华为网络安全立场

2019年11月

HUAWEI

目 录

一、执行概要 ---- 03

二、引言 ---- 06

1. 回顾华为网络安全白皮书的发布情况 ---- 06
2. 简介此立场文件的目的 ---- 07

三、ICT带来巨大的发展前景 ---- 09

四、理性的风险管理 ---- 12

1. 网络安全涉及诸多要素 ---- 13
2. 供应商所在地并非构成安全风险的要素 ---- 15
3. 理性、客观、基于证据的网络安全风险评估 ---- 17

五、系统地治理网络安全 ---- 18

1. 统一的网络安全标准 ---- 18
2. 独立的网络安全验证 ---- 21

六、有能力交付可信的高质量产品 ---- 23

1. 副董事长负责的全球网络安全与用户隐私保护委员会 ---- 23
2. 将网络安全要素嵌入端到端的业务流程 ---- 24
3. 网络安全2.0 ---- 26
4. 通过变革驱动安全技术创新 ---- 27

5. 安全的产品和解决方案 ---- 28
a) HiSec的安全架构 ---- 28
b) 华为5G解决方案的安全架构 ---- 31
c) 华为IoT解决方案的安全架构 ---- 38
d) 华为云的安全架构 ---- 42
e) 智能终端EMUI的安全架构 ---- 43
七、秉承独立的商业精神 ---- 47
1. 100%由员工持有的民营企业 ---- 47
2. 中国政府没有对华为业务或产品安全进行干涉 ---- 47
3. 为客户服务是华为存在的唯一理由 ---- 48
八、开放透明的合作 ---- 49
1. 通过SAB委员会加强与安全学者合作 ---- 49
2. 英国网络安全评估中心提供世界级的安全专业和技术保障 ---- 50
3. 德国波恩安全创新实验室探索新技术的安全标准与验证 ---- 52
4. 比利时布鲁塞尔网络安全透明中心致力于可信的数字环境 ---- 53
九、华为网络安全宣言 ---- 54
十、关于华为 ---- 56

一、执行概要

ICT 技术激发了数字经济的巨大潜力。近年来数字经济强势崛起，过去 15 年全球数字经济的增速是全球 GDP 增速的 2.5 倍。到 2025 年，数字经济创造的新增长潜力将达到 23 万亿美元（2017 年为 12.9 万亿美元），数字经济在全球 GDP 中的占比将从当前的 17.1% 上升至 24.3%。

数字技术的快速发展也带来诸多新的安全挑战。各行各业都在进行数字化转型，全面云化、万物联接、人工智能等新技术正得以应用。所有这一切都意味着网络安全风险在增加，保障安全的 ICT 环境是确保 ICT 产生积极经济影响的关键。作为全球技术提供者，华为深知网络安全对建立人们对数字世界的信任是很有必要的。

国际社会中，网络安全与政治的质疑、贸易的壁垒越来越多地纠缠在一起，但政治的质疑并没有促进网络安全问题的解决，贸易的壁垒只是把网络安全作为借口，人们往往无法从中识别出主要矛盾。

从事实来看真相，就是最有力的证明。我们鼓励数字生态体系的所有利益相关方采取理性、客观、基于证据的风险评估模式。如果我们把注意力放在不相关的因素上（比如供应商的所在地），这只会滞后安全问题的真正解决。如果我们对风险持情绪化态度或者存在偏见，结果就会变得不可控，我们也就无法达成安全目标。

网络安全涉及很多因素、很多利益相关人，全行业、全社会要通力合作，加强网络安全治理的系统性。

政府和行业组织需要合作建立统一的网络安全标准。网络安全标准应该是技术中立的，同等地适用于所有企业、所有网络。一直以来，电信行业不断通过制定统一标准来提升电信网络的连续性、可靠性和兼容性。正如麻省理工学院媒体实验室联合创始人尼古拉斯 · 尼葛洛庞帝在《Fast Company》杂志发表的一篇文章中写到：“电信政策应该基于客观标准，而不是地缘政治问题。”[1]

有了清晰、统一的网络安全标准之后，要基于统一的网络安全标准进行独立的全面验证。我们需要建立面向所有行

[1] 尼古拉斯 · 尼葛洛庞帝，2019年5月9日，《不要禁止华为，而是这么做》，https://www.fastcompany.com/90344450/dont-ban-huawei-do-this-instead

业和企业的第三方网络安全验证机制。信任也好，不信任也罢，都应基于事实，而非感觉。可验证的事实和统一的验证标准有助于产生客观的验证结果，让各个组织基于自身安全要求来比较和选择所需的产品。

华为将网络安全作为最高纲领，努力为客户网络安全和稳定运作提供保障支持。在过去 30 年里，华为在 170 多个国家和地区运营，服务全球 30 多亿人，没有重大网络瘫痪，也没有恶性网络安全事故。华为从未做过任何危及客户网络或设备安全的事情，也没有任何证据表明华为曾经这么做过。

二、引言

1. 回顾华为网络安全白皮书的发布情况

2012 年 9 月，华为发布第一版网络安全白皮书《网络安全透视：21 世纪的技术和安全——一场艰难的联姻》[2]，阐明华为在网络安全上的态度，以及华为如何保证网络安全问题上的独立性。

2013 年 10 月，华为发布第二版网络安全白皮书《网络安全透视：构筑公司的网络安全基因——一套综合流程、政策与标准》[3]，阐明华为端到端的网络安全流程和实践，以及华为如何系统和开放地保证网络安全。

2014 年 12 月，华为发布第三版网络安全白皮书《网络安全透视：与你的技术供应商考虑端到端网络安全时的 100

[2] 华为第一版网络安全白皮书《网络安全透视：21世纪的技术和安全——一场艰难的联姻》，https://www.huawei.com/cn/about-huawei/cyber-security/whitepaper/white-paper-2012

[3] 华为第二版网络安全白皮书《网络安全透视：构筑公司的网络安全基因——一套综合流程、政策与标准》，https://www.huawei.com/cn/about-huawei/cyber-security/whitepaper/hw_310546

个要求》[4]，阐明华为在网络安全标准上的努力和贡献，以及华为在网络安全领域的扎实行动。

2016 年 6 月，华为发布第四版网络安全白皮书《全球网络安全挑战：解决供应链风险，正当其时》[5]，阐明华为应对供应链风险的方法和工具。

2. 简介此立场文件的目的

今天，数字技术的快速发展带来诸多新的安全挑战。各行各业都在进行数字化转型，全面云化、万物联接、人工智能等新技术正得以应用。所有这一切都意味着网络安全风险在增加。

随着联接数的增加，网络攻击面也在扩大。随着全球化云平台的发展，传统的安全边界超越了地理及法律范畴，已

[4] 华为第三版网络安全白皮书《网络安全透视：与你的技术供应商考虑端到端网络安全时的100个要求》，
https://www.huawei.com/cn/about-huawei/cyber-security/whitepaper/hw_401492

[5] 华为第四版网络安全白皮书《全球网络安全挑战：解决供应链风险，正当其时》，
https://www.huawei.com/cn/about-huawei/cyber-security/whitepaper/huawei-cyber-security-white-paper-2016

经变得模糊。人工智能和大数据正帮助我们利用数据创造巨大价值，但数据泄露的风险也在增加。

如何剖解网络安全的问题？通过分析我们发现关于网络安全的讨论通常聚焦在如下两类问题：

第一类是关于问题的分析方面，网络安全是政治问题还是技术问题？供应商所在地是构成网络安全风险的要素吗？5G 比 4G 的网络安全性降低了吗？设备提供商可以掌控运营商网络的数据吗？设备提供商可以使用 kill switch 一键关停运营商网络吗？

第二类是关于解决的措施方面，全球供应链之下如何解决网络安全问题？为了保证安全，是要基于统一的标准进行验证还是禁止某个厂商进入市场？如何制定统一的网络安全标准和验证标准？如何避免或者减少迫于政治压力的产业有害消耗？

作为全球技术的提供商，华为力图针对上述两方面阐述华为的立场，使政府、行业等利益相关方既能正确地分析问题，又能找到有效的解决措施。

三、ICT带来巨大的发展前景

ICT 极大地促进社会与经济的发展。无论回顾过去，还是展望未来，我们都能看到 ICT 对社会与经济的撬动和渗入作用。根据华为的《全球联接指数 2018 年报告》，近年来数字经济强势崛起，过去 15 年全球数字经济的增速是全球 GDP 增速的 2.5 倍。位于 GCI-S 曲线前列的领跑者国家，正在利用智能联接加速数字经济发展，挖掘新的增长机遇。在智能联接的支撑下，各行各业将获得前所未有的发展机会。到 2025 年，如果各国的 ICT 基础设施投资平均每年增加 8%（年复合增长率），数字经济创造的新增长潜力将达到 23 万亿美元（2017 年为 12.9 万亿美元），为 GCI-S 曲线上的各类经济体注入新的活力。换言之，到 2025 年，数字经济在全球 GDP 中的占比将从当前的 17.1% 上升至 24.3%。[6]

宽带、数据中心、云、大数据和物联网五大使能技术在人工智能的加持下，正在重新定义联接。人工智能的应用可

[6] 华为《全球联接指数》，https://www.huawei.com/minisite/gci/cn/

以增强 ICT 基础设施的内在价值，提升自动化和智能化水平，最终实现智能联接。投资 ICT 基础设施和人工智能有助于提高生产效率、改善经济结构，这也是数字经济的真正价值所在。从长远来看，数字技术的投资回报率是非数字技术投资的 6.7 倍。

制造业将是智能联接的主要受益行业之一。就数字经济而言，传统制造产业引入智能联接后，预计将在 2025 年创造 6.4 万亿美元的数字经济规模。通过智能技术，传统行业可以更好地扩大数字溢出效应，促进数字经济的整体发展。

其他发展潜力较大的行业，包括主要由数据驱动的行业，也更有可能先于其他行业引入人工智能技术。数字经济有望驱动 ICT、专业服务和金融等行业的繁荣发展，市场价值将分别实现 5 万亿、3 万亿和 1.7 万亿美元的增长。社会及个人服务业、零售、交通和公用事业等行业也在稳步实现数字化转型，在智能联接的驱动下，这一节奏正在加快。

根据 GSMA 在 2019 年世界移动通信大会上发布的最新预测，到 2025 年，5G 联接数量将达到 14 亿，占全球联接总数的 15%；全球物联网的联接数量将增加两倍，达到

250 亿，全球物联网收入将达到 1.1 万亿美元。5G 将在未来 15 年内为全球经济贡献 2.2 万亿美元，其中制造业、公用事业、专业和金融服务等关键部门受益最多。[7]

第四次工业革命正在到来，拥抱这一历史性的机遇，将与时代共舞，否则就会丧失发展的先机。

[7] GSMA新研究：《5G网络部署加速，到2025年5G联接数将占全球移动行业联接数的15%》，2019年2月25日，https://www.gsma.com/newsroom/press-release/new-gsma-study-5g-to-account-for-15-of-global-mobile-industry-by-2025/

四、理性的风险管理

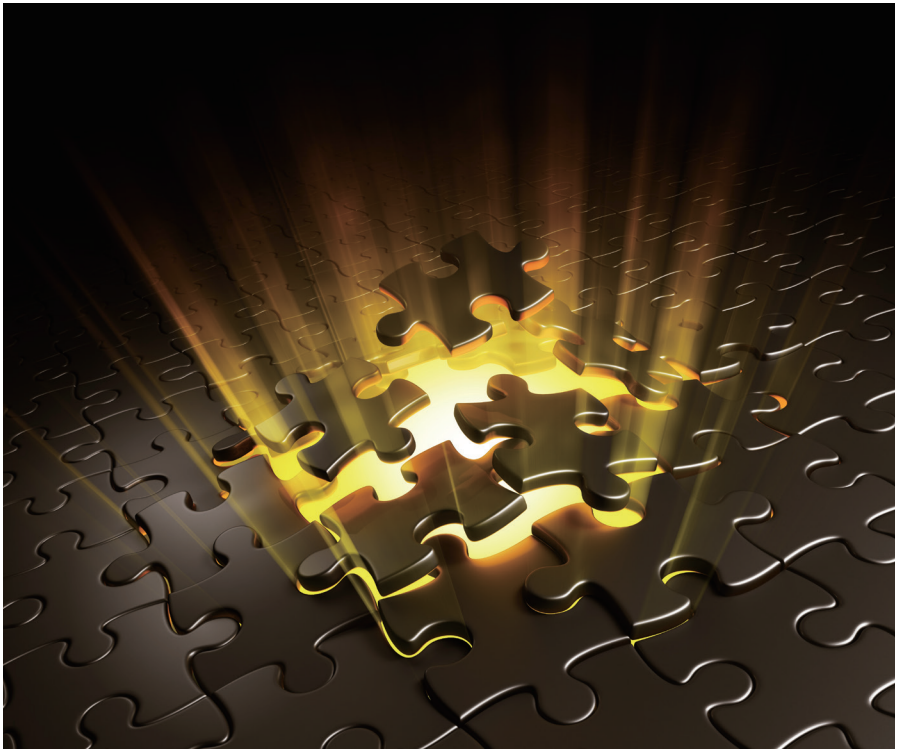
在 ICT 带给经济和社会巨大发展的同时，网络攻击的数量也在快速增长，根据 T-Systems 的统计，2017 年 4 月每天德国电信基础设施遭受的安全攻击数量是 400 万，2018 年 4 月每天的安全攻击数量达到 1,200 万，而 2019 年 4 月每天的安全攻击数量就达到了 3,100 万。

网络攻击成为攻击者可以租用、购买的服务。每天会出现 3-8 种新的攻击向量。分布式拒绝服务攻击（DDoS）、高级持续性威胁（APT）、暗网等攻击层出不穷，勒索病毒加密了被攻击者的文件，要求被攻击者支付赎金。电影《黑客帝国》中的场景在互联网中一步一步成为现实，企业和个人的资产蒙受损失，这影响了人们对互联网的信任，加剧了人们的恐慌。而 AI 的发展，也被攻击者利用，这就出现了一种 AI 技术与另一种 AI 技术的对抗。

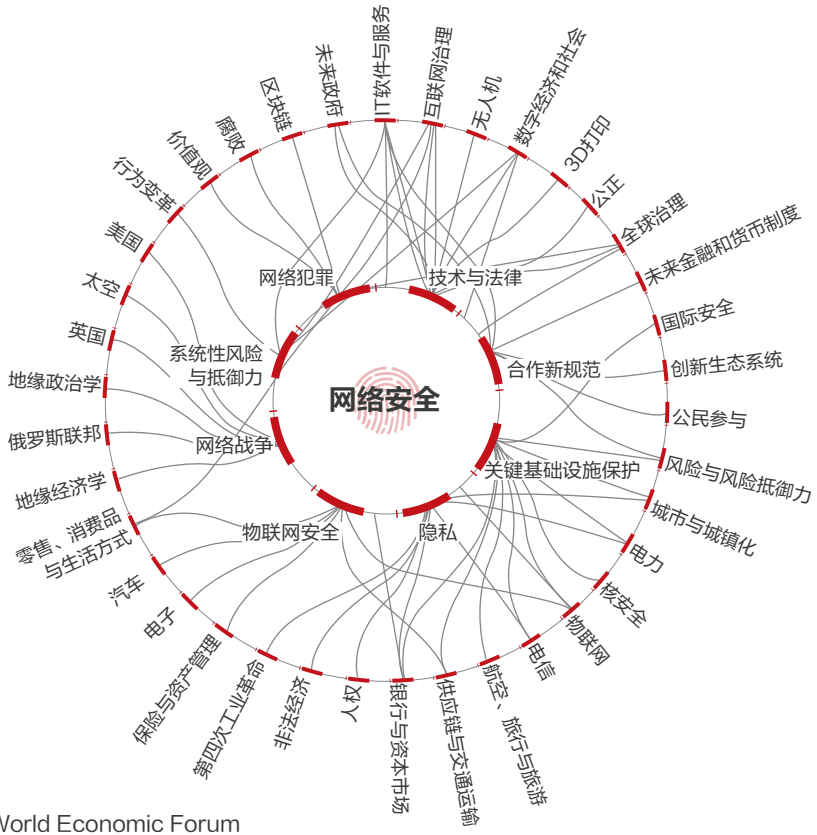
面对这一切，我们该如何分析、如何评估、如何应对？我们是采取主观的恐慌、猜忌、排斥，还是采取理性、客观、基于证据的风险管理？

1. 网络安全涉及诸多要素

随着各行各业数字化转型的深入开展，网络安全风险也在增加。比如联接数的增加，导致网络攻击面的扩大；全球化云平台的发展，传统的安全边界超越了地理及法律范畴，正在不断扩大；人工智能和大数据正帮助我们利用数据创造巨大价值，但数据泄露的风险也在增加。



网络安全涉及很多因素、很多利益相关人，也会涉及多个法律和治理机制。世界经济论坛网络安全中心识别了网络安全相关的八大要素[8]，包括技术与法律、物联网安全、隐私、合作新规范、系统性风险与抵御力、网络战争、关键基础设施保护和网络犯罪。详见下图：



© World Economic Forum

[8] 网络安全中心，https://www.weforum.org/centre-for-cybersecurity

网络安全挑战的复杂性决定了我们不能在某个单点上解决问题，也不可能靠任何个人、公司或国家来解决问题。我们需要携手共同解决网络安全挑战。

2. 供应商所在地并非构成安全风险的要素

网络安全与政治的质疑、贸易的壁垒越来越多地纠缠在一起，但政治的质疑并没有促进网络安全问题的解决，贸易的壁垒只是把网络安全作为借口，人们往往无法从中识别出主要矛盾。

从事实来看真相，就是最有力的证明。2018 年 8 月，欧洲联盟网络和信息安全局（ENISA）分析了欧洲电信运营商在 2017 年遭遇的 169 起安全事故，分析结果如下[9]：

- 62.1% 的安全事故根因是系统故障，平均每起事故影响 110 万个用户联接。
- 18.3% 的安全事故根因是人员误操作，平均每起事故影响 120 万个用户联接。

[9]“运营商上报 169 起安全事故，极端天气为主要因素”，2018 年 8 月 31 日，https://www.enisa.europa.eu/news/enisa-news/169-telecom-incidents-reported-extreme-weather-major-factor

- 17.2% 的安全事故根因是自然灾害，平均每起事故影响 60 万个用户联接。
- 2.5% 的安全事故根因是恶意攻击行为，平均每起事故影响 30 万个用户联接。

英国国家网络安全中心（NCSC）最新的公开发布显示：自其成立以来面临的 1,200 个重大网络安全事件中，大量的攻击是由攻击者寻找网络架构和运行上的弱点而实施的，并不是由供应商所在地发起的。[10]

从这些发现中，我们可以得出以下两个结论。

第一，系统故障和人员误操作是最主要的风险，应该在风险评估时优先关注。

第二，在评估产品的潜在风险时，应关注影响安全的主要因素，包括产品的安全架构、安全机制和安全特性等。

华为既是数字产品和服务的提供者，也是网络安全的共同守护者。如果在网络安全风险评估时把注意力放在不相关

[10] Ciaran Martin 在布鲁塞尔 CyberSec 大会上的发言，https://www.ncsc.gov.uk/speech/ciaran-martins-cybersec-speech-brussels

的因素上（比如供应商的所在地），这只会给我们造成伤害，却没有防范安全风险。

3. 理性、客观、基于证据的网络安全风险评估

作为全球技术提供者，华为深刻理解安全和可信数字环境的重要性。我们全力支持为客户提供安全的数字环境所做的努力，并致力于提高我们在这方面的能力。同时，我们认为所有利益相关人应采取更理性、客观、基于证据的网络安全风险评估模式。这有助于各方更加深刻地理解网络安全挑战，并制定自身的网络安全能力提升路标。

如果我们对风险持情绪化态度或者存在偏见，结果就会变得不可控，我们也就无法达成安全目标。如果我们希望真正解决网络安全挑战，采取理性、客观、基于证据的方式进行风险评估是唯一的出路。通过全行业、全社会的共同努力来系统化解决网络安全挑战，这将极大地降低网络安全风险敞口，增强投入产出比。

五、系统地治理网络安全

1. 统一的网络安全标准

政府和行业组织需要合作建立统一的网络安全标准。网络安全标准应该是技术中立的，同等地适用于所有企业、所有网络。

麻省理工学院媒体实验室联合创始人尼古拉斯 · 尼葛洛庞帝给出了极好的描述。最近在《 Fast Company 》杂志发表的一篇文章中，他写道，“ 电信政策应该基于客观标准，而不是地缘政治问题。”[11]

一直以来，电信行业不断通过制定统一标准来提升电信网络的连续性、可靠性和兼容性。在制定网络安全标准时，我们可以并且应该采取同样的做法。

例如，3GPP SA3 在推动统一的 5G 安全标准上取得了良好成果。5G 在安全架构上是 4G 的继承和发展，5G 的安全机制相比 4G 更完善。

[11] 尼古拉斯 · 尼葛洛庞帝，2019年5月9日，《 不要禁止华为，而是这么做 》，https://www.fastcompany.com/90344450/dont-ban-huawei-do-this-instead

- 在用户隐私保护上，5G 利用“ 用户永久标识符 ”（ SUPI ）对用户身份数据进行加密传输。
- 在通信数据保护上，5G 增加了数据完整性保护功能，确保数据在传输时无法被监听或篡改。
- 在运营商网络之间，5G 增加了端到端安全通道，防范黑客通过利用七号信令系统（ SS7 ）漏洞来盗取数据。
- 针对网络功能访问，5G 核心网提供了更高级的认证机制。

如今，由于公众对 5G 边缘网络和核心网络的工作机制存在误解，因此出现了一些关于 5G 安全的担忧。有人认为 5G 的核心部分和边缘部分没有区别。对此，英国国家网络安全中心 CEO Ciaran Martin 给出了清晰的解释：“ 技术精度对 5G 安全至关重要。5G 是一项重要的创新，但 5G 不是魔法，它无法改变科学规律或永恒不变的安全概念。5G 有着一套极其复杂的工程、技术能力和架构。标准组织的 5G 分析报告长达数百页，里面提及众多技术行话。因此，不能将 5G 过度简单化，提出‘5G 的核心部分和边缘部分没有区别’的说法，对所谓的‘核心部分和边缘部分没有区别’的说法不经证实或不提供证据，甚至没有针对‘核心’和‘边

缘’给出明确定义。这都不是考虑 5G 问题的正确方式。”[12]

也有人担心 5G 网络的集中式单元（CU）和分布式单元（DU）并没有分离。3GPP SA3 主席 Anand R. Prasad（作为联合作者）的一篇文章直接回应了这些担忧：“在 5G 中，基站的 CU 和 DU 之间逻辑上是分离的，CU 和 DU 之间的接口有安全保护机制。在 4G 中这种分离也是可能的，但在 5G 中，它是可以支持许多部署选项（如 CU-DU 共站部署）的架构的一部分。部署在网络边缘的 DU，在启用机密性保护的情况下，不能访问任何用户数据。即使在 CU-DU 分离的情况下，5G 的空口安全点仍与 4G 相同。”[13]

华为与数字社区密切合作，制定统一的安全标准。我们是 3GPP 安全与隐私标准的主要贡献者。2018 年，华为向 3GPP SA3 提交 464 篇 5G 安全提案，其中 227 篇获得批准。

---

[12] Ciaran Martin在查塔姆社2019年网络安全峰会上的主题演讲，
https://www.ncsc.gov.uk/speech/ciaran-at-chatham-house

[13] 如需了解更多关于5G安全优化功能，请访问
https://www.3gpp.org/news-events/1975-sec_5g。

2. 独立的网络安全验证

有了清晰、统一的网络安全标准之后，要基于统一的网络安全标准进行独立的全面验证。

我们处在全球供应链的时代，如果我们要真正确保所有系统和所有基础设施的安全，就应该对所有的供应商和部件采取同样的验证措施。我们不能只对某个联网系统的某个部分进行安全验证，因为这样的话，破坏分子就会盯上没有经过安全验证的部分。

不论是对电信运营商、政府还是个人用户，安全验证机制的重要性不言而喻，即便是某些机制尚不完美。例如，汽车碰撞试验无法模拟所有可能发生的车祸场景，但碰撞试验机制无疑极大地提升了汽车安全性。类似地，我们需要建立面向所有行业和企业的第三方网络安全验证机制。信任也好，不信任也罢，都应基于事实，而非感觉。可验证的事实和统一的验证标准有助于产生客观的验证结果，让各个组织基于自身安全要求来比较和选择所需的产品。

从电信行业来看，这一系统性的方法正在得以应用。目前，3GPP 和 GSMA 在网络设备安全保障机制（NESAS）方面

正取得巨大进步。这一机制可以对无线通信设备进行安全评估。为了让 NESAS 尽快落地，GSMA 将对第三方认证实验室进行资质审核，只有具备资质的第三方认证实验室才能对网络设备的安全性进行测试与评估。

华为强烈主张采取独立的安全验证。华为支持开放透明、公平合理无歧视的安全验证。华为产品已通过多个第三方机构的独立认证。目前已获得 39 个 CC 认证证书和 20 个 FIPS 认证证书。

美国 CFI 公司对 177 个运营商、12,300 位客户的调研数据及历史记录显示，华为产品的客户满意度、现网运行稳定性和可靠性指标均持续 3 年高于业界平均水平。

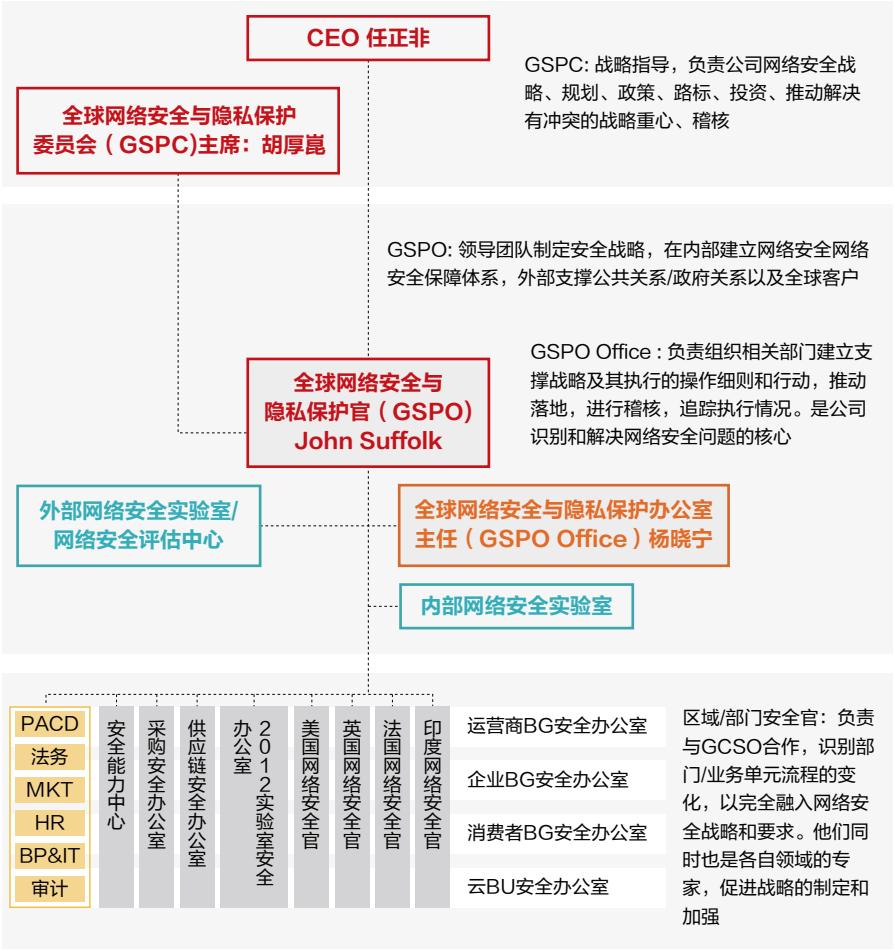
六、有能力交付可信的高质量产品

1. 副董事长负责的全球网络安全与用户隐私保护委员会

正如第三版网络安全白皮书《网络安全透视：与你的技术供应商考虑端到端网络安全时的 100 个要求》所述：“如果董事会和高级管理者都不认为网络安全是一个优先事项，那组织的员工也不会认为它是优先事项。确保网络安全融入到组织的组织设计、治理与内控框架是设计、开发和交付良好网络安全的开始。”[14]

华为在 2010 年设立了副董事长负责、多名董事会成员和业务总裁参与的全球网络安全与用户隐私保护委员会，管理网络安全与用户隐私保护的战略制定和执行。作为董事会成员和高级管理者，对网络安全用户隐私保护有清晰的认知和明确的责任，提供充分的资源，确保网络安全用户隐私保护融入公司的战略设计、治理架构。

[14] 华为第三版网络安全白皮书《网络安全透视：与你的技术供应商考虑端到端网络安全时的100个要求》，
https://www.huawei.com/cn/about-huawei/cyber-security/whitepaper/hw_401492



2. 将网络安全要素嵌入端到端的业务流程

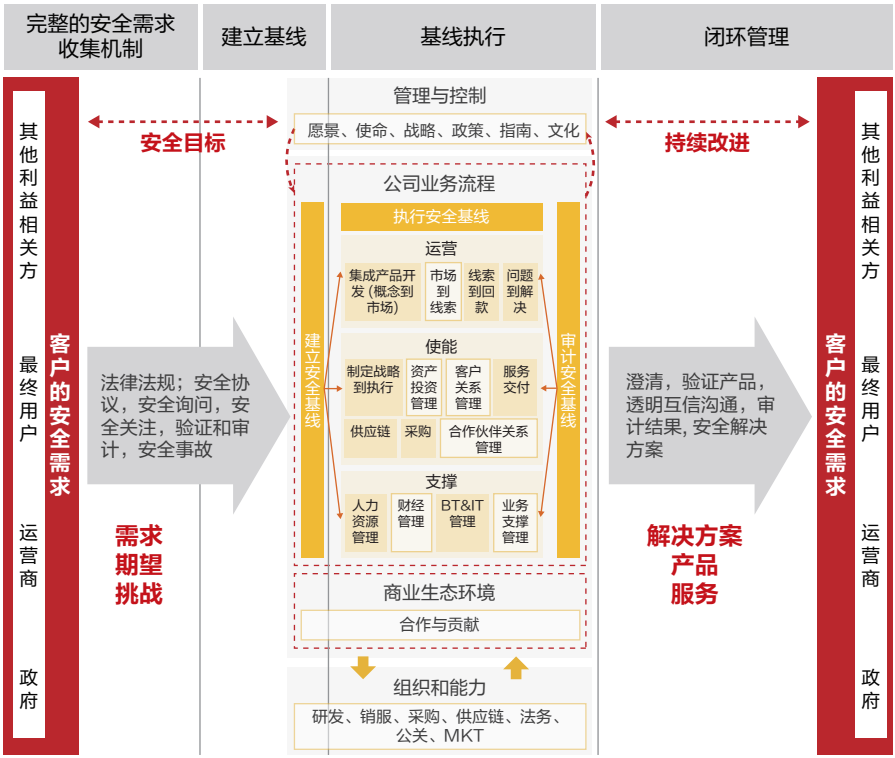
在华为第一版网络安全白皮书中，我们曾经阐述：“为满足网络安全的要求，在我们的标准流程、基线、政策和规范中融入了所需要的最佳实践。这种方式使网络安全并不是

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。”[15]

通过与美国权威顾问合作，华为打造了集成产品开发（IPD）流程并将网络安全要求嵌入流程。目前，华为正在开展 IPD 2.0 变革，进一步确保网络安全要求在所有流程环节中得到落实，包括需求分析、设计、编码、测试和生命周期管理环节。通过IPD 2.0变革，我们不仅能保障结果可信，也能保障流程可信。

如下图所示，华为打造了端到端的网络安全框架，具备四个特点：安全需求来自客户需求、法律法规等，华为对这些需求进行总结提炼，形成安全基线；基线嵌入业务流程，从而可重复执行，而非随机执行；建立了闭环机制，内部审计部检查业务部门是否执行了网络安全活动；高层管理者的思想输入网络安全管理系统，各业务总裁在全球网络安全委员会参与讨论、决策的意见，通过决议、战略、政策的方式指导业务在网络安全上的方向。

[15] 华为第一版网络安全白皮书《网络安全透视：21世纪的技术和安全——一场艰难的联姻》，https://www.huawei.com/cn/about-huawei/cyber-security/whitepaper/white-paper-2012



3. 网络安全 2.0

面向未来，云计算、万物联接、人工智能等新技术将对 ICT 产业带来深刻的改变，也带来了更大的网络安全挑战和机遇。在新形势之下，基于“ 网络环境是不安全的，网络攻击是常态化的 ”假设，华为启动网络安全 2.0 工作，目标是把网络安全打造成华为产品、解决方案和服务的核心竞争力之一，助力客户实现网络韧性。

具体而言，我们要提升整体网络安全环境洞察能力，识别威胁并与行业最佳实践保持同步。要持续夯实合规，系统性强化合规能力。要构建质量文化和安全文化，安全价值与商业价值并重，不断提高安全专家和主管的能力。安全治理要更加贴近业务，从“ 管控型 ”治理转变为“ 能力型 ”治理，加强基于结果的度量与监督，确保战略执行落地。

我们坚持技术、商业两轮驱动，持续提升产品质量以及关键安全技术 & 工程能力，基于网络韧性构筑产品与解决方案的安全竞争力。既要开放透明、主动宣传产品、解决方案和服务的安全竞争力，又要同客户、政府、媒体等利益相关方营造积极良性的环境，打造安全领域的“ 朋友圈 ”。

4. 通过变革驱动安全技术创新

华为在产品设计、开发及交付全生命周期，将网络安全与隐私保护置于战略优先地位，不因为成本、进度、功能等原因降低对安全的要求。目前，华为产品在网上运行质量已处于业界领先，运行质量好、性能强。面向未来，华为将每年投入 200 亿美金，打造高质量、安全可信的产品。

华为积极投入安全技术创新。网络环境正日益变得复杂，

这提高了产品安全要求。为了进一步增强产品安全，华为投入 20 亿美元启动资金进一步提升软件工程能力。华为是一个流程型组织，可重复的流程从根本上驱动组织运作，保障产品和服务质量水平的一致性。我们采用嵌入式方法，将安全融入所有流程环节，打造可信的高质量产品。

我们不只是回顾过去，看看哪些地方需要提升。我们还展望未来，与行业一起预测未来可能出现哪些新的安全威胁，从而增强我们的技术能力，以应对未来几十年可能出现的安全挑战。

华为在安全技术上进行研究和创新，包括可信计算、数据安全、应用密码、隐私保护和车联网安全等。在对这些研究方向进行探索的过程中，华为与学界和产业界进行深入合作。

5. 安全的产品和解决方案

a)HiSec 的安全架构

华为 HiSec 是华为各产品和解决方案的安全基石，围绕安全风险识别 、安全态势感知、安全风险防御、安全生态，

提供一系列安全公共的产品和组件。华为 5G、IoT、云等解决方案通过集成这些安全产品和组件，打造网络韧性，形成有效的保护网络边界、防御威胁攻击、实时态势感知、快速安全风险闭环的能力。

安全风险识别：构建漏洞感知系统来实现对华为现网产品的漏洞快速感知、漏洞被利用分析、漏洞风险评估、处置优先级排序等，来大幅度缩短漏洞发现和运维修补周期，补齐华为在漏洞管理的主动发现和快速响应能力，降低产品漏洞带来的被利用风险。具体包含漏洞管理工具等。

安全态势感知：围绕风险感知分析、风险处置响应、整网风险可视，构建华为通用的安全态势感知系统。该系统充分利用华为广泛的数据源、大数据、AI 智能技术的优势，对现网数据进行采集和实时威胁检测，发现威胁事件可自动的智能处置风险，并实现威胁攻击链的呈现、溯源，以及风险全面可视管理和威胁预警。具体包括大数据安全态势感知产品。

安全风险防御：打造云、管、端的安全产品和提供适配各产业的安全公共部件。一方面提供有效的网络安全产品保

护网络边界或者业务系统不受外部威胁攻击，例如 NGFW、IPS、WAF、Anti-DDoS 产品等，另一方面在产业中提供安全部件，用来被集成和共享安全能力，构建单产品多层防御的安全保护机制，包括底层完整性保护、OS 层安全、主机防漏洞攻击、应用层 WEB 防护等。

安全生态：HiSec 在安全领域和业界安全公司进行了广泛合作，积极构建自己的“ 朋友圈 ”，来为公司各解决方案提供有效和可靠的生态合作产品。

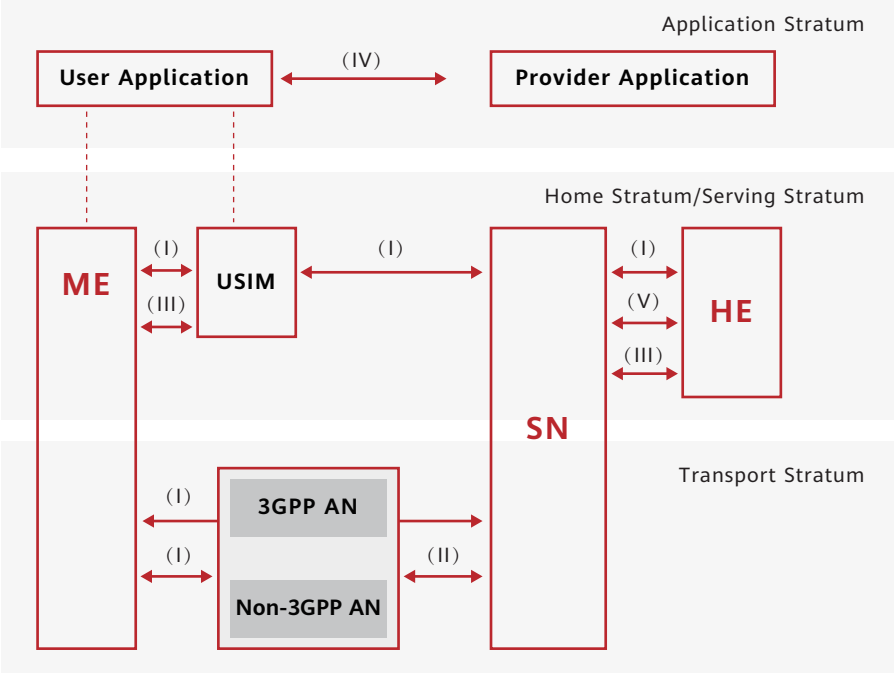
b)华为5G解决方案的安全架构

5G安全架构是4G的延续。2019年5月29日，华为发布了《5G安全白皮书》阐述了5G解决方案的安全架构。[16]

目前3GPP SA3 已制定完成5G R15 的安全标准，正在制定5G R16 安全标准。在3GPP，安全标准的制定和架构、无线等标准的制定保持一致的进度，以确保5G 标准的推进在各个技术层面进度一致。R15 已完成安全基础架构的定义，完整定义eMBB 场景的安全标准，包含了SA（独立组网）与NSA（非独立组网）两种组网架构；R16，R17 将基于R15 安全基础架构，面向mMTC 和uRLLC 场景进行安全优化。

移动网络按照分层分域的原则来设计网络的安全架构，5G 的安全架构主要分成如下几个域：

[16]《5G安全白皮书》，
http://www-file.huawei.com/-/media/CORPORATE/PDF/white%20paper/2019/huawei-5g-security-white-paper-4th-cn.pdf



网络接入安全 (I)、网络域安全 (II)、用户域安全 (III)、应用域安全 (IV)、服务域安全 (V) 。

- 网络接入安全 (I): 一组安全特性，用于使 UE 安全的通过网络进行认证和业务接入，包括 3GPP 接入和非 3GPP 接入，特别是保护对空中接口的攻击。它包括从服务网络到接入网络的安全上下文的传递，以实现接入安全性。具体的安全机制包括双向接入认证、传输加密和完整性保护等。

- 网络域安全（II）：一组安全特性，用于使网络节点能够安全地交换信令数据、用户面数据。网络域安全定义了接入网和核心网之间接口的安全特性，以及服务网络到归属网络之间接口的安全特性。与 4G 一样，5G 接入网和核心网分离，边界清晰，接入网和核心网之间的接口可采用安全机制如 IPSec 等，实现安全分离和安全防护。

- 用户域安全（III）：一组安全特性，用于让用户安全地访问移动设备。终端内部通过如 PIN 码等安全机制来保护终端和 USIM 卡之间的安全。

- 应用域安全（IV）：一组安全特性，用于使用户域（终端）的应用和提供者域（应用服务器）中的应用能够安全的交换消息。本域的安全机制对整个移动网络是透明的，需应用提供商进行保障。

- 服务域安全（V）：一组安全特性，用于使 SBA 架构的网络功能能够在服务网络域内以及在服务网络域和其他网络域间安全地通信。这些特性包括网络功能注册、发现、授权安全等方面，以及保护服务化接口。这是 5G 新增的安全域。5G 核心网使用 SBA 架构，需要相应的安全机制保证 5G 核心网 SBA 网络功能之间的安

全。该域主要安全机制包括 TLS（传输层安全性协议）、OAUTH（开放式授权）等。

- 安全可视化和可配置（VI）：一组安全特性，用于使用户获知安全特性是否在运作中。【注：安全可视化和可配置在图中不可见】

与 4G 一样，5G 安全架构又可分为应用层（Application Stratum）、归属层（Home Stratum）、服务层（Serving Stratum）与传输层（Transport Stratum），这四层间是安全隔离的：

- 传输层：最底层的传输层安全敏感度较低，包含终端部分功能、全部的基站功能和部分的核心网功能如 UPF，基站和这部分的核心网功能不接触用户敏感数据，如用户永久标识，用户的根密钥等，仅仅管理密钥架构中的低层密钥，如用户接入密钥。低层密钥可以根据归属与服务层的高层密钥进行推导、替换和更新，而低层密钥不能推倒出高层密钥。

- 服务层：服务层安全敏感度略高，包括运营商的服务网络的部分核心网功能如 AMF（接入和移动性管理功能）、

NRF（网络存储库功能）、SEPP（安全边缘保护代理）、NEF（网络开放功能）等。这部分的核心网功能不接触用户的根密钥，仅管理密钥架构中的中层衍生密钥，如 AMF 密钥。中层衍生密钥可以根据归属层的高层密钥进行推导、替换和更新，而中层密钥不能推导出高层密钥。这一层的安全架构不涉及基站。

- 归属层：归属层安全敏感度较高，包含终端的 USIM 卡和运营商的归属网络的核心网 AUSF（鉴定服务功能）、UDM 功能，因此包含的数据有用户敏感数据如用户永久标识，用户的根密钥和高层密钥等。这一层的安全架构不涉及基站和核心网的其他部分功能。

- 应用层：应用层和业务提供商强相关，和运营商网络弱相关。和 4G 一样，对安全性要求较高的业务，除了传输安全保障之外，应用层也要做端到端地安全保护；例如移动支付，即使 4G/ 5G 网络保障了传输的安全，应用层也要做端到端地安全保障，确保资金转移不出现问题。

5G 网络继承了 4G 网络分层分域的安全架构，接入网和核心网的边界清晰，通过标准协议互联，支持异厂商互联互通，并且有基于标准的安全保护机制。对于监管者来说，需要从这

四层去看护网络安全风险。对业务提供商来说，需要从应用层端到端地管理网络安全风险。对运营商来说，需要从下面三层去管理网络安全风险。对设备提供商来说，主要需要关注底层网络设备安全风险。全行业应当在标准架构下共同致力于解决业务、架构、技术的安全风险。

根据 Ovum 发布的《5G 的事实》白皮书[17]，外界担心核心网和接入网在架构上的分离程度将弱化，这意味着核心网和接入网之间的接口会变得模糊、不稳定。实际上，我们有充分理由认为这些问题并不会出现。

- 首先，从技术上来说，核心网 / 接入网分离是 5G 架构标准的基本原则，在前几代移动技术中也有体现。倘若核心网和接入网没有分离，标准制定可能更加复杂和困难，阻碍创新速度。任何弱化核心网 / 接入网分离的技术都是极具颠覆性的，不论是设备厂商还是运营商都不会支持这种技术。实际上，5G 标准已经实现了核心网 / 接入网分离，任何打破这种分离状态的移动技术都不能称为 5G 技术，也无法和 5G 网络兼容（也无法和上一代网络技术兼容）。

[17]《5G的事实》，https://huaweihub.com.au/the-facts-on-5g/

- 更重要的是，如果核心网 / 接入网分离被弱化，运营商和设备厂商都将面临挑战。

  I. 如果核心网 / 接入网分离不清晰，移动运营商就难以 采用多厂商解决方案，无法以模块化方式轻松地连接各厂商的核心和接入设备。运营商将被迫使用单一厂商的设备，并一直依赖该供应商。这会减少该设备厂商面临的竞争压力，导致运营商为此付出更高的成本。

  II. 设备厂商似乎愿意看到核心网 / 接入网分离被弱化，但他们依然会竞相提供支撑核心网 / 接入网分离的标准化 5G 解决方案。如果某个技术无法充分利用核心网 / 接入网分离带来的优势，该技术就不具备市场竞争力，无法产生规模经济效应。即便是某个运营商要求定制化的非标准解决方案，但方案部署带来的额外成本无法分摊到整个行业，导致解决方案的价格高昂。任何一家理性的设备厂商都不会采取这个做法。

- 再者，供应商多元化策略是保障网络安全的最佳途径，有助于提高网络韧性，避免单点攻击造成整网瘫痪。支撑这个理由的论点如下：

I. 减少对单一供应商的过度依赖，强化竞争。首先，网络不应该只依赖一个供应商，因为这会影响网络的韧性。

II. 其次，通过要求移动网络运营商使用多厂商设备，这将强化供应商之间的竞争，迫使他们提高安全标准。这么做不仅可以全面提高网络安全标准，还可以落实更严格的监管并实施这些标准。

c) 华为 IoT 解决方案的安全架构

2018 年 10 月 23 日，华为在第四届全球物联网解决方案大会期间发布了《物联网安全技术白皮书》[18]，其中阐述了华为 IoT 解决方案的 3T+1M 安全架构。

物联网安全涉及低功耗广域网络（LPWA）、车联网、工业物联网、可穿戴等领域。与传统网络安全威胁相比，在物联网万物互连互通的生态环境中，海量的物联网终端生成并使用海量的数据，管道为这些数据提供高并发的安全通信保障，云端和物联网平台支撑着丰富的物联网应用，这些支撑的系统和应用有可能沦为潜在恶意攻击的目标。

“3T+1M 安全架构”聚焦端、管、云和平台的安全特性

[18]《物联网安全技术白皮书》，https://www.huawei.com/cn/press-events/news/2018/10/huawei-iot-security-whitepaper-2018

的组合协同，应对物联网基础架构中的感知层、网络层和应用层的安全威胁；同时立足于平台安全和云端安全的基础上，依托传统电信网络安全保障能力优势，提供物联网安全态势感知与分析检测；联合生态合作伙伴，共同致力于解决物联网的安全威胁与挑战。基于不同行业应用对 IoT 云管端的安全需求的分析，尤其是具有行业特点的差异化安全需求，促进“3T+1M 安全架构”的架构不断演进和技术创新。在创新中构筑安全，在演进中满足多元化的应用需求。

T: 安全技术族，M：安全运维与管理

3T+1M 物联网安全解决方案，核心在于基于 IoT 应用场景（车联网、LPWA 应用、工业物联网等）安全威胁，构建起 IoT 终端防御、管道保障、云端保护三个 IoT 安全技术族（Technologies）和端到端安全运维与管理 (Management)，特别是针对 IoT 安全属性的关键安全技术和方案族，以此满足国家和区域法律法规、行业标准等合规要求，构建起物联网安全端到端纵深防御体系。这其中包括：

1. 物联网终端防御技术族（1T）：针对 IoT 不同应用场景终端，提供与其能力相匹配、端云协同的关键安全技术族，对于弱终端（如 LPWA 智能抄表、共享单车锁等）需满足基本安全能力，如传输安全 DTLS 或 DLTS+、终端可信 DICE、FOTA 升级、安全启动等，而对于强终端（比如车联网 T-Box、OBU 等），还进一步需满足安全证书管理、入侵检测、加密认证、TPM 等。

2. 物联网管道保障技术族（1T）：IoT 管道安全最核心的关键能力在于恶意行为检测与隔离，特别是针对物联网终端（比如车联网 T-Box、LPWA 智能路灯等）异常行为（比如流量异常、上报频次异常等）进行快速检测和隔离。同时针对不同场景增强物联网管道安全能力，

比如针对 NB-IoT 场景增强防 DDoS 攻击和防信令风暴能力，而针对车联网 C-ITS 则需重点构建车路网协同通信可信能力等。

3. 物联网平台保护技术族（1T）：重点构筑 IoT 平台和云端提供基于大数据安全分析的态势感知、车联网安全分析感知能力，以及更好的聚焦平台的 IoT 数据安全与隐私保护，为客户提供可配置的云安全保障能力。

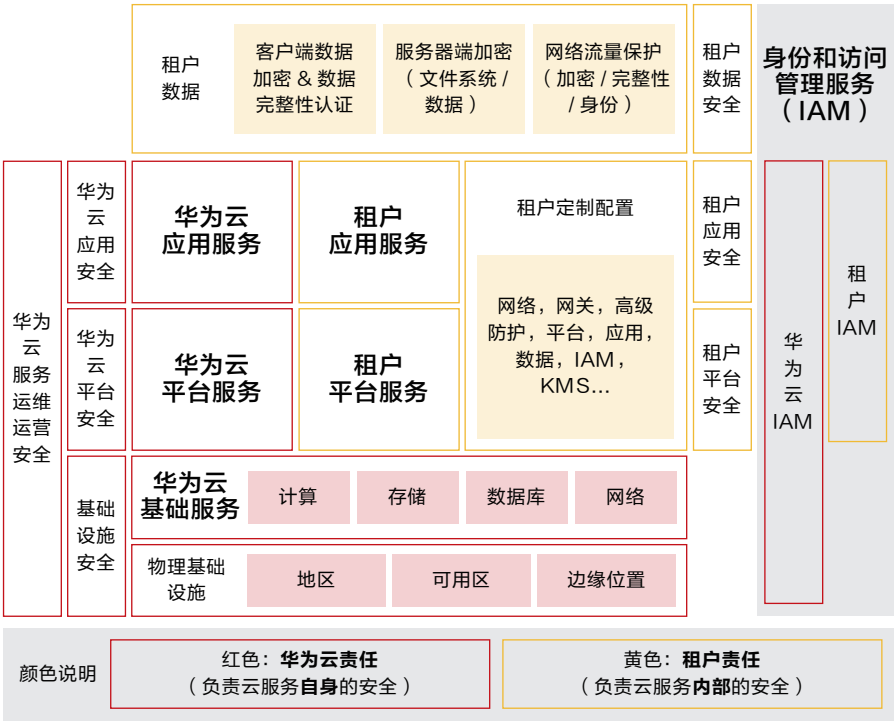
4. 物联网安全运维和管理（1M）：重点在于构建端到端的安全运维工具和制定安全运维操作规范和流程，提高安全运维人员和测试人员效率，提升整个 IoT 安全体系事前预防预警、事中检测分析和事后处理等能力，包括安全巡检工具、定期物联网安全评估、自动化终端和应用安全检测工具、威胁情报库等。

需要强调的是，3T+1M 架构中 IoT 安全关键技术能力构建，虽然侧重点有所不同，有些侧重于端侧，有些侧重于管道或者云端，但都不是孤点的防御，需要通过端、管、云、运维相互协同，构筑整体的安全防御体系。特别是物联网终端受限于资源和应用场景，在构建防御能力上，需要通过云端或管道来进行协同，比如终端可信、恶意终端检测、

DTLS+ 等。

d) 华为云的安全架构

2017 年 9 月，华为发布了《华为云安全白皮书》[19]，其中阐述了按业界常规做法定义的华为云服务安全责任共担模型，如下图：



[19]《华为云安全白皮书》，https://res-static1.huaweicloud.com/content/dam/cloudbu-site/archive/china/zh-cn/securecenter/security_doc/Security_cn_201709.pdf

如上图所示，华为云的主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

租户的主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和 IAM 层的各项安全防护措施的定制配置，运维运营安全，以及用户身份的有效管理。

e) 智能终端 EMUI 的安全架构

华为非常重视移动智能终端的安全性，2018 年 11 月 30 日，华为发布了《EMUI 9.0 安全技术白皮书》，系统地描述 EMUI（Emotion UI）提供的安全保护方案。

安全是系统化的工程。EMUI 提供从硬件、系统、应用

到云端的端到端安全保护（如下图所示），包括硬件芯片、系统内核、数据、应用、网络、支付、云服务 和设备管理的安全以保护。

EMUI 从底层硬件芯片开始提供安全启动机制来保证 EMUI ROM 镜像不会被篡 改，ROM 镜像必须经过签名校验才能在设备上正常运行，保证了设备 Bootloader、Recovery 以及 Kernel 镜像的启动安全，同时 Android 原生系统提供 Verified Boot 保证 Android 系统启动过程的安

全性，防止启动过程中对 Android 的篡改和恶意代码植入，从而确保系统从硬件芯片到 Android 启动的安全。

为保证数据安全，用户数据基于硬件提供的 HUK（Hardware Unique Key，设备 唯一密钥）和用户的锁屏密码进行加密，不同的应用之间的数据文件存储在应用 自己的目录，其它应用无法访问。在设备回收或恢复出厂设置时，提供安全擦除 功能来永久清除数据，避免数据被非法恢复。同时 EMUI 与云服务的结合，帮助 用户进行数据的备份和同步以保证数据的安全。

为保证应用安全，除了 Android 安全沙箱和权限管理等安全机制外，EMUI 通过 预置手机管家提供病毒查杀、骚扰拦截、流量管理、通知管理等功能，安装应用时会自动检测应用是否包含病毒木马，并对应用提供细粒度的权限管理、流量管理和通知管理功能。

简言之，华为能提供安全的产品和解决方案。美国 Cigital 公司从 2013 年开始每年持续对华为产品的安全、设计、工程和测试管理进行 BSIMM 评估，共测试了安全治理、安全设计、安全编码和安全测试 12 个安全实践项目。华为在 12 项安全实践中均高于业界平均水平，其中 9 项安全实

践达到最高级别。

2019 年 6 月 17 日，美国著名未来学家乔治 . 吉尔德在与华为创始人任正非、麻省理工学院媒体实验室联合创始人尼古拉斯 · 尼葛洛庞帝教授的咖啡对话中谈到：“ 我希望能够帮助重新打造互联网的架构，解决互联网面临的重大安全问题。这是个华为可以解决的技术问题，而不是一个政治问题。”[20] 让技术回归技术，必将解决安全问题。

[20] 美国学者与任正非的咖啡对话，2019 年 6 月 17 日，http://xinsheng.huawei.com/cn/index.php?app=group&mod=Bbs&act=detail&tid=4332625

七、秉承独立的商业精神

华为坚持独立的商业精神，全力为客户网络和业务的安全运营提供保障支持。

1.100% 由员工持有的民营企业

华为是一家 100% 由员工持有的民营企业，没有任何政府部门及其它第三方机构持有公司股权、干涉公司经营、或影响公司决策。虽然华为不是上市公司，但我们一直参照上市公司的标准和实践，坚持每年发布公司年报，年报中的财务报表经独立审计师毕马威（KPMG）审计，让外界了解华为业务的真实性、独立性和财务透明性。

2. 中国政府没有对华为业务或产品安全进行干涉

最近，围绕中国情报法的辩论非常激烈。有些政治家宣称，中国法律允许政府强迫企业为其收集情报。这并不是事实。中国政府已经做过澄清，独立的法律教授及知名的国际律师事务所也清晰表达了他们的观点：企业的协助支持义务的前提必须是“ 依法 ”，中国没有任何一部法律赋予国家情报机关权力要求电信设备制造企业收集情报信息、植入后门

或者中断客户网络。中国政府没有对华为业务或产品安全进行干涉。如果我们真的收到来自任一国家或组织的此类强迫性要求，我们会直接加以拒绝。

我们在这一点上的态度是明确的：如果我们的独立性、产品安全、客户网络或其他国家的国家安全受到安全威胁，我们宁愿关闭公司，也不愿违背我们的原则。如果签署“无后门、无间谍”协议能让我们的全球客户或政府更放心，我们愿意签署这样的协议。

3. 为客户服务是华为存在的唯一理由

无论是面临自然灾害、社会冲突、还是网络攻击，我们都全力与客户共同维护网络的稳定、可靠、安全运行。在汶川大地震、福岛核泄漏期间，华为人冒着生命危险竭力抢修通信网络，确保网络服务可用性。

在过去 30 年里，华为在 170 多个国家和地区运营，服务全球 30 多亿人，没有重大网络瘫痪，也没有恶性网络安全事故。华为从未做过任何危及客户网络或设备安全的事情，也没有任何证据表明华为曾经这么做过。

八、开放透明的合作

1. 通过 SAB 委员会加强与安全学者合作

2014 年 8 月，华为成立安全顾问委员会（SAB），每年聘请近十位全球顶级的安全与密码专家做顾问，指导华为更好地从事安全研究和安全工程实践。每年夏末秋初，华为都会在欧洲召开 SAB 研讨会，邀请顾问和其他一些在网络安全研究或实践上卓有成效的学者和业界专家前来演讲，并与华为内部的安全专家与技术主管进行深入的交流，共同讨论安全大趋势、热点安全技术和华为所遇到的安全技术挑战。所涉及的主要安全技术方向包括：5G 安全、IoT 安全、AI 安全、云安全、区块链安全、硬件安全、未来网络的安全、后量子密码等。基于此，华为与这些顾问和专家还进行了广泛的安全技术合作。

为了普及业界对网络安全的正确认知，顾问们也撰写、发表安全文章。SAB 委员、英国伯明翰大学的 Mark Ryan 教授在 The Birmingham Brief 上发表了名为《互联互通是解决华为困局的方案》的文章，提出开放统一的标准是解决安全问题的核心要素：“要避免技术锁定和垄断问题，就

需要建立开放的国际标准，鼓励大量组织和个人开发满足各自需求的硬件和软件。开放、无歧义的标准能保障产品兼容性，任何客户都不会被迫向某个厂商购买设备，还能任意切换不同厂商的设备，切换也不会影响设备兼容性。作为 5G 标准的协调组织，3GPP 将技术规格提供给所有人查看和实施。对于部分受专利保护的技术，3GPP 要求基于公平、合理和无歧视的原则进行专利许可授权。”[21]

2. 英国网络安全评估中心提供世界级的安全专业和技术保障

2010 年 11 月 24 日，华为与英国政府成立网络安全评估中心（HCSEC），对在英国现网部署的华为产品进行独立的安全评估，英国政府提出改进思路和建议。

在运作机制上，HCSEC 独立执行测试，英国国家网络安全中心（NCSC）每年委托安永对 HCSEC 的独立运作进行审计，监管委员会（OB）对 HCSEC 的独立性、有效性和能力进行监管。HCSEC 具有选择和使用测试工具、环

[21] Mark Ryan，《互联互通是解决华为困局的方案》，2019 年 5 月 20 日，https://www.birmingham.ac.uk/news/thebirminghambrief/items/2019/05/interoperability-is-the-solution-to-the-huawei-dilemma.aspx

境、方式、过程、时间等全方位的自由，且并不会告知 HCSEC 以外的华为其他组织和人员。

英国对华为采取的 可以说是全世界最强硬、最严厉的监督机制。NCSC 继续认为英国缓解策略（包括 HCSEC 执行技术工作和 OB 提供保证两部分）是管理华为参与英国电信业务而带来的风险的最佳方式。在 HCSEC OB 2018 年年度报告中，监管委员会称赞 HCSEC 为“ 世界级 ”的网络安全专业和技术保障：“ 根据当前阶段英国的华为保障框架所需足够的范围和质量，很显然 HCSEC 能够继续提供其独特、世界一流的网络安全专业技能和技术保障。”[22]

在全球主流电信设备供应商中，华为率先主动、自愿地接受了这种最严苛的源代码级监管审查，体现出华为在公开、透明方面做出的积极努力。也希望政策制定者鼓励更多厂家开放、透明地与监管机构合作、识别和削减风险，主动披露自己的不足和改进计划。

---

[22] 华为网络安全认证中心（HCSEC）监管委员会2018年年度报告（2018年7月），https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf

3. 德国波恩安全创新实验室探索新技术的安全标准与验证

2018 年 11 月 16 日，华为在德国波恩成立安全创新实验室，德国联邦信息安全办公室 (BSI) 主席 Arne Sch□n-bohm(阿恩 – 舒博姆) 先生与华为副董事长胡厚崑先生共同为该实验室揭牌。该实验室旨在提供一个平台加强现有技术的安全性，并探讨保障未来技术安全的创新理念，并致力于对 ICT 安全认证和全球标准化做出贡献。在三个方面与监管机构、客户、合作伙伴和研究机构在内的众多德国利益相关方开放合作：

1. 新技术及安全挑战交流：持续沟通，共同理解新技术及其带来的网络安全风险，并开展前瞻性和创新性的合作。

2. 信任验证机制探索与实践：通过技术合作，验证现有产品或者新技术领域的合作成果。

3. 安全标准与认证合作：探讨和推动行业统一的安全标准与规范，提升行业的安全管理水平。

4. 比利时布鲁塞尔网络安全透明中心致力于可信的数字环境

2019 年 3 月 5 日，华为在布鲁塞尔成立网络安全透明中心。其职能包括三个方面：

首先，展示华为端到端的网络安全实践，从战略、供应链，到研发、产品和解决方案，可以体验到华为在 5G、IoT 和云等领域的产品和解决方案的安全性。

其次，促进华为与关键利益相关方之间网络安全战略和端到端网络安全实践的交流，华为与业界合作伙伴一起推动安全标准和验证机制的建立，以及全行业网络安全方面的创新。

最后，也将为我们的客户提供产品安全测试和验证的平台。

我们欢迎监管机构、标准组织和华为客户利用这一平台，在安全标准、验证和安全创新方面进行更为密切的合作。通过一起努力，我们就可以提升整个价值链的安全性，帮助建立基于验证的互信。

九、华为网络安全宣言

网络安全：我们做得更多

安全的复杂性超乎大多数人的想象。

对华为而言，安全始于我们的价值观和信念。

今天，互联的数字世界使人们从技术上广泛受益。从酷热难耐的热带地区到冰冷刺骨的极寒地区，华为人的足迹遍布全球各个角落，只为实现我们联接世界的愿景。

我们相信，安全意味着要确保网络在任何情况下都能正常运行。不论是面临飓风、地震、海啸甚至是战争，我们始终与客户坚守在一起。

安全不仅关乎比特和字节，也关乎人们的生活。不论环境条件是好是坏，我们都要确保网络随时可用。这意味着我们将网络安全置于商业利益之上。

技术很神奇，但技术也很复杂。技术发展不可仅凭一己之力，而是需要合作伙伴、全球供应链、行业与政府共同努力，才能让技术造福整个世界。

华为致力于通过各种方式保障网络安全。我们欢迎各方提供输入、观点和建议，促进我们全面改进，最终为我们的客户以及他们的客户带来更大福祉。今天，华为也许是全球最开放、最透明、接受审查最严格的公司。

我们将一如既往地把安全置于成本、进度和特性之上，把安全流程融入整个产品生命周期：从产品设计、开发到交付。

如果有需要去完成的安全标准和认证，我们就会去完成。

我们认为，如果安全没有保障，那么隐私将得不到保护，反之亦然。

华为永远不会做违法的事情。我们绝不伤害任何国家或个人，也不会接受任何恶意利用华为产品的要求。如果收到此类要求，我们宁可关闭公司，也不会执行。

华为致力于帮助客户最大化提升其资产价值。以客户为中心是我们坚守的核心理念，为此，我们不断加大投入来构建信任、提升能力、提高透明度并推动协作。

安全不仅仅意味着持续投入，安全是我们的价值观，是华为生存的基石。

我们努力在安全上做得更多，您也可以对我们有更多的期待。

十、关于华为

华为的产品与解决方案覆盖 170 多个国家和地区，服务于世界超过 30 亿人口。我们有 188,000 多名员工，8 万多名研发员工，占公司总人数 45%。华为 5G 在技术和商用上均处于业界领先，华为是目前行业内唯一能提供端到端 5G 全系统的设备厂商。截止 2019 年 8 月，华为已经获得 50 个 5G 商用合同，并与全球 50 多个商业伙伴签署 5G 合作协议。我们的 5G 商用基站发货数量也已经超过 20 万个，在行业内遥遥领先。2019 年上半年，华为发布搭载自研 5G 芯片的 5G 智能手机，并将在 2019 年下半年实现规模上市。

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。华为每年将超过 10% 以上的销售收入投入到研发，2018 年研发费用支出为折合 148 亿美元，约占全年收入的 14.1%。近十年累计投入的研发费用超过 700 亿美元。面向未来，华为每年研发投入将达到 150-200 亿美元。

截至 2018 年 12 月 31 日，在全球获得授权专利 87,805 件。联合国下属的世界知识产权组织（WIPO）公

布数据称，2018 年度华为向该机构提交了 5,405 份专利申请，在全球所有企业中排名第一。华为投入 5G 技术研究已超过 10 年之久，累计向 ETSI 声明 2570 族 5G 标准 必要专利。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。

华为通过与 25 家领先客户的 NetCity 联合创新，全面升级意图驱动的网络解决方案。约 46.4% 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。2018 年，我们对 2778 家涉及网络安全的主流供应商进行了风险评估和跟踪管理，与 582 家涉及隐私保护的供应商签署了数据保护协议（DPA）并作了隐私保护尽职调查。

2019 年华为智能手机达到 1 亿台的出货目标只用了 149 天，比 2018 年提前了近两个月。

华为支持主流国际标准，并为这些标准的制定积极做出贡献，加入 400 多个标准组织、产业联盟和开源社区，担任 400 多个重要职位，在 3GPP、IIC、IEEE-SA、BBF、ETSI、TMF、WFA、WWRF、CNCF、OpenStack、LFN、LFDL、Linaro、IFAA、CCSA、AII、CUVA 和 VRIF 等组织担任董事会或执行委员会成员。2018 年全年提

交标准提案超过 5000 篇，累计提交近 60000 篇。

华为持续投资“ 沃土计划 ”，全球注册开发者近 30 万人，增长超过 150%，新增认证联合方案近 600 个、新增认证开发人员 1,700 多人。

华为“ 未来种子 ”项目十周年，累计共有 108 个国家和地区的 4,700 多名学生来到华为参观学习。华为 ICT 学院已覆盖 60 多个国家和地区的 557 所高校。

截至 2018 年 12 月 31 日，公司的员工持股计划参与人数为 96,768 人。员工持股计划将公司的长远发展和员工的个人贡献有机地结合在一起，形成了长远的共同奋斗、分享机制。这让我们能够有长远的眼光，保证在风险、激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。

华为技术有限公司
深圳龙岗区坂田华为基地
电话：+86 755 28780808
邮编：518129
www.huawei.com

商标声明
HUAWEI，HUAWEI，是华为技术有限公司商标或者注册商标，在本手册中以及本手册描述的产品中，出现的其它商标，产品名称，服务名称以及公司名称，由其各自的所有人拥有。

免责声明
本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺，华为不对您在本文档基础上做出的任何行为承担责任。华为可能不经通知修改上述信息，恕不另行通知。

版权所有© 华为技术有限公司 2019。保留一切权利。
非经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。