# 网络安全透视

## 21世纪的技术和安全
## — 一场艰难的联姻

**约翰·萨福克**
高级副总裁 | 全球网络安全官
华为技术有限公司

HUAWEI

# 目录


1 前言 ..... 1

2 执行概要 ..... 2

3 通信与我们的21世纪社会 ..... 4

3.1 日益增长的网络安全挑战 ..... 5

3.2 终端、数据和事件 ..... 7

3.3 识别参与者 ..... 8

3.4 理解全球供应链的影响 ..... 9

3.5 数字世界的法律 ..... 11

4 华为的方法 ..... 12

4.1 网络安全是公司的全球政策 ..... 12

4.2 从内部构筑安全——“嵌入” 而不是“附加” ..... 14

5 管理全球安全难题——这需要共同合作 ..... 18

6 共同前进 ..... 19

7 关于华为 ..... 20


2012年9月

# 1 前言

本文件公开坦诚地阐述了华为对于以下问题的观点：网络安全以及其对技术、社会和我们日常生活带来的后果和影响。

在本文件中，我们结合历史背景从总体上阐述了网络安全的现状、参与者以及空前扩展的全球供应链给我们大家带来的独特挑战。

文件还概述了华为的网络安全方法和全球供应链的挑战，并就全行业如何积极务实地解决这些担忧提出了一些建议。毫无疑问，我们需要在全行业的公共和私有部门之间持续增强透明，更加团结合作，主动管理网络安全并降低全球供应链风险。

作为一个全球性的公司，华为致力于与各利益相关方密切合作、持续创新、共建标准，确保我们提供的网络解决方案和服务的完整性和安全性能够满足或超越我们客户的需求，并为他们的客户提供必要的保障信心。本文件是为了促进全行业对我们的了解而采取的一个举措，促进行业了解我们在全球范围内为确保我们大家将来有一个安全和更好的网络而做出的努力，并就企业和政府在管理全球网络安全风险方面需要采取的行动提出自己的意见。

# 2 执行概要

我们所处的世界已经变得真正相互连接。

过去的二十年间，我们见证了商业互联网的蓬勃发展，为一个相互连接的全球数字网络播下了种子，使得从电子邮件到远程医疗、网站浏览、社交网站、网上银行和零售等服务无处不在且让人们能负担得起。

网络空间是不同于我们习以为常的地理空间的新的战略领域，已逐步成为社会运转的“神经系统”。各国现在都高度重视网络空间技术的发展。网络的发展有助于促进社会进步。网络的开放促进信息流动和分享，带来更多创新机会，降低创新成本，促进了世界的健康、富裕和繁荣。

网络技术是伟大的创新。网络的开放使信息获取和分享更加便捷，并为人类带来了大量创新机会。随着技术的普及，创新的成本也降低了。这就意味着，消费者、中小型和微型企业有机会跟大企业在同一个平台上展开创新。

互联网的发展带动了投资，创造了新的消费模式。这些新的消费模式推动了全球经济发展，驱动了全球经济。网络的开放使世界相互连接，促进了不同区域的经济交流和全球化贸易的便利。信息技术已经成为经济增长的重要引擎。世界银行的报告显示，发展中国家的宽带普及率每提高10%，GDP将增长1.38%。[1]

随着数据以及技术使用的大量增长，我们要用正确积极的态度面对信息的增长，不要一味视之为洪水猛兽。我们必须利用信息去消除数字鸿沟，让更多的人接入通信和信息系统，更好地实现信息资源的分配。这样地球上人人都可以从使用技术中获益。网络的开放有助于保障人们平等地接触信息，促进社会公平，平衡区域发展。网络的开放促进了文化交流，有助于不同文化背景的人们消除误解和歧视，减少文明冲突。

然而，虽然我们看到了数字和宽带革命对个人、社会和企业带来的里程碑式的利益，现实社会中一些由来已久的罪恶，如：故意破坏、盗窃、扰乱、间谍活动和肆意毁坏等行为，已经自然地延伸到了新的数字环境。

华为是一个全球性的公司，业务延伸到140多个国家，连接世界三分之一的人口。作为这样一家公司，华为积极正面地应对这些挑战。作为全球领先的ICT解决方案提供商之一，华为从技术方面能深刻地理解网络如何运行，以及技术如何从根本上支撑和促进全球公民的健康、富裕、安全和成功。

[1] http://www.broadbandcommission.org/Reports/Report_2_Executive_Summary.pdf

但是，我们没有一天不耳闻目睹政治上煽动或竞争对手煽动的一些网络安全负面评论。虽然对网络安全破坏的担心是可以理解的，但是这样一些言辞可能会让我们不聚焦于行业所面临的各种挑战。要形成一个有效的全球以及全行业的解决方案需要进行冷静且实事求是的对话，而不是基于商业竞争或政治斗争。

当今世界，全球有超过87%的人口是移动用户，苹果应用商店的下载已经超过了250亿，Google Play应用商店下载量也超过了200亿次。现实是，网络安全已经成为一个日益增长的全球挑战，需要理性的全球解决方案。[2、3、4]

技术不再是仅在一个国家设计、开发和部署；任何国家或大型企业再也不能说他们只依赖一个采购模式；如今技术生态系统和架构很复杂，我们再也不能说我们能阻止来自所有威胁方的所有威胁。

政府、企业和消费者都越来越依赖ICT解决方案。这些解决方案集成了由世界各地多个供应商设计、开发、编程和制造的产品。因此，网络安全挑战的规模也成倍增长。

网络安全并不是某个国家或公司的问题。所有的利益相关方——政府和行业——都必须意识到网络安全是全球共同面临的问题，需要我们采取基于风险的方法以及最佳实践，并进行国际合作去应对这个挑战。

最近公布了一些威胁，如Stuxnet和Flame等。随着这些威胁的公布，世界已经到达了这样一个决策点：我们要不要沿着现有道路前行？在这条道路上，任何误入歧途的行为人，无论出于什么动机，都能在这个没有管制的世界中进行任意操作，为任何目的开发恶意软件。如果我们接受这条道路的话，我们就必须停止抱怨，而且要接受这样的后果：网络会驰入一个深渊，西部荒漠将会卷土重来。或者正如我们面临其他形式的冲突时那样，我们应该集体从悬崖边上退回来，建立法律、规范、标准和协议——接受事实：信任是需要建立并持续验证的，而现在谈到网络安全，各利益相关方之间缺乏信任。在这种形势下，我们必须要实际和坚定。

本白皮书赞同并支持将国际合作、开放和可验证的信任作为这个世界的基础：对全球70亿人口中的大部分人来说，技术能够持续促进经济和社会发展。

我们希望你们也能支持这个选择。

在华为，我们做出了如下承诺：我们将支持和采用广义的国际认可的网络安全标准或最佳实践；我们将支持增强网络防御能力的研究工作；我们将继续改善和采用开放透明的方法，让政府能够评估华为的安全能力。最后，正如我们迄今为止所做的一样，我们热烈欢迎我们的客户来帮助我们增强流程、提高技术、改进网络安全的方法，让我们可以为他们以及他们的客户带来更多的利益。

---

[2] http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf

[3] http://www.apple.com/pr/library/2012/03/05Apples-App-Store-Downloads-Top-25-Billion.html

[4] https://sites.google.com/a/pressatgoogle.com/google-i-o-press-2012/android

# 3 通信与我们的21世纪社会

## 这是关于保持对全球生态系统的信心……

世界上大多数人往往认为通过声音和数据进行沟通是理所当然的，我们期望这种沟通所应用的技术永远且随时可以获得。通信技术已经融入到我们社会生活的交互中了，其融入方式本身就是一个奇迹。我们已经逐渐依赖于日常使用的系统和应用，其可用性及各种功能让我们的生活更加便捷。

政府、企业和消费者对技术的使用大幅增长。2011年底，全球移动用户达到了59.6亿，占全球人口的86%，比2010年增加了12.3%。[5]

电信和互联网应用日益丰富，而且随处可以获得。智能手机的市场份额逐年增长。以美国为例，智能手机的市场份额2011年12月时为47.8%，而在2012年3月增加到了50.4%。[6] 智能手机集成的功能和应用越来越多，其中有些应用程序涉及个人数据，如联系人、位置数据、个人照片、手机银行等。 智能手机应用程序的数量飞速增长，比如，苹果应用商店的程序数量已经达到了250亿下载的里程碑，也就是说，每个iPhone、iPod Touch和iPad用户下载的应用程序平均数量为79个。[7]

恶意搜集个人数据和无意的设计错误都可能会对网络及其用户造成破坏。

社交网站全球范围的增长也带来了一些个人安全挑战。一次调查显示，在英格兰和威尔士，“每40分钟就有一个通过Facebook进行的犯罪在发生，12,300个案例都跟这个网站相关。”[8] —— 这并不能反映社交网站提供的网络安全，而是反映了本身无害的社交网络技术能如何被误用或滥用。

随着智能手机使用的增加，攻击智能手机的动机和方法也随之增长。2004年到2011年间，智能手机恶意软件的感染率增加了6倍。[9]

随着业务能力的丰富和用户体验的提升，ICT相关软件的复杂程度和规模都迅速膨胀。在软件的规模和复杂性增加的同时，安全漏洞的数量也出现了增长。[10]

过去的电信网络基础设施是封闭和专用的。现在，随着VOIP IMS等新型业务的发展，网络基础架构也向第三方服务提供商开放接口，基于IP的开放协议应用得越来越多。过去的电信设备通常在专用的硬件上运

[5] http://www.itu.int/ITU-D/ict/statistics/

[6] http://techcrunch.com/2012/05/07/nielsen-smartphones-used-by-50-4-of-u-s-consumers-android-48-5-of-them/

[7] http://www.guardian.co.uk/technology/appsblog/2011/jul/07/apple-iphone-app-store-downloads

[8] http://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked-site.html

[9] F-Secure Mobile Threat Report Q4 2011

[10] Alhazmi OH et al., Measuring, analyzing and predicting security vulnerabilities in software systems, Computers & Security (2006), doi:10.1016/j.cose.2006.10.002

行。而现在，越来越多的设备基于通用架构的硬件和操作系统。基于通用架构硬件和操作系统的ATCA(高级电信计算架构)平台的发货量在2008年到2011年间增长了10倍，现在有一百多家公司参与构建了ATCA的生态系统。[11]

不确定能否安全地通信并访问在线数据及应用程序，会造成混乱和困惑，并动摇用户的信心。作为通信技术的提供者，我们需要确保这种信任得到维护，关系、流程和方法得到持续改善以应对21世纪以及之后的数字化挑战。

## 3.1 日益增长的网络安全挑战

网络安全方法最初是为了保护网络和数据。近几十年来，网络安全开始演进到打击网络犯罪以及其他在线恶意活动。网络犯罪与其他种类的犯罪一样——都有罪犯和受害人。跟其他犯罪一样，要构成网络犯罪，需要：犯罪动机、犯罪机会和犯罪方式。技术已经变得越来越普及，而且越来越融入政府、企业和个人日常生活的使用中。网络犯罪的潜在利益也是如此。由于可访问性和连接性的增加，造成网络事故的方式和机会也增加了。在互联网时代之前，只有少数人知道如何使用电脑，攻击它们的原因也很少。如今，通过你口袋里的移动终端就可以很便捷地访问互联网。因此，网络犯罪的方式和机会就大大增加了。现在，几乎人人都通过网络相互连接，有很多方式去利用网络空间，不论是为了个人还是商业用途——出于好的还是坏的动机。

来自丹麦计算机安全服务提供商Secunia公司的史蒂芬.弗雷博士在RSA会议的演讲中阐述了威胁环境如何变化：由脚本小子因好奇而进行黑客攻击，发展到专家为个人利益而帮别人开发攻击手段。只要有钱或有利益的地方就会有犯罪——技术领域并没有什么不同，在某些情况下，技术只是让犯罪变得更加容易而已。[12]

**全球的技术公司必须要保护他们的技术以避免一系列恶意用途，包括：**

**用于破坏：**控制、瘫痪、破坏或破解网络或基础设施

**用于间谍活动：**促使第三方能够通过他们的技术非法监视其他个人或组织

**成为其他组织/国家的延伸：** 公司的全球触角和能力被其他政府/组织主导用来与其他国家/亚国、组织或个人进行对抗。

**缺少预防措施和能力**：缺少最佳实践以及端到端的网络安全能力从而使得技术成为一个非常容易的攻击向量——任何威胁方都能够使用公司的技术或能力用于非法或不当的目的。

---

[11] http://www.heavyreading.com/details.asp?sku_id=2228&skuitem_itemid=1111

[12] http://secunia.com/resources/reports/?action=fetch&filename=Secunia_Moving Target_presentation_RSA2012.pdf

**所有进行技术开发和支持的公司都必须嵌入风险告知机制、应对措施、政策和程序，以减少主观感知的或客观存在的威胁成功攻击的可能性。这些威胁包括但不限于：**

- 硬件/软件的“致命切断开关”（固定或远程控制）
- 通过后门、木马、病毒或软件逻辑炸弹进行控制
- 公司（个人或团体）受到指使去关闭网络；从事间谍或破坏活动；或帮助第三方进行非法活动
- 促使能够访问数据（包括技术情报、国家安全信息、商业安全信息和私人数据）
- 嵌入“自动通报”/监听能力以转移数据或控制到其他国家/组织
- 研发流程的弱点—安插人员或软件威胁
- 供应链的弱点—植入组件（构建之前或之后）
- 人员的弱点—贿赂
- 现场支持能力的弱点—安插/贿赂人员或安装非法软件

一个技术供应商的硬件和软件可以通过一系列方法和方式被恶意利用。这就要求对技术和潜在弱点进行持续评估。在华为，我们评估所有这些项目，并问自己这样的问题：“若有人想要实施这些攻击机制中的其中一个，他需要做些什么？”然后，我们再问：“成本和风险更低、成功可能性更高的机制是什么？”从这些问题的答案中，我们知道如何最好地降低此类事件的发生。我们现在的模式是：我们不假定任何事情，我们不相信任何人，我们检验所有的东西。

## 3.2 终端、数据和事件

由于媒体对网络安全的强烈关注，你可能会认为“数据/知识产权丢失”是新事物，是在非数据或纸质时代没有出现的。但是，它以前确实发生过，而且现在仍在继续。

要知道，那些离开公司的人随之带走了客户名单、将来的产品组合或产品定价模型，甚至是下一个产品的设计和技术图纸。而技术恰好帮助了这些想要这样做的人更快、以更低的成本去做，获得更多的数据——他们甚至可以远程操作。近期，一个调查发现，欧洲有51%的上班族在他们换工作的时候从他们现有雇主那里带走信息，帮助他们访问机密客户数据库，尽管有数据保护法禁止他们这样做 。[13]

虽然无法精确评估这种损失，但无论是无意的数据泄露或恶意的工业间谍，数据泄露的代价都可能达到数十亿。可以肯定的是，既找不到一家公司，其资产价值因所谓的网络间谍而减少；也无法在外部审计报告或上市公司董事因诚信义务而发布的股票交易声明中看到这种潜在的损失。除非我们坦诚面对所发生的事情，否则我们无法评估在哪里投资。重要的是，我们可能会因为过度管制而走向灭亡，减少技术带来的很多好处。

其他的事情也发生了变化。我们几乎完全依赖于技术去存储数据、进行交易、管理生意，并在某种程度上，经营我们的生活。我们存储的数据继续以显著的速度在增长。

我们拥有的终端越来越多，连接的终端也越来越多。在发达国家，移动渗透率超过公民人数，这并不罕见——每个终端都给了我们另外一个地方去存储数据，但仍有可能丢失数据。关键是，对于有些人来说——想要从你的基础设施中偷取数据、全部毁坏，或更糟的是，对你的数据进行部分破坏，大大降低你对所持有数据的信心，这些终端还是他们的潜在入口。

想象一下，存储的血型信息被随意更改会造成什么样的恐慌，或你的有些银行交易偶尔被随意篡改数目——这很难发现、很难追溯，因此也很难解决。想象一下这种事件对受影响机构的公众信任带来的负面影响。

当然，威胁不限于随意操作。可能有人攻击你的汽车技术，通过一条短信开启或关闭你的引擎[14]，尽管有很多公司努力阻止这种情况发生[15] 。或者，可能是网络恐怖主义者攻击电站。英国皇家联合服务研究所（RUSI）杂志里有一篇题为“网络——武器”的文章详细描述了这种情况。这篇文章由里德和麦克伯尼撰写，清楚地指出关键基础设施是如何经常远程访问，从而是可以被利用的。[16]

还有一些场景没有那么戏剧化。比如，你下载的一个小小的智能手机应用程序——它要求处于“信任状态”才能访问你存储的电话数据。如果无意之间下载了恶意软件，你的日程、联系人、邮件和信息都突然被上传（可能是未加密的）到某个远程服务器上，其目的你永远不知道，而且你可能不会知道发生了这样的事情。

---

[13] http://www.businesscomputingworld.co.uk/when-employees-leave-your-company-so-does-your-data/

[14] http://www.securityweek.com/car-hacking-researchers-highlight-emerging-risks-and-lack-security-automobiles

[15] http://www.reuters.com/article/2012/08/20/us-autos-hackers-idUSBRE87J03X20120820

[16] http://dx.doi.org/10.1080/03071847.2012.664354

## 3.3 识别参与者

我们要识别出我们生活的这个网络世界中的众多对手，这点很重要。他们包括：

- 个人：从事骚扰、恐吓、欺辱或诱拐儿童进行性侵等一系列活动的人；
- 黑客：有特定目的去利用或通过黑客攻击提升其事业的个人或组织（松散的或紧密相连的组织）；
- 犯罪分子：有组织的（和没组织的），实施非法交易、伪造商品、工业间谍等各种诡计；
- 恐怖主义者：不论其定义是什么，是指那些预谋制造危害的人；
- 政府支持的人员：利用技术以及其他情报方法去收集对他们有利的数据和信息；
- 其他各方：从事商业间谍活动，从某个国家或竞争者获得先进信息为自己所用。

毋庸置疑，人人都需要考虑技术安全的问题，因为它是我们生活和工作中大的风险环境的一部分。随着世界相互连接得更紧密，以及政府、企业和消费者对技术的日益依赖，挑战的规模也大幅增加。

我们可能已经丢失了比地球上的人口更多的机密信息。人们很容易会有这样的印象：安全破坏比暴风雨的雨点还多。很少有一天看不到这样的报道：某个地方的关键基础设施被网络犯罪分子攻击（或有被攻击的可能性）。

我们部署的技术越多，连接、使用和共享的技术越多，我们会更加觉得个人和公司数据以及所使用的技术会无关紧要。这种无知体现了对数据在我们日常生活中重要性的不尊重。这种不尊重是危险的，本身也加快了安全风险的增长。

设想一下：国际上防护软件供应商宣称每秒[17]有12种由新的、专门的恶意软件造成的技术威胁产生。如果知道在哪里能找到价格仅为249美元的专门的恶意软件，我们每个人都可能会去购买。这样的价格还包含了服务水平协议和更换保证，保证所购买的恶意软件在9个月之内如果被任何防病毒软件发现，将负责更换。

将政府列入网络世界的对手名单中似乎不对，因为政府很坦率，激烈地谴责那些攻击他们国家的人。但是我们必须要清楚，纵观历史，间谍活动都持续在外交中发挥着作用，无论是积极还是消极的。最近，福布斯杂志的两篇文章《对话黑客：销售间谍软件——攻击你电脑的工具（并收取六位数的价格）》和《购买零天漏洞：黑客秘密软件攻击漏洞价目表》说明了有一个识别和销售零天漏洞的“生机勃勃”的行业，也就是说，安全漏洞一经发现就对其进行攻击。实际上，文章还表明，世界各国政府经常购买零天漏洞，并且大型的国防承包商也购买和销售零天漏洞。如果政府确实参与购买零天漏洞或者开发或利用像Flame和Stuxnet之类的攻击软件作为武器，脑海中出现这样一句话：“我们播种什么就会收获什么”。[18、19、20、21]

---

[17] http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=2011_in_numbers&om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Apr_worldwide_ISTR17

[18] http://www.bbc.co.uk/news/technology-12633240

[19] http://www.dailytech.com/CBS+US+Israel+Opened+up+Cyberwarfare+Pandoras+Box+with+Stuxnet/article24155.htm

[20] http://www.europeaninstitute.org/EA-November-2011/main-cyber-threats-now-coming-from-governments-as-state-actors.html

[21] http://news.cnet.com/8301-1009_3-57445975-83/flame-a-glimpse-into-the-future-of-war/

## 3.4 理解全球供应链的影响

打开任何一个智能手机、平板电脑、个人计算机、电视机、甚至是消费者白色家电，你都会看到这些设备中有一个全球供应链在起作用。以台湾为例，它每0.35秒生产一台笔记本电脑；每8.54秒生产一台PDA；每0.68秒生产一台台式电脑。[22]

**美国审计总署2012年3月发布的报告指出：IT产品的全球供应链可能会给国家安全带来风险：**

> “联邦机构广泛依赖计算机信息系统和电子数据去实施其行动。通过全球供应链去攻击信息技术的产品和服务已经成为一个新兴威胁，将削弱关键和敏感机构网络和数据的机密性、完整性和可用性。”[23]

报告称：能源部、国土安全部、司法部以及国防部的官员告诉审计总署的调查员说：他们不知道他们的通信网络中究竟包含多少国外开发的设备、软件或服务。根据这份报告，能源部和国土安全部并没有制定供应链保护措施。司法部已经制定了保护措施，但是并没有实施或制定流程去监控这些措施的遵从程度。

似乎也没有对“国外开发”的含义做出定义。虽然这篇报告关注的是电信网络，但是它确实需要考虑来自所有供应商的所有技术。

现实是：一个单一的设备，如手提电脑，包含的器件可能来自世界各地——加拿大、爱尔兰、波兰、意大利、捷克、斯洛伐克一直到中国、以色列、日本、马来西亚、菲律宾、新加坡、韩国、台湾、泰国、越南和其他很多国家和地区。

再看一下，中国成都，有16,000家公司注册，其中820家是外商投资公司。[24] 在这些公司中，189家为《财富》500强企业。一些家喻户晓的品牌也落户这里，举几个例子： Intel、微软、思爱普、思科、甲骨文、BAE、爱立信、诺基亚、波音、IBM和阿朗等。这些公司所做的事情应该被认为是“国外开发”吗?

思科在中国有着庞大的组织，在6大城市设有研发中心。思科所有的产品中超过25%是由其中国伙伴生产的。思科宣布在中国投资160亿美元，其中包括培训10万名网络工程师，并将在职业技术学院成立300个中心给学生培训网络技术。[25] 思科CEO 约翰·钱伯斯宣称：“我们正在努力勾勒成为中国公司的整体战略”。[26、27] —— 这构成“国外开发”吗?

根据相关公司报告，每个主要的电信设备供应商都在中国设有重要基地。阿尔卡特朗讯全球1/3的生产制

---

[22] http://www.taiwan-technology.com/edit/p/epaper/200902180.htm
[23] http://www.gao.gov/assets/590/589568.pdf
[24] http://www.chengduhitech.co.uk/Default.asp
[25] http://www.usatoday.com/tech/products/2007-11-01-425344141_x.htm
[26] http://www.epi.org/publications/trade_policy_and_the_american_worker/
[27] http://news.xinhuanet.com/english/2005-06/17/content_3096764.htm

造由上海贝尔完成；[28] 爱立信的合资企业南京爱立信熊猫通信有限公司已经成为爱立信全球最大的供应中心；[29] 截至到2011年底，诺基亚西门子网络的全球10家工厂中有5家在中国、2家在印度[30] ——他们做的是“国外开发”吗?

我们再看一看印度。在过去的二十多年中，已经建立了很多成熟、专业的国际公司和支撑服务，向全球企业界提供国内外技术。从纯粹的财政角度来讲，印度2011财年IT行业的总出口额为590亿美元。在全球经济增长放缓的情况下，该行业在2007到2011财年间，仍实现了强劲增长，达到了16.4%的复合年增长率。[31] 印度也产生了一些世界一流的企业，如TATA、Wipro、Infosys和HCL技术等。另外，上述提到的一些世界一流品牌，以及像西门子、惠普、飞利浦、ABB、伟创力和AT&T等一些企业都在这里设立了运营基地。思科在印度有8000多名员工，包括研发、销售和业务支持，建立了18个物流中心为客户提供强大的支持系统。思科在班加罗尔的研发中心是美国之外最大的全球研发中心。另外，思科还与Wipro技术和Infosys技术在班加罗尔建立了联合发展中心；与HCL技术在钦奈，与Zensar技术在普纳也成立了联合研发中心。[32]

总之，“国外开发”的概念在如今全球相互连接的世界中没有任何意义，正如这个理念是一样的：世界某个地方的公司或产品比另外一个地方的公司或产品更值得信任。你们必须要思考一下这个想法是否更像是披着国家安全外衣的贸易保护主义。在当今全球化的世界中，任何仅基于供应商国籍或供应商总部所在地而制定的网络安全政策都必定无效。简单地因为公司的母国而将这些公司孤立的网络安全方法是不符合逻辑的。而且，这样的方法本身就带有歧视性，违反了最惠国待遇。

**我们完全赞同微软的白皮书《网络供应链风险管理：实现透明和信任的全球构想》。该文件说道：**

> “首先，供应商有极大的经济动机来抵制政府出于以下简单原因而破坏供应链的工作：后门或其他有意缺陷很有可能被发现和公开，此类公开将导致公共信任的丧失，并最终丢掉市场份额。实际上，故意从事此类活动的公司很可能被强制破产，特别是当它认识到将在全球范围内丧失信任时；也就是说，即使插入后门的主要目的是为使本国政府可在防御外敌时赢得优势，供应商本国的人们也可能拒绝包含秘密后门的产品。在许多国家/地区，不仅担忧外国监视，而且担忧国内监视。”

**他们的结论是：**

> **“…虽然政府担忧可以理解，但政府响应不要威胁全球信息和通信技术（ICT）部门的活力，以免压制创新和竞争。”** [33]

事实上，当你把从不同的供应商获得的设备跟你的技术基础设施连接时，设备和软件可能是由世界各地的公司设计、开发和制造的，如果没有几百家，也有几十家公司。

---

[28] http://www.alcatel-sbell.com.cn/Default.aspx?tabid=262&ArticleID=1173

[29] http://www.ericsson.com/cn/thecompany/ericsson-china/background-china

[30] http://i.nokia.com/blob/view/-/1015984/data/3/-/form20-f-11-pdf.pdf

[31] http://www.ibef.org/industry/IT-ITeS.aspx

[32] http://www.cisco.com/web/IN/about/company_overview.html

[33] http://www.microsoft.com/en-us/download/details.aspx?id=26826

全球ICT供应链问题是由理查德•克拉克总结出来的。他曾经是乔治.布什总统下属的反恐安全小组负责人和国家安全委员会成员，他也曾经在克林顿政府任过职。2002至2003年间，克拉克担任布什总统的网络安全特别顾问以及总统关键基础设施保护委员会主席。该委员会帮助起草了布什总统于2003年2月发布的《美国网络空间国家安全战略》。克拉克说：“我的态度是，不管来自于纽约州还是上海市，软件都可能有同样的风险。在美国，也有人可能会被贿赂。”[34]

## 3.5 数字世界的法律

网络安全是一个全球问题。数据的传输和处理是一个全球性的活动，数据流并不因为国家边界、政府或法庭的地域限制而停止。发生在美国的一个搜索可能由在美国的服务器处理，但也可能由欧洲甚至亚洲的服务器处理。但是，法律和法规体系都是基于地域边界的。这就给所有涉及到处理和传输数据的跨国企业带来了一系列的挑战。

在所有影响ICT行业的法律中，以网络安全和隐私保护法律为例，欧洲在数据保护法方面有着更加统一的方法。但即使这样，虽然欧盟数据保护指令提供了欧洲对数据保护法律的统一方法，欧盟27个成员国对该指令的实施却大相径庭。在美国，隐私法律分散在联邦和州法律中。联邦法律仅限于在具体领域，如金融、医疗和某些行业来保护隐私，并没有综合的联邦法律来保护隐私。各州也有隐私法律，但是并没有实现让各州的法律保持一致。例如，事实上，每个州都颁布了自己的数据安全违规通报法律。但是，关于违规通报内容以及公司是否要通知监管机构、州司法部长或信用局等义务可能会大不相同。

很多国家和地区（如：澳大利亚、印度、中国、阿根廷、马来西亚、香港等）在立法和执法方面的义务都存在很大不同。即使是一个国家的不同区域在相关法律的执行和解释上也可能不一致。企业在有些国家还面临这样的挑战：制定了标准和规范，但是并没有写入正式的法律。

总之，这些都说明，所有公司，包括像华为这样的设备供应商及其企业客户，都面临着不同法律法规的混合，其义务不仅会因地域而变化，还会因标的物而变化。法律法规环境规定了关于监控和监听的义务，从而影响了行业标准。因此，设备制造商必须生产遵从众多的行业标准和法律的设备。另外，因为法律绝不会是静止的，设备制造商还面临着额外的挑战。随着法律的变化，硬件和软件也必须改变以体现新的法律要求。

**在数据保护和网络安全方面，华为欢迎一个原则上协同一致的国际方法。我们相信这种方法将帮助建立更好的基于全球的数据保护整体标准，而不是让设备商、服务提供商和企业努力在不同国家采用不一致的标准和方法。正如本白皮书所说，像华为这样的设备制造商是在一个复杂的法律法规环境中运营。华为承诺遵从其运营的每个行政区域所有适用的法律法规，并将其运营限制在必要的范围内以遵从国际制裁法案和当地法律。**

---

[34] http://www.networkworld.com/news/2011/091911-clarke-cybersecurity-251014.html

# 4 华为的方法

网络安全，是一场马拉松，而不是短跑。

华为为自己的历史感到骄傲，为拥有一个具有创业精神的创始人而感到自豪——我们的创始人，命运使然，恰好出生在中国。如果我们是一家美国、印度、德国或其他国家的公司，我们也会感到同样骄傲。

通信基础设施的复杂性、供应商的多样性、快速发展而带来的技术漏洞以及遵从变化的法律法规指令的难度都使得管理供应链风险非常具有挑战性，但是，根据我们的经验，这个问题并非无法克服。华为的商业价值观之一就是在商言商,保持政治上独立。作为一家总部在中国的全球性公司，华为知道它需要努力在网络安全保障方面多走一步。华为从来没有获取任何国家、公司或个人敏感信息的动机，也不允许我们的技术被用于非法目的。华为没有，也绝不会支持、容忍或从事任何类似活动。

**这是一个持续努力的过程。华为致力于提供业界最好的产品和服务以满足客户的需求（“业界最好”由客户和政府利益相关方来定义）。我们非常重视网络安全，已经投入了很多资源去提升和改善我们公司、业界同行以及其他各方的能力，提供尽可能好的安全保障，确保所有人有一个更加安全的网络世界。**

## 4.1 网络安全是公司的全球政策

华为一直理解，在少数市场上，地方或区域的政治、商业环境会要求购买“本地”或“西方”产品，面对这种“挑战”， 客户会要求华为展示可信度。这就需要我们进行本地化的同时对产品和流程进行独立评估，从而确保供应/支持流程的完整性得以维持，可以保证高水平的安全保障。

华为构筑并全面实施端到端的全球网络安全保障体系。我们强调：将公司对网络和业务安全性保障的责任置于公司的商业利益之上，保障客户网络和业务的稳定安全运营（特别是在遭遇地震、海啸等自然灾害和其他突发事件时）是我们的首要责任，并以此来指导我们的具体行动；我们理解行业、社会对网络安全的关注日益高涨。

由于上文提到的微软白皮书里面详述的原因，为了我们的生存，我们从来没有危害任何国家、或者获取任何国家信息、企业机密、侵犯个人隐私的动机，也永远不会支持或容忍任何类似行为。我们在任何国家都绝不会支持希望我们从事非法活动的任何实体。世界的眼睛总是在关注我们；我们积极鼓励审计和审查我们的能力。在这种背景下，那些希望某个供应商能够从事这种行为的人更大可能会选择一个监督比较少的公司。

我们理解所从事的行业的敏感性以及任何先进技术的脆弱性。我们从政策、组织、流程、管理、技术和规范等方面构筑并全面实施端到端可信赖的全球网络安全保障体系。华为1999年就正式开始了网络安全旅程，发布了首批安全技术规范，以增强产品与解决方案的安全性。2011年，公司创始人及CEO任正非签署并发布了如下的网络安全保障政策，进一步强调了我们的承诺：

“作为全球领先的电信解决方案供应商，华为技术有限公司（以下简称“华为”）充分理解网络安全的重要性，同时我们也理解各国政府及客户对此的担忧与高度关注。随着电信网络和信息技术的不断演进与发展，网络安全面临的威胁和挑战将日益严重。我们也心存忧患。华为对此高度重视，并致力于采取切实有效的措施提升产品和服务的安全性，从而帮助客户规避和减少安全方面的风险，以赢得各利益相关者的信赖。华为认为，构建一个开放、透明、可视的安全问题解决框架，将有助于整个产业链持续健康发展，也将会促进通信技术创新和人类沟通交流。

鉴于上述认识，华为在此承诺：将构筑并全面实施端到端的全球网络安全保障体系作为公司的重要发展战略之一，在遵从所有适用的国家和地区安全法规、国际电信标准和参考行业最佳实践的基础上，从政策、组织、流程、管理、技术和规范等方面建立和完善可持续、可信赖的安全保障体系，并与有关政府、客户及行业伙伴以开放和透明的方式，共同应对安全方面的挑战，全面满足客户的网络安全需求。华为同时承诺：将公司对网络和业务安全性保障的责任置于公司的商业利益之上。

在组织方面，全球网络安全委员会作为华为公司的最高网络安全管理机构，负责决策和批准公司总体网络安全战略。全球网络安全官是全球网络安全委员会的重要成员，负责领导团队制定安全战略，统一规划、管理和监督研发、供应链、市场与销售、工程交付及技术服务等相关部门的安全组织和业务，确保网络安全保障体系在各体系、各区域、全流程的实施，积极推动与政府、客户、合作伙伴、员工等各利益相关方的沟通。全球网络安全官直接向公司CEO汇报。

在业务流程方面，安全保障活动融入研发、供应链、市场与销售、工程交付及技术服务等各环节中，作为质量管理体系的基本要求，通过管理制度和技术规范来确保其有效实施。华为通过内部审计和接受各国政府安全部门、第三方独立机构的安全认证和审计等来监督和改进各项业务流程。华为的安全管理体系自2004年起已通过BS7799-2/ ISO27001认证。

在人员管理方面，华为全体员工以及合作伙伴、外部顾问都必须严格执行公司相关安全政策，接受安全培训，使安全理念融入整个组织之中。华为对积极参与网络安全保障的员工给予奖励，对违反网络安全保障政策的员工给予处罚，违反相关法律法规的员工，将依法承担法律责任。

华为愿意以开放、透明的态度真诚地与各国政府、客户、行业伙伴通过各种平台、组织、渠道开展安全交流与合作，共同应对全球网络的安全威胁和挑战。华为将根据需要设立区域安全认证中心，这些认证中心对当地政府和客户是高度透明的，由当地政府认可的机构和人员对

相关产品的安全性进行审查，确保华为对当地客户的安全交付。同时，华为积极、持续地参与ITU-T、3GPP、IETF等国际电信标准组织中的安全标准制定，加入FIRST等安全组织，并通过和主流安全厂商紧密合作，为行业的健康发展作出自己的贡献，努力保障全球客户的网络安全。

本声明适用于深圳市华为投资控股有限公司及其全球范围内直接或间接控股子公司和分支机构。

本声明应符合所在国家的法律、法规，在与当地法律、法规发生冲突的情况下，以当地法律、法规为准。公司将每年进行一次本声明的审核，根据相关法律规定进行重新修订。

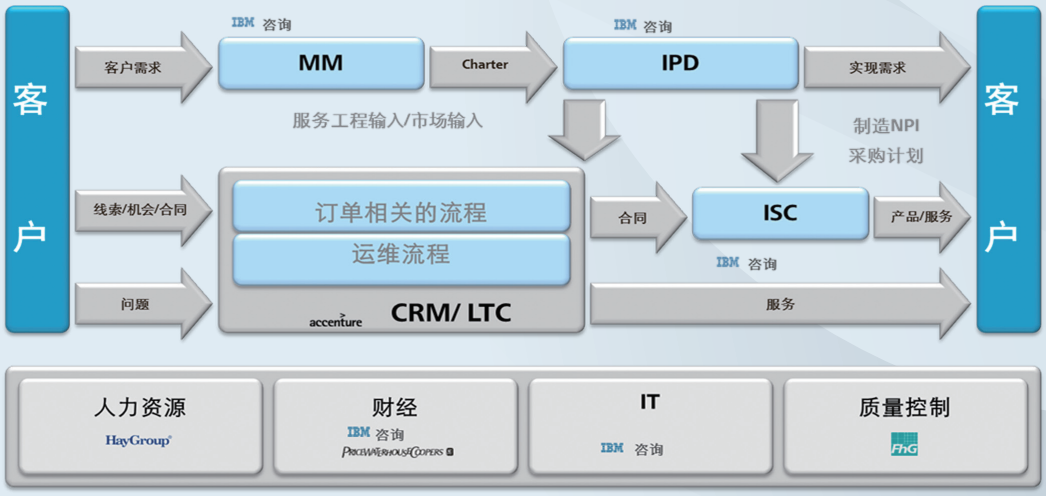
华为技术有限公司

CEO 任正非”

## 4.2 从内部构筑安全——“嵌入” 而不是“附加”

很多公司都会谈质量和创新。但是为了交付持续、创新的高质量产品和服务，需要一致、可重复且在全球推行的流程。否则，每件事、每个产品、每次客户互动都将成为随机事件——客户体验和产品质量时好时坏。华为自1997年起就聘请IBM促进、培训和支撑华为成为一个基于流程的组织，由可重复的流程进行驱动，交付质量一致的产品和服务。

下图展示了我们的高阶流程图。从图中可以看到，我们聘请了世界最具有创新精神的专业组织提供支撑：流程和技术方面是IBM；客户关系管理方面是埃森哲；人力资源管理方面是合益集团；财务方面是普华永道；外部财务审计方是毕马威（图中未显示）。



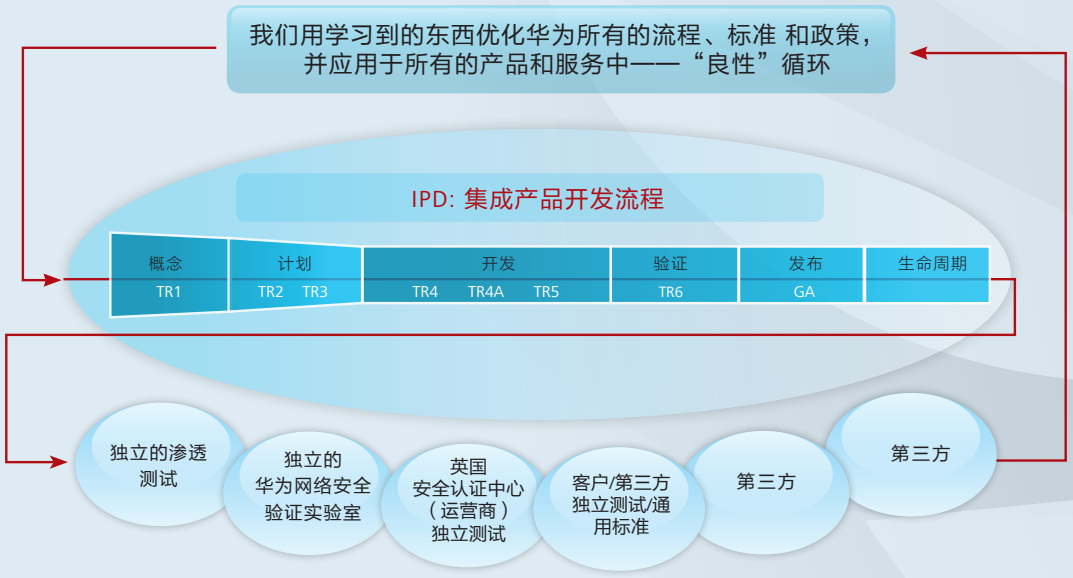

**LTC:**线索到回款(Lead To Cash) | **IPD:**集成产品开发(Integrated Product Development) | **MM:**市场管理 (Market Management) | **ISC:**集成供应链(Integrated Supply Chain)

为满足网络安全的要求，在我们的标准流程、基线、政策和规范中融入了所需要的最佳实践。这种方式使网络安全并不是马后炮，而成为我们日常经营方式的一个标准部分——我们基因的一部分。

但是，我们大家都必须接受这样的事实：你有一个流程并不意味着这是一个好的流程，或者人人都执行了这个流程。为了解决这些问题，我们采取了如下行动：

- 华为已经在全球建立了标准化的业务流程，明确了全球流程责任人（GPOs），并识别出了每个流程的关键控制点（KCPs）。此外，公司还制定了适用于所有子公司和业务单元的全球流程控制手册和职责分离矩阵。全球流程责任人（GPOs）负责根据运营环境和风险暴露的变化，确保整体内控的有效性。
- 管理方面，成立了一个专门管理网络安全的委员会，由副董事长领导，其成员包括主要的董事会成员，以及在确保网络安全要求融入流程、政策以及标准并有效执行过程中发挥作用的全球流程责任人（GPOs）。在网络安全方面，如果出现了任何冲突或资源问题，该委员会有权力和资格自行做出决策，调整业务，不需要获得其他人批准。
- 华为的审计方利用关键控制点和全球流程控制手册确保流程有效且得到执行。审计、外部调查和第三方审查都是通过将发生的事情与应该发生的事情对比来进行验证。个人的职责和责任（规章制度）融入到了华为的《商业行为准则》（BCG）和业务流程中，在商业行为准则和业务流程中详细说明了我们在日常业务中应该如何执行。每年都会通过在线考试的方式让员工都收到最新信息，了解最新知识。这也是我们内部遵从措施的一部分。

但是，没有什么比开放你的流程和内部系统，允许客户和政府进行审计和审查更加重要。让真正的客户、来自各领域的专家以及政府来审查和验证我们的方法。这种能力真正促使我们建立世界一流的流程和有机结合的体系。华为之所以能在140多个国家运营是因为它被140多个国家的客户所信任。再次强调，这是一个可重复的流程，也是一个良性的循环：我们开发——我们测试——我们验证——我们学习——我们优化——我们开发。这种模式如下图所示：



具体如何操作呢？举一个例子：很多全球技术提供商，如华为，都许可和使用从很多第三方来的软件组件，将其整合在我们自己开发的计算机代码中。我们自己的软件可能由多个国家的多个团队开发。但是，一旦出现安全问题或发现漏洞，你的内部流程和系统要能够让你向前和向后追溯到开发的软件组件，找出他们包含在哪些产品中。这点至关重要。

在华为，我们持续增强内部系统和流程，让我们能够从前端客户的原始需求一直追踪到所开发的计算机代码，也可以从后端的计算机代码（或补丁/修改）一直追溯到要求开发该计算机代码的原始需求。

在这个模式中，我们确保研发流程中的职责分离。软件开发工程师不能对最终测试的结果或最终发布的版本进行审批。软件开发工程师无法授权发布他们自己的软件，而是需要通过一个独立而严格的审查和签发流程——一旦发布，软件就自动上传到支撑网站，供生产环节或客户站点下载。

但是，网络安全并不仅仅是关于技术的，还与人、法律、激励和控制措施相关。毋庸置疑，我们在关注技术的设计、开发和部署时，我们也同样关注其他的流程——人力资源、法律、销售、财务、市场、供应商管理等。例如，在供应链的多样性方面，华为使用的70%的物料来自于中国大陆之外的供应商，其中美国的供应量最大，占32%，主要是技术含量相对较高的物料。台湾和欧洲两者加起来的供应量为32%。在人员的多元化方面，华为在其运营的140多个国家的平均本地化水平为72%。

在华为，因为我们已经将网络安全要求融入到业务流程，每个管理者和员工都要履行职责并承担责任。要形成这种责任感，需要一些基本要素：持续培训；在激励和个人责任之间找到平衡；不断地回顾流程，以增强我们的能力，并验证我们的保障水平。这就是华为应对网络安全挑战的方法。

在华为，我们采取“多眼多手”的策略。我们所做的事情都保持开放和透明。我们积极鼓励对包括华为在内的所有技术供应商开展公平无歧视的审查，促使这些公司挑战他们的思想、政策以及流程，从而增强能力、产品质量和产品安全。华为已经提供了可让客户和政府对我们的产品开展全面验证的能力。

随着移动互联和云计算的发展，华为紧紧跟随这种爆炸性增长带来的网络容量需求的激增，我们积极参与并开展了云计算研究。在虚拟化平台安全、虚拟化网络防护以及云计算数据安全等方面，我们开发了业界领先的技术和产品，构建了全面的云计算安全能力。华为已经成为业界具有影响力的云安全标准组织(CSA)的国际标准委员会(ISC)的核心成员之一。CSA ISC授权我司作为CSA联络官,代表CSA负责和中日韩安全workshop、中国通信标准化协会（CCSA）进行CSA云安全标准方面的宣讲和交流。

为应对网络安全威胁，华为正积极与政府、运营商、业界专家沟通，酝酿成立一个全球网络安全顾问委员会，指导华为网络安全能力的建设。华为建立了独立于业务的网络安全验证实验室，对华为的产品进行独立的安全测试，并向华为的客户提供验证报告，详细说明所验证产品的质量和安全能力。同时这个实验室也向华为的客户和政府开放，验证华为产品的网络安全。

华为与反钓鱼工作组（APWG）、中国CERT（CNCERT/CC）、OPERA、中国互联网络信息中心

（CNNIC）、中国反钓鱼网站联盟（APAC）、防病毒软件提供商AVG、国际刑事警察组织（InterPol）、互联网监视基金会（IWF）等组织在威胁建模、恶意软件检测、攻击行为分析等关键网络安全领域建立了深度合作关系，有效共享安全能力。

华为赞助并参加了多个网络安全论坛和会议，相互分享和相互学习。比如，在东西方研究所（EWI）会议上研讨如何形成全球网络安全共识、供应链安全等；赞助并参加了全球信息基础设施委员会（GIIC），是其董事会的成员（主席），还参与了卓越论坛（Quest Forum）等。

华为是全球安全标准的一个主要贡献者。例如，华为每年向第三代合作伙伴项目（3GPP）提交多篇安全方面的文稿，华为牵头H(e)NB安全标准的制定，并与业界主要运营商和制造商一起推动机器对机器通信（M2M）和公共告警系统（PWS）的安全研究。华为鼓励员工在互联网工程任务组（IETF）与业界的专家一起讨论IP安全相关的问题，并在多个工作组如IPsec、 Karp、 syslog、 OSPF、 MPLS、 Hokey 和 IPv6等做出了贡献，通过积极参与，已有多篇标准建议被接纳。华为对虚拟网络的安全及垃圾信息的防范标准做出了贡献。华为是开放群组（Open Group）的成员，并采用了其供应链发展的草案。华为还参与了电气和电子工程师协会（IEEE）、开放移动联盟（OMA）、通用即插即用论坛（UPnP Forum）及WiFi联盟（WiFi-Alliance）等组织的安全标准活动。

总体来说，华为认为，寻找网络安全问题的解决方案是我们共同面临的挑战。我们必须开展开放透明的合作。而且我们大家必须积极增进我们的知识、改进我们的流程和产品，并积极支持国际法律、标准、政策和最佳实践的形成和实施。

# 5 管理全球安全难题——这需要共同合作

我们不应该认为我们在应对网络安全的挑战方面无能为力。威瑞森（Verizon）2012年的《数据泄露调查报告》(DBIR)指出，连续四年来，大部分的数据泄露（97%）都能够通过实施一些简单的应对措施而得以避免。[35]

澳大利亚国防部情报机构——国防通讯局（DSD）制定了“最重要的35项缓解战略”。该文件首次于2010年2月发布，之后根据DSD对澳大利亚政府内的事故分析定期进行修订。他们宣称，实施这些战略中的前四项就可以阻止DSD 2009年所响应的至少70%的入侵事故，2010年所响应的至少85%的入侵事故。[36] 通过采取这些缓解行动，澳大利亚和其他政府能够大大降低他们对网络安全风险的担忧。

如果我们有共同的意志和决心，并保持开放透明，我们能做的有很多。

智能手机和云计算日益发展，应用商店也得到了广泛使用。这些应用商店包含了世界各地开发的质量和安全标准各异的软件。在这种情况下，技术场景是非常复杂的，并且会变得越来越复杂。

网络安全问题增加了这种复杂性，因为网络安全本身包含横跨社会多个行业和层次的政策、技术、行为、标准、指南和法律。为了充分解决网络安全问题，私有部门和公有部门必须统一他们的目标和责任，在基于风险的框架内共同合作，确保数据和信息系统的完整性和安全性。

网络安全领域的合作不应受地理、政治或竞争力差异的限制。有些人可能会认为这是一个竞争优势，但事实上，不合作将会给坏人带来很多机会去攻击全球网络安全链条上的脆弱链接。现在有很多可以合作的论坛，但是这些论坛仍然是一个松散的合作，并没有形成一个真正综合统一的战线。

在这个背景下，政府必须发挥主导作用，建设统一、综合的管理，促进形成网络安全的全面合作方法——华为承诺将会支持这样的努力。

[35] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[36] http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

# 6 共同前进

回顾网络安全的历史，思考网络安全的现状，我们发现利益相关方之间普遍缺乏合作和信任，从而阻碍了我们为综合解决这些问题做出努力。所有的技术使用者和提供商也有同样的责任去寻找解决这些挑战的方法，我们必须树立更好的榜样。行业和政府必须紧密合作，制定适当的政策框架，增强网络安全。我们共同的工作必须由一系列原则来指导，提供一个协调行动的框架，按照一致的战略重点、目标和里程碑推动前进。我们还必须能够接受这样的事实：相关方的承诺刚开始可能会因为他们之间缺乏信任、地方政治和地缘政治的问题、贸易保护主义和竞争者散布虚假消息等原因，不如我们期望的那样坚定——尽管如此，我们不应该将这些事情作为不采取行动的借口：

**指导原则**

1. **它是全球性的：**增强网络安全的努力必须在管理、法律、标准和制裁等方面适当地反映当今网络环境无边界、相互连接和全球性的特点。
2. **它是关于法律的：**必须要努力去协调和统一国际法律、标准、定义以及规范，接受文化差异带来的挑战。
3. **它是合作性的：**增强网络安全的努力必须建立公有和私有部门的合作关系，最大程度上增强我们集体对抗攻击的能力。
4. **它是基于标准的：**制定针对ICT供应商的国际标准和标杆，达成一致并实施。基于所感知的风险等级建立标准。——在安全和风险之间必须达到平衡。
5. **它是基于验证的：**设计、开发和实施全球独立验证的方法论，达成一致并采取行动，确保产品符合一致的标准和标杆。
6. **它是基于证据的：**增强网络安全的举措必须要基于证据，证实存在风险和攻击者，并且会造成损失或影响——我们应该关注事实而不是想象。
7. **它是关于做好基本要素的**: 我们共同的首要任务应该是努力改善网络安全的基本要素，从而将提升成功攻击的门槛。

本白皮书赞同并支持将国际合作、开放和信任作为这个世界的基础：对全球70亿人口中的大部分人来说，技术能够持续促进经济和社会发展。我们希望你们也同样支持这个选择。

# 7 关于华为

华为是一家全球性信息和通信技术（ICT）解决方案提供商，在140多个国家运营，产品和解决方案服务于世界三分之一的人口。我们有140,000名员工，平均年龄为28岁。在我们所运营的国家，本地员工的平均比例为72% 。全球前50大电信运营商中，有45家使用我们的产品。截至2011年，全球超过500个运营商部署了华为的无线网络产品和解决方案。近年来，华为累计出货超过200万台基站，为超过15亿的移动手机用户提供服务。

华为是一家以科学和工程为基础的私营企业，致力于研究、开发和部署新的商用技术。华为通过不断的创新保持在行业中的领先地位，拥有电信行业最有价值的知识产权组合之一。华为尊重和保护他人知识产权。华为每年将10%的收入投入到研发，2011年研发投入37.6亿美元，近十年投入的研发费用超过150亿美元。

华为已与许多公司达成专利许可或交叉许可协议，如：爱立信、索爱、诺基亚、诺基亚-西门子、Sisvel、高通、阿尔卡特-朗讯、北电、杜比公司、乐威（Rovi）、英国电信和荷兰电信等。2011年支付3亿多美元专利许可费，至今已累计支付12亿美元。我们的内部创新来源于1,265名世界一流的博士，44,690名硕士和62,000名研发员工。截至2011年底，华为在中国提出了36,344项专利申请，根据专利合作条约（PCT）提出了10,650 项申请，在海外提出了10,978项专利申请。华为被授予了23,522项专利证书。知识产权保护对华为持续成功至关重要。因此，华为坚决拥护对知识产权的保护。

华为全球有23个研发中心，与一些重要客户一起成立了34个联合创新中心，还有45个培训中心。68%的营业额来自于海外。华为使用的70%的物料来自于中国大陆之外的供应商，其中美国的供应量最大，我们从185家美国供应商购买32%的部件（2011年从美国公司的采购额为65亿美元），主要是技术含量相对较高的物料；台湾的供应量占22%；欧洲的供应量占10%；中国大陆的供应量占30%。

华为为60个国家的115个网络提供管理服务，帮助客户实现卓越运营。华为已经建立了基于云的IT解决方案，并与300多个伙伴合作，加快云计算技术在多个行业的商业应用。截至2011年底，我们已经帮助了世界各地的客户建立了210个数据中心，包括20个云计算数据中心。

2011年，华为消费者业务的发货量近150,000,000台，包括55,000,000台移动电话。2011年，华为向全球交付了6000多万台MBB设备以及3000多万台家庭终端，包括固定接入和固定台。

华为支持主流国际标准，并为这些标准的制定做出贡献。截至2011年底，华为已经加入了130个行业标准组织，如3GPP、IETF、ITU（国际电信联盟）、OMA、ETSI（欧洲电信标准化协会）、IEEE、Open Group 和3GPP2。华为共向这些标准组织提交了28,000个议案，并成为以下组织的董事会成员：OMA、CCSA、ETSI、ATIS（电信行业解决方案联盟）以及很多其他权威组织，在这些组织中占180多个席位。

有些人报道说华为是不同的，其运营的规则也不同。在某种意义上来说，这是对的：华为完全由持股员工所拥有，截至2011年12月31日，65,596名员工购买了公司股权。这让我们能够有长远的眼光，保证能够在风险、奖励和战略之间达成平衡。员工知道如果自己不能很好地服务客户，或者进行不当的活动，他们的股权和奖金将会受到影响。我们还培养了大量的人才，从世界一流的大学引进一流的科学家和工程师，培养他们，让他们很快拥有全球经验。

最后，华为是以创新为基础的公司：2010年，华为被FAST公司评为继Facebook、亚马逊、苹果和谷歌之后的第五大以创新为基础的公司，被《经济学人》杂志授予“2010年度公司创新大奖”。

在本文件的编写过程中，我优秀的团队提供了极大的帮助，也提出了很多建设性意见，并逐一体现在本文的字里行间。他们的专业精神和良好协作证实了我的印象：我们雇佣了世界上最优秀的一些员工。在此我特别希望感谢以下提供宝贵意见的朋友：南建峰、王唯践、彭丽巍、余志林、Paul Michael Litherland、刘晨曦、Andy Purdy、Andy Hopkins、杨光磊、John Koshy、Peter Rossi、Didier Blanchard，还有其他人员直接或间接地提供了帮助，恕不一一列举。

**Copyright © 2012 华为技术有限公司 版权所有**

您可以为内部、参考的目的复制和使用本文件。禁止除此之外的其他任何形式的使用。本文件未授予任何其他许可。

本文件“按原样”提供，不作任何明示或暗示的保证。任何保证均明确予以否认，包括但不限于不侵权、商用性以及对特定目的适用性的保证。华为不负责保证所呈现信息的精确性。本文件提供的任何信息可能会被纠正、修改和改变，恕不另行通知。使用或信赖本文件所提供信息的风险自行承担。本文件提供的所有关于第三方的信息均来源于公开资源或他们发布的报告和报表。

HUAWEI、**华为**、是华为技术有限公司的商标或者注册商标。

本文档提及的所有其他公司的名称和商标均为其各自所有人的财产。