2013 年 4 月

在 ICT 全球供应链中建立信任 12 法

达雷尔•M. 韦斯特

对电脑生产过程的分析显示，有 18 个国家为笔记本电脑生产提供了关键部件（不包括诸如生产这些部件中使用的稀有矿物等原材料）。这包括供应液晶显示器部件的八个国家（中国、捷克共和国、日本、波兰、新加坡、斯洛伐克、韩国和台湾），内存生产中涉及的 11 个地区（中国、以色列、意大利、日本、马来西亚、菲律宾、波多黎各、新加坡、韩国、台湾和美国），处理器生产中的九个国家（加拿大、中国、哥斯达黎加、爱尔兰、以色列、马来西亚、新加坡、美国和越南），生产主板的一个地区（台湾），以及硬盘生产中的八个国家（中国、爱尔兰、日本、马来西亚、菲律宾、新加坡、泰国和美国）。[1]

正如笔记本电脑生产过程所揭示的，商业及贸易全球化带来了诸多益处。许多产品的供应成本下降。电脑及其他产品可由不同地区生产的部件组装而成。各个国家可专门生产特定产品而各公司可专注于各自所最擅长的领域。原材料可能来自某个地区，制造及生产过程却在另一地区，而销售及营销又在一个不同地区。在本例及其他例中，当代商业涉及到来自不同大陆间的数百或数以千计个人、组织、技术以及流程的种种交换。

但在产品部署前，过长的供应链及产品评估不够充分或压根就不存在产品评估的情况造成了这样一种局面，产品及网络中存在大面积漏洞，导致其他人可在设计、生产、交货、及安装后保养过程中利用这些漏洞牟利。在采购、运输及管理中存在全行业性漏洞。从原材料到自然灾害到市场力量、国家法律再到政治冲突，问题无处不在。一个领域中的问题可能会传导到另外一个领域并显著放大对整体系统的风险。

这些困难并不是某个具体公司或国家所独有的。赛门铁克在《2012 年智能安全分析报告》中发现，40.9%的恶意病毒来自美国境内，24.9%来自英国，9.1%来自澳大利亚，另有 4.3%源自印度。[2] 事实上，恶意软件已成为全球商业中的一个常见现象。质量控制不足现象出现在全球许多地方。

按 EWA 信息和基础架构技术公司首席执行官 John Lindquist 的说法，“信任不应基于一个组织总部设于何处。”市场是全球性的，供应链问题与网络安全问题及国际贸易更广泛地交织在一起。对美国联邦政府各首席信息官展开的一次调查显示，网络安全位列他们忧虑事项之首。[4] 事实上，无处不在的漏洞需要全面的标准化全球性解决方案。我们需要的是涉及产品评估及对可信赖交付系统依赖的全行业性解决方案。针对整个生态系统中一个部分提出的特殊解决方案注定不会成功。

在本文中，我讨论了在 ICT 全球供应链中建立信任的 12 种方法。在由布鲁金斯学会于 2013 年 2 月汇聚起来的一流专家团队的帮助下，再加上后续跟进访谈的基础上，我在文中探讨了我们面临的运营威胁及技术漏洞，同时就识别最佳惯例、标准及供应链保障进行第三方评估提出建议。

我认为，一般说来，供应链及产品开发中存在的漏洞会为一系列攻击及借此牟利的技术大开

方便之门，例如在产品部署后意在从事种种恶意活动的未经授权远程访问、ICT 网络降级以及对关键基础设施的破坏。我的看法是，开发议定标准、运用独立评估机构、创设认证与鉴定系统以及建立可靠交付系统将会建立起业界对全球供应链以及维系全球供应链的公共与私有行业网络的信心。上述及其他类型评估将便于采购员获得相关信息，从而获得更坚实产品挑选基础。

运营威胁的不可预测性

不可预测性是当代商业所面临威胁的标志。自然灾害、内乱或经济冲击何时会出现难以预知。近年来，对多家公司供应链造成严重后果的此类事件的已不止一次发生。

世界经济论坛在其供应链风险研究中识别出五种主要运营干扰项：自然灾害、冲突与政治动荡、突然性需求冲击、出口/进口限制、以及恐怖主义。5 这些问题可在毫无征兆的情况下对运营、所需原材料的供应、生产及交货时间表以及关键运输网络产生威胁在当前价值链碎片化及严重依赖于分包商的背景下，保障全球范围内产品与服务的及时安全交付已成为一项严峻挑战。

在被问及面临的威胁时，接受世界经济论坛调查的 400 家企业领导人中有 93%表示，他们认为供应链风险在过去五年里有所增加。[6] 日本海啸、大萧条、关键地区内乱以及多个国家贸易保护主义情绪的共同作用使得大多数高管对供应链安全性感到忧心，进而使得他们担心由此造成的特定风险。几乎所有被调查高管都认为，供应链管理及应对种种威胁是各自组织需要优先考虑的事项。

源自环境的危险、地缘政治混乱以及各种经济力量的存在使得几乎所有行业的运营都变得复杂化。按 Don Davidson——美国国防部首席信息官办公室扩展、科学与标准、可靠任务系统与网络项目主管——在我们研讨会上的说法，他掌管的部门需要“为 20 套武器系统采购 120 万种零件”。而且，他还指出，在许多情况下供应商“需要在一周内交付零件”。这使得他的部门面临极其严峻的挑战。

对离岸业务、外包及供应链全球化的日益依重在整个供应链全程各环节增加了漏洞。对离岸业务、外包及供应链全球化日益依重在整个供应链全程处处增加了漏洞。

在产品部署前或在产品生命周期里缺乏漏洞识别及弥补措施的质量控制，这一事实使得该风险进一步加剧。即便是供应链上的一个薄弱环节都可能沿生产线及运输线深入传导下去，危及全球交货时间表。互联网安全联盟首席执行官 Larry Clinton 解释称：“没有漫长的供应链，你便无法在当今全球市场的竞争中立足。”依赖多个供应商会增加竞争性，刺激质量改进，从而削减整体风险。

自然灾害

近期多次发生的自然灾害为供应链面临中断的危险提供了确凿证据。2011 年 3 月日本发生的地震及海啸明确说明了天气及环境变化能够对众多行业的生产及配送产生何种影响。这次风暴横扫多家制造企业所在的日本海岸地区。这场突如其来的灾害夺去 15,000 条生命，导致福岛核电站关闭，随后核电站释放出的放射性物质迫使 90,000 人撤离灾区。因此造成的冲击对多家公司供应链造成严重破坏。例如，日本当月汽车产量较前一年同期下滑 57%。[7]

由于该地区在电子业扮演着里向中国、韩国、台湾及其他地区制造商供应零件的角色，发电厂的关闭拖累了整个电子业。[8]

在同一年里，当大洪水袭击泰国北部地区并最终漫延及该国 77 个省份中的 61 个时，发生了同样的问题。暴涨的洪水淹没了 1,000 家生产厂并导致大面积运营及配送网络中断。汽车及电子产品制造商受灾尤其严重。大多数公司报称大幅减产。该国是电脑硬盘第二大生产国，分析师们称该类硬盘当年产量下滑达 30%。[9] 当这种肆虐广大区域的灾害来临时，很难保证及时交货与满足供应链要求。诸如西部数据等公司估计，至少需要一年时间才能将产量恢复到灾前水平。

地缘政治混乱

地缘政治问题可能肇始于关键地区的内乱、恐怖袭击、腐败或限制全球贸易及商业的法律。原材料产地通常位于存在政治动乱或外部势力间存在争议点。当非洲、亚洲、中东或拉美一旦出现动乱，则生产计划便在事实上不可能完成。

恐怖袭击可扰乱石油、天然气的生产、旅游业及其他重要行业。今年，扣留人质、占领天然气厂四天之久的入侵者曾导致阿尔及利亚天然气短暂停产。该次袭击导致 37 名外国工人死亡，震动了整个北非的贸易及商业。[11]

腐败在世界许多地区都是个严重问题。腐败给商业交易造成额外成本并形成全球供应链瓶颈。

企业永远也无法确定问题将在何处或何时出现，或索贿或特别款项将如何影响交货时间表。联合国全球契约发布的一份报告发现，腐败成本约占全球 GDP 的 5%，或约为每年 2.6 万亿美元。[12] 英国决策与实践证据信息与协调中心 (EPPI-Centre) 在一份研究中发现，“可感知到的腐败指数每增加一个单位则人均收入增速便下降 0.59 个百分点。”[13]

在设置高关税、进入壁垒或过度限制贸易的法律之时，贸易保护主义情绪便招致问题了。[14] 任何限制贸易及商业的举措均为在供应链中设置障碍之举。这种举措可包括针对具体产品设定的关税、对整个板块设定的国内内容规定、或要求国内合作伙伴参与国际商务的规定。微软的 Scott Charney 和 Eric Werner 声称，对国内参与份额设定“自主创新”要求有助于保护供应链，但这种做法的结果却是限制商业、阻碍贸易。[15]

英国商务创新与技能部在一份分析中发现，自 2008 年以来，贸易保护措施已造成全球进口进口额损失 10.4%。[16] 世界贸易组织在一份调查中指出，20 国集团间的贸易限制举措已有所增加。美国与中国就贸易与网络安全的紧张关系不断加剧危及多个不同领域的商业。[17]

经济冲击

经济震荡一直是近年来的主要问题。汇率、大宗商品价格以及宏观经济力量波动剧烈。企业

可以谨小慎微地围绕现有产品配置进行规划，结果却发现自己的规划被经济环境方面的变动所打乱。当经济价格意外上扬时，依赖于最低价投标者的作法就会陷入困境。

如果短期波动扰乱商业模式或导致生产成本难以得到补偿之时，汇率便可能造成问题。均富会计师事务所 (Grant Thornton) 在一份调查中发现，“10 家制造商里超过 4 家 (42%) 称，在过去一年里汇率变动损及自己的业务。”[18] 汇率变动可影响采购决策、设厂地点以及资本投资。

当意外变动导致难以维持品质之时，大宗商品价格波动便造成大破坏。近几年来，能源、金属及农产品价格出现大幅波动。经济合作与发展组织在一份报告中发现，自 2004 年以来，大米成本已增加九倍，小麦成本增加五倍，糖成本增加四倍。[19]

大萧条在全球范围内对众多企业造成严重打击并导致各企业重新关注供应链成本削减。在这种对低成本生产商的依赖增加了由于供应商无法完成紧张交货时间表或质量生产要求而产生的风险。在企业用劣质产品或不合格材料进行替代时，这种行为便威胁到了质量控制措施。

无所不在的技术漏洞

数字技术带来了一系列跟 ICT 供应链相关的具体问题：拒绝服务攻击、刺探机密材料、假冒和恶意替换、重定向系统控制。[20]Davidson 表示：“现代经济是分布式经济，因此我们需要传导需求的有效途径。”加拿大战略关系办公室主任 Carey Frey 指出：“在硬件/软件安全和保安领域尚无管理框架存在”，而且“等产品及系统开发完毕后再就安全要求出台政府政策及处理这一传统事实上的做法”存在问题。[21]

几乎每个国家的企业都会遇到这类漏洞并需要弥补策略。我将在下节中就其对信息及通讯技术造成的风险及问题本质加以描述。在最后一节我将就如何改善 ICT 全球供应链提出建议。

分布式拒绝服务 (DDoS) 攻击

信息系统面临的一个风险是拒绝服务攻击，在这种攻击中大量服务请求同时涌入一个网站并超出其服务器处理负荷。这类攻击会显著拖慢网络并可有效瘫痪网站。

竞争对手可以通过这种做法占用带宽或处理器处理时间、扰乱路由信息，或阻塞用户与服务器间的沟通。这样一来的结果便是阻断网站并使得正常用户无法获取所需服务或信息。对于企业来说，后果可能非常严重。

许多攻击都是针对金融服务公司、电子商务网站或软件即服务型组织展开的。攻击者利用僵尸网络工具包控制互联网中继聊天 (IRC) 信道。这些是为访问互联网提供便利的软件包。通过重复攻击，僵尸网络阻塞了那些通讯工具从而对供应链造成破坏。多份行业报告发现，2012 年的分布式拒绝服务攻击较上一年度增加了 19.2%。[22]

Arbor 网络公司在一份报告中发现，半数企业报称在过去一年中其数据中心受到过分布式拒绝服务攻击。[23] 向云存储的转变已在供应链中增加了新的漏洞，从而创造了一系列新风险。

公私领域的各组织正将越来越多的行政职能放到云平台上。[24] 假以时日，与供应链相关的对任务具有关键重要性的活动很可能也将基于云平台展开。

这些攻击暴露了公司面临的极大风险，同时对基本商业模式形成威胁。参议院情报委员会法律顾问 Clete Johnson 表示："关键问题在于，市场的方方面面并未深入了解如何计算网络安全的成本及收益。"高管们无法评估这种或其他攻击对公司股票价格或财务收入的影响。

移动技术、云计算和自带设备 (BYOD) 的兴起带来了新的威胁，因为许多公司已将供应链管理转移到手持设备（或是平板电脑、智能手机或是非智能手机）或基于云平台的供应商上展开。许多移动设备缺乏基本安全保护。事实上，美国三分之一的智能手机用户报称自己从不设密码保护自己的设备。[25] 而基于云平台展开的服务则将关键基础设施转移到自己公司运营所在地以外区域。

许多移动设备缺乏基本安全保护。事实上，美国三分之一的智能手机用户报称自己从不设密码保护自己的设备。

安全专家称，许多供应商并未因应这些潜在威胁升级自己的安全协议。众多企业及政府并未采纳最优作法，也未实施基本安全保障措施。官员们一方面抱怨称遭到网络攻击、导致数据泄露，但另一方面却不采取必要的自我保护措施。这种情况使得在保护信息技术的同时维持供应链的开放运营颇为困难。

刺探机密信息

对机密信息的刺探是一个古老的问题。在世界进入数字化时代之前，对机密信息刺探的形式是对其他人或组织进行实际监视。由具体的人对其他人进行跟踪并将发现信息向上级汇报。

然而在当代，多数监视都是以电子形式展开来的。比如，侵入者部署窃听设备或安装代码接管网络摄像头并允许其运用音视频实施刺探行为。他们也可以侵入电脑系统并通过间谍软件窃取专有信息。这类程序利用操作系统或网络浏览器中的漏洞以及利用安全漏洞窃取信用卡、金融或对其他组织有价值的产品信息。

"勒索软件"已成为一种较为司空见惯的招式。侵入者利用键盘记录软件、后门病毒以及窃取密码等方式读取专有信息，然后运用这些信息向公司提出不正当支付要求以换取他们不公布这类材料。[26]

近期，美国联邦贸易委员会对数家向客户出租电脑的美国公司提起诉讼，称其有"利用电脑对向其租用电脑的客户进行刺探、对客户机密和个人信息进行抓屏、记录电脑键盘输入以及在某些情况下用网络摄像头对客户房屋拍照"的行为。[27] 通过这种做法，这些公司收集到了金融数据、税标识号、私人邮件、信用卡对账单以及机密密码。

接受采访的福布斯 2000 公司高管中半数表示，他们的公司里设有风险委员会，但大多数公司却并未部署严密程序以应对这类挑战。

尽管存在这些以及其他网络安全威胁，但调查证据显示，许多公司“并未针对网络风险实施关键监管活动，比如审核预算、安全项目评估及顶层政策；就隐私及安全保护设置相应职位及责任；接收关于违规及 IT 风险的定期报告”。[28] 接受采访的福布斯 2000 强公司高管中半数表示，他们的公司里设有风险委员会，但大多数公司却并未设定强有力的程序以应对这类挑战。

假冒产品、盗窃商业秘密以及恶意替换

另一个威胁是以用另一种产品、服务或软件来替代一种产品、服务或软件或是窃取商业秘密的形式出现的。这种威胁可能简单如一般造假。例如，一家公司可能承诺交付 25 个软件包，但只有 18 个是可靠可用的。或者一些公司可能会使用假标签或用质量差些的材料替换针对更高层次市场的产品。[29] 在 1988 年到 2004 年间，商业秘密窃案数量翻了两番，已成为一个严重问题。[30]

据估计，在 ICT 领域仅有 20%的微芯片产自美国。[31] 如果国外公司用劣质电子产品进行替换，则带来了性能问题，从而造成健康及安全风险。对于电子设备、医药产品、玩具以及消费者用品而言，这是一个不争的事实。联合国在一份就从欧洲边界查获的假冒产品报告中指出，57%的假冒产品涉及服装、鞋子及饰品，10%为珠宝及手表，7%为电气设备，6%为药品，4%为 CD 及 DVD，4%为玩具，还有 4%为化妆品。[32]

经合组织在一份报告中估计，全球贸易额的 1.95%涉及假冒或侵权有形商品。该统计并未包括服务或无形产品或内销产品。其他分析则认为该数据在 5-7%之间。[34]

除了简单假冒以外，部分攻击者运用木马程序诱导人们安装恶意软件。卡巴斯基实验室进行的一项分析揭示了这些行为如何通过结合鱼叉式网路钓鱼邮件附件及依赖常见软件程序的后门可执行文件实现侵入及植入恶意代码的目的。[35]

有时侵入者可能会安装键盘输入记录程序来记录键盘录入信息并以电子形式传输给其他人。这样导致的结果便是信息丢失及通讯系统不能执行客户及企业所需要的任务。

随着诸如包裹投递运营商、制造商以及供应商部署“点击支付”设备或库存跟踪装置，近场通讯设备使得窃贼能够利用“手机蠕虫病毒”通过“乱碰感染”(bump and infect) 侵入方式渗入电子设备。[36] 按 Lindquist 的说法，今天最大风险在于“不管在一种产品或服务生命过程的哪一个阶段，系统中都有可能被暗中植入恶意软件”。

重定向系统控制

部分恶意软件会重新定向系统控制并允许组织以外的人员择时控制电脑基本功能。他们运用具有命令-控制功能的软件接管特定活动。他们的代码可以指控电脑进行一些原本设计目的之外的活动，而且通常情况下用户对此毫不知情。[37]

竞争对手可以通过网络浏览器漏洞或安全系统漏洞控制系统功能。许多基于 HTML5 的系统都已解决了如何关闭有风险的插件程序问题。然而，JavaScript 应用程序界面的广泛应用增加了网络漏洞。依赖 JavaScript 应用程序界面的使用者要承受网络被侵入的风险。[38] 不过这些应用及其他有漏洞的软件继续得到广泛运用。

这些类型的大规模攻击要比前文提及的风险更具根本性意义。它们被设计出的目的或是摧毁整个公司或夺取具体关键任务的控制权。在这种情况下，企业面临的挑战在于当关键职能受到威胁时如何保障供应链。

建立信任 12 法

有多个计划正在实施中以应对全球供应链中存在运营及技术漏洞。部分措施专注于企业，因为关键基础设施中的多数都是私有的，而另外部分则致力于将改进政府收购及采购作为传播最优惯例的一个途径。这一切举措将汇聚多个领域的利益攸关者以便就关键事项达成一致。现实需要的是由认识到漏洞普遍性及意识到对行之有据抒缓措施之需的各国及各公司之间的通力协作。

在本节中，我提出了加强对供应链信心的 12 种颇有前景的方法。我列出了可改善商业职能并提高保障度的管理、运营及技术惯例。如果没有这些行动，则全世界的公司将继续承受那些破坏生产、扰乱交货时间表、在硬件、软件及固件中植入恶意软件的种种风险。

建议 1：承认大多数供应链都属企业私有且解决方案的实施依赖于公私双方通力合作这一现实

与开发难以实施且无人真正理解的复杂系统相比，专注于少数几个关键问题领域并打造公私伙伴关系更有意义。

在许多国家里，大多数供应链都由私有公司持有运营。[39] 这为保障商业供应链安全提供了原动力。各国政府应当认识到自己在其中扮演的重要角色，但出台过多标准或制订多如牛毛的规格只能是自毁长城，因为这会让供应商及销售商无所适从。与开发难以实施且无人真正理解的复杂系统相比，专注于少数几个关键问题领域并打造公私伙伴关系更有意义。

上述观点是 EMC 产品安全办公室产品经理 Dan Reddy 在我们研讨会上表达出的。他声称：“行业正与公共领域合作以创设实用的、可衡量的全球标准以解决供应链风险。行业在面对每个地区都出台特别规定的要求做出反弹，这类规定在当今已连为一体的全球经济中不具可扩展性。”然而，如果各国政府及各企业没有加强保护的需要，则就难以确保这个体系的整体安全性。

开放组织信赖技术论坛便是公私合作中颇有前景的一例，该论坛是一个由 400 家企业、政府、学术团体及非营利组织构成的一个非营利团体。

该机构寻求通过“开放、对供应商中立的 IT 标准及认证”实现其目标。其使命陈述中列出四项目标：1）与客户合作以把握、理解及应对已有及新要求，制定政策并分享最优惯例，2）与供应商、联合体及标准化机构合作达成共识并提高互通性、完善及融合规格与开源技术，3）提供一套全面提高联合体运营效率的服务，以及 4）开发运营高品质行业认证服务并提倡采购认证产品。[40]

其标志性计划包括出版《提供商标准快照》。这是为生产或采购现货软件 (COTS) 产品的全球性公司制定的一个标准。该标准向各公司演示了如何在各自组织内部贯彻最优惯例以及在提高 IT 产品保障度方面的各种方法。该标准特别关注假冒产品、被污染物品以及其他类型的“非正宗”资产。开发评估全球供应链的可验证标准是其所有活动的中心议题。

2013 年 4 月，该开放组织就减轻污染物品及假冒产品问题发布了一项提供商标准。该标准“为提高全球供应链安全性向集成商、提供商及部件供应商提出了一系列组织指南、要求及建议”。该标准特别关注现货软件产品。[41]

建议 2：利用标签及跟踪芯片改善度量指标

技术是供应链问题的一部分，但它也可以成为解决方案的一部分。标签与跟踪芯片的应用事实上有助于改善供应链中所有层次上的问题。现在从购买点开始对产品货运及交付进行实时“跟踪与追溯”，从而可以判断在整个产品周期对不同零件质量维护的优劣。

美国国家标准技术研究所在一份报告中表示：“加标签（即序列号）及加标注（即无线射频识别标注）软件包及模块、硬件设备、个体成份及围绕这一切进行的处理流程均可以用于实现这一目的。”[42]

各公司可以对绩效进行监督并要求供应商就每一个序列号提供季度报告、同时查明每一个部件的全部过往经历。供应商可保存关于有多少零件被报废及其报废方式方面的纪录。在我们的研讨会上，思科全球供应链首席安全战略官 Edna Conway 强调指出：“这一切全关乎在适当时间在供应链适当节点上部署适当安全技术、物理安全举措及逻辑安全流程。与此同时，在打造供应链端对端安全解决方案时我们需要与供应商全力合作。在任何我们希望取得成功安全解决方案的设计与实施过程中，我们的供应链合作伙伴必须全程参与。”

建议 3：部署身份认证系统

单点登录及个人身份认证系统的实施改善了供应链中的责任心。美国国家标准技术研究所正在开发一套融计划、生产及调度为一体的“生产与运营管理”系统。研究人员利用“虚拟、分布式、供应链整合试验平台”整合起一个供应链平台，通过该平台验证身份、运用应用软件及创设情景模拟来监控规范执行情况、测试在保障供应链过程中对既定规格及管理策略的坚持。[43] 在个人在登入登出过程中对访问进行控制有助于树立对供应链安全性的信心。

风险度量标准的缺位使得当前许多解决措施复杂化。在缺乏明确数据支持的情况下难以弄明白问题的严重性。全球供应链涉及多个国家、大量供应商及复杂的运营性物流。对供应链的多个环节我们都缺乏数据，因此就难以对风险、降低风险措施或对规范的遵守情况加以评估。一种可以在供应链终端开发的度量标准便是分析查找软件中的漏洞及未经授权插入的代码。

比如说，在造假领域里，问题的严重性难以估量。几乎没有关于非法产品替代真品的直接指标可以使用，大多数研究都依赖于传闻逸事类证据、消费者调查或执法部门的查获纪录。已有的多项研究均依赖于个别国家或个别行业。[44] 制定更优秀度量标准及识别系统将有助于各公司识别问题并制定出可能的解决方案。

建议 4：依赖于独立评估

许多观察人士认为，各国家或公司的供应链问题具有独特性。但 EWA 公司首席技术官 Steven Clemmons 对此观点不以为然。他说："没有一家供应商有多少可信度。比如，任何一家大型供应商都可能有中国制造或软件设计或开发方面的印记。"从苹果与思科这类公司到大多数电信企业均依赖设在中国境内的生产设施。而许多中国公司又从美国公司里采购部件。

Veracode 在 2012 年一份《软件安全状况报告》表示，"来自第三方或外部开发软件的安全风险"与日俱增。

该公司研究副总裁 Chris Eng 评论说："一家典型企业平均有 600 种任务关键型应用，约 65% 是由外部公司开发的，这使得公司在这些应用程序出现安全风险时日益容易受到伤害。"[45] 尽管存在这种种漏洞，但大多数公司在部署产品时仍然甚少加以测试或验证，即便公司在高风险领域内运营的公司亦是如此。

不论是产自哪国的产品，所有产品均需要实施的一个步骤是对其底层软硬件进行评估。如果在有更安全方法存在的情况下而各国政府或各公司却仍然选择低验证模式，这种做法通常是为了节省资金，但他们却是在知情的情况下将自己置于更大险地。他们因此就要为因他们自身的短视而招致的侵入负责。实验室需要分析源代码以识别常规测试方法所无法检测出来的恶意软件及漏洞。Clemmons 称，须对硬件及固件进行评估以检查"交付了何种功能"并确保不存在"硬件后门及其他漏洞"。

有些方法是对所有已部署软件实施完整、独立的验证，排除供应商或第三方部署未列入文献及未经评估的变更的一切机会。就硬件而言，要确保经过初始评估后不存在未列入文献及未经评估的变更，则这些方法就需要对统计上具有显著意义的大量随机样本的线路板进行独立、全面验证。然后可由可信赖的第三方工程服务提供商进行部署，而不是由供应商部署。这些流程是一种当前被称作可信赖交付系统的部件。Clemmons 辩称，当评估结果"上升到证据层面而不仅仅是某个聪明人的观点之时"，信任度便得到提升。

> *如果在有更安全方法存在的情况下而各国政府或各公司却选择低验证模式，这么做通常是为了节省资金，那么他们便是在知情的情况下将自己置于更大险地。他们因此就要为因他们自身的短视而招致的侵入负责。*

建议 5：开发集成管理工具

许多公司缺乏监控自己供应链或评估网络风险的评估工具。马里兰大学 Robert H. Smith 商学院在对 290 家小型 IT 供应商进行的研究中发现，"47.6%的样本从来不使用风险委员会或其他管理机制管理企业；（另有）46.1%的企业从来不用集成供应链仪表板/控制。"[46]

因此，马里兰大学的研究人员建议公司开发集成管理工具并使用基准度量标准对性能进行跟踪。他们的电信管理论坛 (TM Forum) 呼吁“对安全进行可度量化处理：就关键性能指标进行界定、签约并加以实施以防止供应链中出现端对端威胁”。[47]

据美国国家标准技术研究所计算机科学部高级顾问 Jon Boyens 的说法，部分计划与公司治理政策反其道而行之，“过于不合群”且只专注于内部运营及上游供应商而不顾及下游消费者。此外，具体硬件与软件供应链的作法各异，都不可避免地受各自所在领域的独特属性所制约。在制定全面 ICT 供应链风险管理指南时，这种情况会造成一些困难并常常产生一些极其严格的标准及做法，从而导致难以为加强保障而进行有意义的确认与验证。

许多组织从与其他组织的比较中获益匪浅。进行基准比较是将优秀供应链惯例付诸产品开发的一个优秀途径，正如在供应链终端对类似产品进行性能优劣比较一样。如果要公司评估其质量性能，则它们就需要得到激励以便尽一切可能做好工作。行业与政府间必须有协调举措以确保这些条件不会成为组织的沉重负担。

一个值得关注的举措便是信息安全论坛，这是由财富 500 强及福布斯 2000 强中的龙头公司组成的非营利组织。其成员通过开发满足我们成员所需的惯例准则、流程及解决方案来“致力于调查、澄清并解决关键信息安全风险管理事项。信息安全论坛汇编研究、撰写简报、为各公司及商业领域实施基准比较研究。其“基准即服务”在线工具使得各公司得以评估各自安全惯例、对比基准进行结果比较以及与全球各地公司进行比较。[48]

国防部已通过设立供应链风险管理威胁评估中心着手向这个方向努力。该中心协助各公司评估威胁并共享最佳惯例。按国防部官员 Davidson 的说法，其因应用而各异的集成电路设计用于在制造、应用、检测及评估过程中提高漏洞检测效率并补救技术风险。

国防部是旨在改进供应链做法并打击假冒产品的政府间协作供应链组织的一个成员单位。作为《美国国防授权法》的一部分，国防部需要实施一项勾勒供应链风险的并提出具体应对这些威胁解决方案的研究。在一份定于 2013 年秋天发布的关于标准报告中，国防承包商被要求承担起保障产品质量的责任。除了其他责任外，承包商们须对产品进行检测并避免假冒产品，一旦查到有假冒产品则要采取改正措施，同时还制定在国防部产品中使用可信赖供应商的程序。

通信业卓越质量论坛 (QuEST Forum) 代表着全球范围内“致力于提高运营及供应链质量与性能”的 ICT 服务提供商和供应商。其首要任务包括提倡将 TL9000 作为全球质量管理标准、共享最佳行业惯例、行业性能基准比较及提供新产品与服务。其成员包括来自美国、欧洲、亚洲及拉美的服务提供商。

美国方面的举措便是成立了美国跨部门供应链工作组。[49] 除了其他部门外，该工作组由来自国土安全部、国防部、国家安全局以及美国国家标准技术研究所的代表组成。工作组寻求对联邦政府全球供应链政策进行协调，不过相对于网络安全而言，该组更重视实体供应链安全。工作组尤其对联邦采购中的供应链风险管理及在政府收购中全方位确保产品安全感兴趣。[50]

建议 6：加强信息共享

一个挑战是在一个竞争性市场及存在诉讼风险的环境中难以共享信息。公司有时不愿共享其专有数据，担心这会招致法律诉讼或法律责任。[51] 他们担心共享数据会置他们于不利竞争地位或使他们面临数据泄露或被假冒的风险。

负责企业与行业中心是一家非营利组织，“通过与跨国企业合作激励创新与促进经济繁荣，保护知识产权、打击腐败并在全球供应链推行负责任业务惯例及商业网络”。其宗旨在于通过在线评估、实施培训项目及推行独立评估以改善供应链惯例。该中心已开发出用于知识产权保护及防腐败活动的先进惯例。[52]

在对供应链面临挑战所进行的回顾中，该中心提议各公司“加强信息共享以强化供应链的完整性”，以及“制定包括促进并改善监管的供应商合同方面的规定”。[53]

英国当局已就网络安全推出了一项创新性国际合作项目。通过与美国国土安全部及国安局、澳大利亚国防通讯处及自身的网络安全评估中心合作，澳大利亚政府各部门共享关于威胁及补救措施方面的信息。每一组织均已对各自程序进行合理化处理以降低网络安全风险。

美国政府问责局 (GAO) 呼吁制定以结果为重心的度量标准以衡量对通讯网络保护的有效性。在其对国土安全部网络安全活动的审核中，美国政府问责局表示，联邦部门及其私人领域合作伙伴需要“共享关于运营中断及事故的信息”。这将改善网络同时帮助各组织管理其 ICT 供应链。[54]

建议 7：软件保护

信息与通讯技术是供应链中的一个特别问题。为协助应对该领域面临的挑战，诸软件公司已设计出一种旨在“对软件开发流程每一个步骤中制定严密保障惯例的”SAFECode 流程。[55] 为树立对产品及服务能够正常运行且不含病毒并能以所宣称的方式运作的信心，许多公司自愿在在制定评估标准中展开协作。这便是在设计过程不同阶段运用透明最佳惯例法中的一例。

另外一种方法由独立软件顾问 Pravir Chandra 所创，即，作为开放网络应用程序安全项目一部分的开放软件安全成熟度模型，该方法提供度量安全、评估现有产品及生成软件安全记分卡的工具。该团队向外提供帮助各公司实施优秀安全惯例的审核人员及评估人员。

建立安全成熟度模型利用取自 51 个主导性软件安全计划的数据来测量软件安全。这一项目拥有从不同公司抽调来的 134 位成员，项目可以通过创意公用授权条款获取安全产品。这些人每年都私下里举行一次会议共享全行业最佳惯例。

软件标识代表着打造安全流程的另一种途径。可以在产品中安装一个记录每一种应用程序名称、版本以及使用情况的软件身份 (SWID) 标签。这样一来，各公司便可以跟踪库存状态并管理各自供应链。这是一种通过数字资产提高透明度及强化问责机制、用技术加强安全的一种途径。

微软 Windows 8 软件中有一项旨在防止对固件进行更改的“安全启动”技术。该功能旨在阻止启动过程中恶意软件感染电脑软件。通过提高用户对自己软件中不会存在可能在生产或

配送过程中加进去的恶意功能的信心，这一方法解决了供应链中的一个重大风险。

建议 8：制定标准提高性能

对议定标准的开发是另一个非常有前景的领域。[56] 美国国家标准技术研究所一直专注于组织、使命及运营层面标准的开发。据 Boyens 的说法，由于联邦政府是商品与服务的一个大买家，该研究所希望改善联邦采购状况。其希望在于，在该领域取得的改进将会传导至生产与交付系统的其他环节。

为鼓励供应商自愿采纳供应链标准及用户与客户间进行系统整合，美国国家标准技术研究所与白宫计划在未来共同制定一套网络安全框架。由于遭到美国多个行业集团的反对，联邦政府未采纳欧盟青睐的强制性要求。这意味着部分公司将采纳自愿性标准，而其他公司则不采纳该标准。这将使得黑客及侵入者可以利用的安全系统漏洞长久存在下去。

美国国家标准技术研究所已接到要求，要在未来八个月里开发集成管理系统及供应链保障标准求。该研究所于 2013 年 4 月 3 日召集了首次公开研讨会，就本框架征集反馈意见。这类工具将协助各公司管理风险、应对运营挑战并补救供应链中的漏洞。尽管该标准将在本质上是自愿型的，但却将指引联邦政府的采购活动。希望在于，这些指南将在整个商业领域推广开来。

电信工业解决方案联盟 (ATIS) 将全球众多顶级技术公司汇聚起来解决头等商业大事。其网络安全组计划“制定能够创造信息与通讯技术业未来的标准与解决方案”。该组织代表着 166 家不同的公司，并通过委员会及论坛形式展开工作，而且是国际电信联盟及美洲电信委员会的主要贡献者。其首要事件包括基于 IP 部署的基础设施、融合多媒体方案（包括 IPTV）、强化运营与商业支持系统以及提高服务质量与性能该组织是美国标准协会的一个成员。[57]

国际自动机工程师学会有 128,000 名专注于为航天、汽车及航空业撰写标准的工程师及技术专家。他们强调硬件的生产并致力于推广优秀生产惯例。

在制定正式标准中须谨慎对待的一件大事便是，标准要与应对的威胁同步发展。按 Clemmons 的说法，有时候标准的制定与接受过程“过于漫长而现实威胁的进化又过于迅猛”。

国际标准化组织利用由来自商业提供商的专家技术委员制定标准。该组织在过去数十年间已在诸如质量管理及风险管理领域中制定出 19,500 项标准。来自不同国家的参与者已就更改控制、逻辑访问控制、物理访问控制制定出众多标准。这包括多种机制，包括判断什么人出入设施、出入时间、验证访问、控制访问、取得钥匙、检测物理篡改及维持诸如保安、警铃与监控等安全措施。[58] 这使得各公司在改进供应链安全并树立对全球贸易的信任中有一种统一方法。

英国通过其网络安全评估中心及国家信息保障技术局提高安全标准。该中心服务于中央政府

各部门、英国卫生署及其关键国家基础设施。除了其他职能外，该机构制定专注于库存控制、标识加注、管理控制、访问控制、注册及数字签名领域标准的制定。希望得到认证的公司可通过该中心网站提交各自产品取得许可。该中心积极参与公共领域安全的管理。中心专注于将标准作为保障产品质量的一个途径加以推广，同时确保主要政府部门遵守这些标准。中心同时出台严格规则，限制被认为会造成真实或潜在漏洞的存储设备的使用。比如，为保护信息系统，英国要求政府官员在使用记忆棒时要进行加密处理。[59]

在制定正式标准中须谨慎对待的一件大事便是，标准要与应对的威胁同步发展。按 Clemmons 的说法，有时候标准的制定与接受过程“过于漫长而现实威胁的进化又过于迅猛”。我们需要具有充分灵活性、能够与日新月异的威胁及其他挑战保持同步发展的标准。

建议 9：认证具有光明前景的程序与流程

认证是为公司树立对供应链的信心一大途径。运用统一质量保障程序就有可能提高对整体系统的信心。

信息技术安全性评估通用准则认证项目便是其中一例。组内成员已制定取得安全评估认证所必须的 IT 质量控制标准及程序。[60] 需要审核的项目包括“员工身份、对产品资产访问的控制、安全开发流程、开发与配送中的完整性控制以及反假冒措施”。[61] 美国、英国、澳大利亚、新西兰、土耳其、日本、法国、加拿大、韩国、德国、意大利、马来西亚、荷兰、挪威、西班牙以及瑞典等国均已签署这些协议。不过，诸如美国众议院常设特别情报委员会等观察机构对这一做法提出批评，指其不够充分且声称该做法并未取得理想结果。

美国联邦风险与授权计划是政府采购流程中的另外一例。各公司可以就特别产品取得通行于全部联邦政府机构的认证。这是评估软件解决方案并为产品打开通往美国联邦政府各部门之门的一个途径。此前，每一个政府部门均对各自所需产品进行独立认证，而且也没办法保证在一个政府部门得到认证的产品同时能得到另一个部门的认证。

英国网络安全评估中心已宣布推出一个对 IT 专业人士进行认证的项目。该项目旨在提升“在英国境内应对网络安全风险的能力”。[62] 项目报名者接受三个层次的认证：从业者、高级从业者及主导从业者，项目涵盖诸如安全官、审计员、风险顾问与架构师以其他人员。

加拿大要求“承包商不得在加拿大网络或与加拿大网络互连的自有网络或第三方网络基础设施上部署任何设备，除非该设备已经得到经加拿大批准的公认认证机构的外部评估”。[63] 加拿大还强制要求政府数据必须存放于设于该国境内的设备上。

对于某些公司来说，这些标准的重要性要远高于第三方评估。Davidson 表示：“进行自我评估成本更低廉。”按他的观点，各组织应当按照议定标准对生产商进行审计。

建议 10：鉴定表现优异者

一些人建议把鉴定作为打造保障控制的一种途径。该途径允许第三方评估机构把达到某些标准而被鉴定为表现优异的公司进行认证。鉴定可基于是否达到议定标准进行，但关键在于对

鉴定范围及本质的描述。按 Conway 的建议，“关键在于明确界定具有代表性的流程、产品及惯例，正是这些使得供应链安全认证才对潜在技术采购者有意义。”

开放组可信技术论坛正在制定一项标准及相关可信赖鉴定流程以协助保障全球供应链安全。在完成制定一系列最佳惯例后，该论坛允许各公司提交信息证明是否达到这些运营标准。鉴定有效期为三年，期满后各公司可以申请重新鉴定。

雷迪指出，鉴定流程是基于组织而不是基于产品实施的。审核者对组织流程及质量管理进行检查以确定申请者是否在质量保障方面超过合理临界值。这便跟对特定产品进行认证区别开来。

重要的是要保持认证与鉴定与时俱进。Lindquist 评论说：“大多数认证与鉴定都只是进行认证审计时的环境静态视图。”某些技术的半生命周期或许就是半年到一年，这使得这种审计不合时宜。

建议 11：实施审计找出特殊问题

表现审计允许外部组织在进行现场检查时或对表现及质量保障进行审核时介入。Conway 声称：“实施区区数个国际标准便是提高全行业安全之路。”她指出，“尽管各原始设备制造商有审计、现场检查及整合进供应商表现度量标准中的安全举措，但对此类标准的认证或鉴定需要由经公认的审计员及国际认证实验室实施。”

部分公司把产品评估作为一种审计形式。他们把定期审计产品作为确保其质量及可靠性的一种方式。他们对装运的产品进行抽样复查以判断产品是否达到广告性能并满足议定标准。美国华为首席安全官 Andy Purdy 表示：“鉴于当前的威胁态势，为确保产品得到评估，业界需要制定并实施行业性标准及最优惯例——从生产结束到交货到安装再到安装后保养与更新——以防止出现漏洞或恶意功能项。”

现在许多审计员都专注于特定产品，但重要的是增加合格检查人员的数量。Johnson 指出，“当今社会没有谁是全能人才。”“我们需要一个专家社区。”得到业界认同、合适专家的匮乏加剧了在供应链内进行基准比较及审计的复杂性。

建议 12：区分低、中及高风险问题并设计应对不同层次威胁的适当补救措施

传统风险管理理念认为，并不是所有威胁都是同等程度的漏洞。有些威胁有高风险因而需要有比应对其他威胁更强有力的补救措施。比如说，美国国家标准技术研究所区分了低、中及高风险领域，并建议在应对从低到高风险的产品时相应提高补救措施层次。

从其立场看，企业需要对供应商组织的数个方面进行调查并设立相关保障措施。这包括诸如公司历史生产流程的稳健性、外部影响、可被利用的漏洞、供应链薄弱环节及整体过往成就等特征。[64] 为改善供应链，该机构呼吁制定基于更严厉联邦采购规则的“多方面、任务驱动

型”风险评估法、采纳国际标准、加强数据共享并运用技术及在线工具跟踪供应链惯例。[65]

结论

总而言之，我认为，ICT 全球供应链中的问题不局限于任何一地，而是普遍存在于全球商业中的共同特征。漫长的供应链、产品评估不力以及许多拟议补救措施的自愿实施性质都削弱了我们解决普遍威胁的能力。在应对运营性及技术性威胁时，我们需要更具可持续性、整合度更高、更全面的方法。为保障供应链安全，我们必须改进标准并加强第三方评估。

在全球供应链许多环节上显然存在众多问题与漏洞。由于公司与政府部门日益依赖商业现货产品，确保软件、硬件及运营达到安全标准已成为一件非常棘手的事。要树立对于整个系统至关重要的信赖感，各公司必须就哪些产品可靠、安全共享信息。必须提高下列各方面的确定性，相互竞争产品间的相对保障性及安全以及在供应链是否加入恶意软件或硬件，或产品中是否包括可被利用的漏洞。

接近十几家美国商业协会称，挑出几个国家并加以惩罚性措施的结果只会适得其反。许多美国技术公司依赖于在中国制造或组装的部件。声称政府部门不应当依赖于中国产品的说法便是对供应链中每一个点上处处存在的风险视而不见。美国商会、电信工业协会、美国科技、以及商业软件联盟/软件联盟恰如其分地指出：“产品安全是一种产品制造、使用及维护方式的函数，而不是由谁或在何处制造的函数。”[66]

在近期，美国通过立法对联邦部门从中国技术公司采购产品设限后，奥巴马政府抱怨称，这种限制“可能会被证明为具有极大破坏性却无法显著加强所涉部门的网络安全”。[67]

我们需要构思出打造可信赖网络及对当前举措如何实现重要目标加以评估的方法。本报告所展示的想法勾勒出了一系列通过实施最优惯例、独立评估、议定标准、认证、鉴定与对供应链惯例进行审计以消弥风险的运营及技术计划。

每一项活动的目标均在于，开发可信赖网络及第三方验证机构以改善供应链运营质量与提高产品及网络保障水平。业界需要具有合理透明度、问责机制及互动性的可信赖交货系统，因此供应商们才可以对远在天边的合作伙伴感到放心。如果没有这种信任，则就难以维持分布在全球各地的漫长供应链的消费品、药品、国防器材、食品、汽车或技术等领域产品的质量。[68]

但不管制定何种标准、认证或鉴定都必须是动态的。国际贸易规则及通用电气顾问 Sandy Merber 表示，“我们希望确保这种认证程序不会成为问题的一部分。这是一个极具活力的领域。系统必须与时俱进。”

尾注

注意：*我谨在此向 Elizabeth Valentini 对本论文的宝贵研究协助表示感谢。*

1. Gregory Wilshusen, “IT Supply Chain: National Security-Related Agencies Need to Better Address Risks.” Government Accountability Office, March, 2012, p. 5.

2. Symantec, “Intelligence Report,” December, 2012, p. 7.

3. Georgia Institute of Technology, “Emerging Cyber Threats Report,” 2013, pp. 4-5 and Georgia Institute of Technology, “Consensus Cyber Security Controls,” March 6, 2013.

4. Tech America, CIO Survey, 2012, p. 4.

5. World Economic Forum, “New Models for Addressing Supply Chain and Transport Risk,” 2012, p.4.

6. World Economic Forum, “New Models for Addressing Supply Chain and Transport Risk,” 2012, p. 7.

7. Fujita Masahisa and Hamaguchi Nouaki, “Japan and Economic Integration in East Asia: Post-Disaster Scenario,” RIETI Discussion Paper Series 11-E-079, December, 2011.

8. Hidetaka Yoneyama, “The Lessons of the Great Tohoku Earthquake and Its Effects on Japan’s Economy,” *Fujitsu Research Institute*, April 8, 2011.

9. Simeon Ang, “Thailand Floods Disrupt Supply Chains & Raise Inflationary Risks,” Shares Investment, November 4, 2011 and Thomas Fuller, “Thailand Flooding Cripples Hard-Drive Suppliers,” *New York Times*, November 6, 2011.

10. Fang Zhang, “Thai Floods Continue to Impact Hard Drive Manufacturing,” Applied Market Intelligence, February 12, 2012.

11. Adam Nossiter, “Chad Says It Killed Algeria Hostage Crisis Mastermind,” *New York Times*, March 3, 2013, p. 4.

12. United Nations Global Compact, “Fighting Corruption in the Supply Chain,” June, 2010.

13. Mehmet Ugur and Nandini Dasgupta, “Evidence on the Economic Growth Impacts of Corruption in Low-Income Countries and Beyond,” London: EPPI-Centre, Social Science Research Unit, Institute of Education, University of London, 2011, p. 2.

14. United Kingdom Department for Business Innovation & Skills, “Protectionism: Trade and Investment Analytical Papers,” 2011.

15. Scott Charney and Eric Werner, “Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust,” Microsoft Corporation paper, July 26, 2011, pp. 6-8.

16. United Kingdom Department for Business Innovation & Skills, “Protectionism: Trade and Investment Analytical Papers,” 2011, p. 4.

17. World Trade Organization, “Report on G-20 Trade Measures,” May 31, 2012.

18. Grant Thornton, “Supply Chain Solutions,” *World Trade Magazine*, 2010.

19. Organization for Economic Cooperation and Development, “Competition and Commodity Price Volatility,” 2012, p. 23.

20. Edna Conway comments at Brookings Institution Supply Chain Workshop, February 4, 2013.

21. Carey Frey, “Cyber and Supply Threats to the GC,” Communications Security Establishment Canada, June 12, 2012, p. 29.

22. Prolexic, “Quarterly Global DDoS Attack Report,” Q4, 2012, p. 2.

23. Arbor Networks, “Worldwide Infrastructure Security Report,” 2012, Volume VIII, p. 7.

24. Paul Wormeli, “Mitigating Risks in the Application of Cloud Computing in Law Enforcement,” IBM Center for the Business of Government, 2012.

25. *Time*, “How Has Wireless Technology Changed How You Live Your Life?,” August 27, 2012, pp. 34-39. This Time Mobility Poll was undertaken in cooperation with Qualcomm between June 29 and July 28, 2012.

26. McAfee, “2013 Threats Predictions,” 2013, p. 5.

27. Federal Trade Commission, “FTC Halts Computer Spying,” September 25, 2012.

28. Jody Westby, “Governance of Enterprise Security,” CyLab Report, 2012, p. 5.

29. CREATe, “Health and Safety Risks From Counterfeits in the Supply Chain,” October, 2012, p. 8.

30. CREATe, “Trade Secret Theft: Managing the Growing Threat in Supply Chains,” 2011, p. 6.

31. Jason Miller, “Agencies, Vendors Ramping Up To Fight Supply Chain Cyber Threats,” *DoD News*, June 15, 2012.

32. United Nations Office on Drugs and Crime, “The Globalization of Crime,” undated, p. 178.

33. OECD, “Magnitude of Counterfeiting and Piracy of Tangible Products,” November, 2009, p. 1.

34. United Nations Office on Drugs and Crime, “The Globalization of Crime,” undated, p. 173.

35. Kaspersky Lab, “‘Red October’ Diplomatic Cyber Attacks Investigation,” 2013.

36. McAfee, “2013 Threats Predictions,” 2013, p. 4.

37. Scott Charney and Eric Werner, “Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain,” Microsoft Corporation paper, 2012.

38. McAfee, “2013 Threats Predictions,” 2013, p. 10.

39. Telecommunications Industry Association, “Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain,” 2012, p. 2.

40. Drawn from the About Us section of the Open Group website at http://www3.opengroup.org/aboutus.

41. The Open Group, “Open Trusted Technology Provider Standard Version 1.0.” April, 2013.

42. Jon Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, and Stephanie Shankles, “Notional Supply Chain Risk Management Practices for Federal Information Systems,” National Institute of Standards and Technology, NISTIR 7622, October, 2012, p. 28.

43. Shigeki Umeda and Albert Jones, “Virtual Supply Chain Management: A Re-Engineering Approach Using Discrete Event Simulation,” undated, p. 8.

44. Stijn Hoorens, Priscillia Hunt, Alessandro Malchiodi, Rosalie Liccardo Pacula, Srikanth Kadiyala, Lila Rabinovich, and Barrie Irving, “Measuring IPR Infringements in the Internal Market,” Rand Europe, 2012.

45. Veracode, “Enterprise Testing the Software Supply Chain,” November 12, 2012.

46. University of Maryland Robert H. Smith Business School, “Assessing SCRM Capabilities and Perspectives of the IT Vendor Community,” 2012, p. 88.

47. TM Forum, “Securing the Cyber Supply Chain,” Morristown, New Jersey, 2013, p. 19.

48. Taken from its website at http://www.securityforum.org.

49. White House, “National Strategy for Global Supply Chain Security,” January, 2012.

50. National Institute of Standards and Technology, “Supply Chain Risk Management for Information and Communications Technology,” January 7, 2013.

51. Jarrellann Filsinger, Barbara Fast, Daniel Wolf, James Payne, and Mary Anderson, “Supply Chain Risk Management Awareness,” Armed Forces Communication and Electronics Association Cyber Committee, February, 2012, p. 6.

52. Material drawn from its website at www.create.org.

53. CREATe, “Health and Safety Risks From Counterfeits in the Supply Chain,” October, 2012, pp. 17-19.

54. Government Accountability Office, “Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts,” April, 2013, p. 31.

55. Software Assurance Forum for Excellence in Code, “Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain,” June 14, 2010.

56. John Suffolk, “Cyber Security Perspectives,” Huawei paper, 2012, p. 19.

57. Summarized from its website at www.atis.org.

58. Tyson Storch, “Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity,” Microsoft Corporation paper, July 26, 2011, pp. 7-9.

59. Chris Mayers, “Information Assurance as a Flexible Security Solution,” Info Security, January 19, 2012.

60. Common Criteria, “Common Criteria for Information Technology Security Evaluation,” September, 2012, Version 3.1, Revision 4.

61. Scott Charney and Eric Werner, “Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust,” Microsoft Corporation paper, July 26, 2011, p. 12.

62. The Chartered Institute for IT, “BCS Certify Information Assurance Professionals for Government Departments Including CESG,” October 9, 2012.

63. Communications Security Establishment Canada, “Technology Supply Chain Guidelines,” October, 2010, p. 11.

64. Jon Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, and Stephanie Shankles, “Notional Supply Chain Risk Management Practices for Federal Information Systems,” National Institute of Standards and Technology, NISTIR 7622, October, 2012, p. 20.

65. Jon Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, and Stephanie Shankles, “Notional Supply Chain Risk Management Practices for Federal Information Systems,” National Institute of Standards and Technology, NISTIR 7622, October, 2012, p. 1.

66. Brendan Sasso, “US Industry Rallies Against Ban on Chinese Tech Products,” Hillicon Valley, April 4, 2013 and April 4, 2013 letter signed by 11 major U.S. industry groups.

67. Brendan Sasso, “White House Criticizes Ban on Technology Products From China,” *The Hill*, April 5, 2013.

68. Scott Charney and Eric Werner, “Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust,” Microsoft Corporation paper, July 26, 2011, pp. 8-9.

Governance Studies

The Brookings Institution

1775 Massachusetts Ave., NW Washington, DC 20036

电话：202.797.6090

传真：202.797.6144

www.brookings.edu/governance.aspx

编辑

Beth Stone

Donna Ra'anan-Lerner

制作和排版

Beth Stone

欢迎您将您的意见发送至 gscomments@brookings.edu