representatives, June 2012.
88 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012, 20-21. 89 John Lee, "The Other Side of Huawei," Business Spectator, March 30, 2012.
90 The Economist, Huawei: The Company that Spooked the World," Economist, August, 4, 2012. http://www.economist.com/node/21559929 (accessed September 30, 2012);
91 House Permanent Select Committee on Intelligence, Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Congress, 2nd session (September 13, 2012).
92 Huawei, Slide Presentation dated November 2011, 8.
93 Huawei, Responses to HPSCI Questions for the Record, September 25, 2012, 1. 94 Ibid.
95 Ibid.
96 Inteviews with Huawei officials, February 23, 2012
97 Huawei, Corporate Presentation, February 23, 2012, 26.
98 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012, 2.
99 Huawei, Corporate Presentation, February 23, 2012, 27.
100 Huawei, Responses to HPSCI Questions for the Record, September 25, 2012, 2.
101 Inteviews with Huawei officials, February 23, 2012.
102 House Permanent Select Committee on Intelligence, Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Congress, 2nd session (September 13, 2012).
103 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012, 21.
104 Interviews with Huawei officials, February 23, 2012.
105 Ren Zhengfei, speech at Huawei BT Division & Huawei UK, June 30, 2007, quoted in Huawei magazine Improvement, Issue 58.
106 The Commerce Department, working with the Defense Department, has sought information from the private sector to better understand the entire scope of cyber-risks facing the country's critical telecommunication infrastructure. The Commerce issued a survey under the Defense Production Act to dozens of U.S. based companies to gather better information on the security of their networks. The review of that information is still ongoing.

107 The Committee has offered on numerous occasions to provide Huawei an opportunity to provide the information the Committee needs to evaluate the security of U.S. networks in a closed forum or under an agreement to provide such information confidentially. Huawei has continuously refused to accept any such offer, option instead to simply assert that such details are confidential. The Committee intends to continue evaluating these issues and plans to approach Huawei in the future for more details on these contracts to fulfill the Committee's duty to evaluate the risk posed by these firms.
108 House Committee on Foreign Affairs, Hearing on Unfair Trade Practices against the US, 112th Congress, 2nd session (July 19, 2012).
109 Interview with Huawei officials, February 23, 2012.
110 Interview with Employees.
111 John Lee, "The Other Side of Huawei," Business Spectator, March 30, 2012.
112 Interview with Huawei officials, February 23, 2012.
113 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012.
114 Interview with Huawei Employees.
115 Interview with Huawei Employees.
116 Interview with industry experts.
117 Huawei representatives admitted to Committee staff that using this presentation was in violation of McKinsey's copyright protections, and that McKinsey and Huawei have no business relationship thus undermining any claim that Huawei had a right to use the slide. Huawei, Slide Presentation dated November 2011, 8 (using McKinsey & Co. material).
118 Interview with Huawei Officials, February 13, 2012.
119 Ibid.
120 Marguerite Reardon, "Huawei Admits Copying," Light Reading, March 25, 2003. http://www.lightreading.com/document.asp?doc_id=30269 (accessed on August 13, 2012)
121 Ibid.
122 House Permanent Select Committee on Intelligence, Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Congress, 2nd session (September 13, 2012).
123 Huawei, Submission to House Permanent Select Committee on Intelligence, July 3, 2012, 6.
124 Ibid.
125 Ibid, 5-6.
126 Ibid, 3-4.
127 Ibid, 3.
128 Interviews with Huawei officials, February 23, 2012.
129 Huawei, September 25, 2012 Responses to Questions for the Record, 12.
130 Ibid.
131 Internal Huawei email, dated July 1, 2011.

132 Ibid.
133 Interviews with former Huawei employees.
134 Interviews with former Huawei employees.
135 Huawei, Slide Presentation dated November 2011, 8.
136 ZTE August 3, 2012 submission, at 12-17.
137 ZTE, Submissions to HPSCI, August 3, 2012, 23.
138 ZTE, 2011 Annual Report, 68-69.
139 "The national '12th Five Year Plan' has provided driving force for the further development of the domestic telecommunications industry." ZTE, 2011 Annual Report, 69.
140 Meeting with ZTE officials, April 12, 2012, Shenzhen, China.
141 ZTE, Submissions to HPSCI, July 3, 2012.
142 Ibid, 4.
143 Ibid.
144 As a report commissioned by the U.S. China-Commission stated: "The IT sector in China can be considered a hybrid defense industry, able to operate with success in commercial markets while meeting the demands of its military customers. The Chinese telecommunications market is heavily influenced by its largest domestic members—such as hardware and networking giants Huawei Shenzhen Technology Company, Zhongxing Telecom (ZTE), and Datang Telecom Technology Co., Limited. These companies and some smaller players are not always directly linked to the PLA or C4ISR modernization because of their strong domestic and international commercial orientation. The digital triangle model, however, allows them to benefit directly from a background network of state research institutes and government funding in programs that do have affiliation or sponsorship of the PLA." Northrop Grumman Corp, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage, prepared for U.S.-China Economic and Security Review Commission, March 7, 2012, 69.
145 ZTE, Submissions to HPSCI, July 3, 2012, 2.
146 Ibid, 9
147 Ibid.
148 Ibid, 4.
149 House Permanent Select Committee on Intelligence,Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Congress, 2nd session (September 13, 2012).
150 John Merrigan, letter to Katie Wheelbarger, September 28, 2012.
151 Affidavit of Timothy Steinert, at para. 6.
152 ZTE, Submissions to HPSCI, August 3, 2012, 5.
153 Meeting with ZTE officials, April 12, 2012, Shenzen, China.
154 Ibid.
155 House Permanent Select Committee on Intelligence, Hearing on Investigation of the Security Threat

Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Congress, 2nd session (September 13, 2012).
156 Ellen Nakashima,"Chinese telecom firm ZTE probed for alleged sale of U.S. surveillance equipment to Iran," Washington Post, July 13, 2012. http://www.washingtonpost.com/world/national-security/chinese-telecom-firm-zte-probed-for-alleged-sale-of-us-surveillance-equipment-to-iran/2012/07/13/gJQA6mKUiW_story.html.
157 House Permanent Select Committee on Intelligence, Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Congress, 2nd session (September 13, 2012).
158 ZTE, Submissions to HPSCI, April 2012, 4.
159 Ibid.
160 Ibid.
161 ZTE, Submissions to HPSCI, July 3, 2012, 17.