# 《可信网络白皮书》聚合众智　展现领先网络安全理念和实践

2023年，随着国家和企业数字化转型不断深入，网络安全面临的形势将更加复杂，威胁场景和技术的升级势必将驱动整个安全行业快速向前发展。特别是对于国之重器——运营商网络而言，如何恰当应对安全威胁更是重中之重和当务之急。近日，中国联通、中国信通院和华为三方在北京正式发布《可信网络白皮书》（以下简称《白皮书》），首次发布了可信网络的定义、目标架构、能力要求及发展思路等内容，为我国打造可信网络、护航数字经济安全发展、实现中国式现代化提供了坚实基础。

“链长”责无旁贷 积极发挥主体支撑和龙头带动作用

互联网的快速发展和普及，给我们带来许多便利的同时，也暴露了许多安全隐患和风险。

没有网络安全就没有国家安全，网络的安全可信已经上升为国家战略，全球各国都在通过立法、安全准入认证标准以及新的技术重新构建网络防御体系，在国家层面加强整体网络安全能力建设。我国对网络安全一直高度重视，通过不断完善立法加强监管保障关键基础设施的安全。随着《网络安全法》《数据安全法》《关键信息基础设施安全保护条例》的相继颁布实施，我国网络安全法律体系处于逐步完善阶段，相关配套的标准、认证体系等也正在逐步推进中，这需要整个产业链，包括运营商、设备商、科研机构等，一起努力构建系统化网络安全能力，共同构筑国家关键基础设施安全底座。

其中，电信运营商基础网络作为国家数字基础设施的“大动脉”，是支撑数字中国战略落地的关键环节。保障基础网络安全可信和稳定可靠，是大家的核心职责。

作为网络安全现代产业链“链长”，一年来，中国联通积极发挥主体支撑和龙头带动作用，努力做好产业基础能力提升支撑者、产业发展方向引领者和产业协同合作组织者，采取了多项关键行动，全力保障网络安全产业健康、合理、有序发展，包括与行业内的专家和学者深入开展了研究和探讨，创造性提出了可信网络的概念和产业发展思路。

本次《白皮书》发布，正是聚焦未来网络安全的最新趋势、挑战，提出了业界领先的网络安全理念以及创新实践。

管理模式需与时俱进 安全性、可靠性和韧性要全面升级

随着企业数字化转型的发展，业务向云化、物联化、无线化的方向发展，业务边界、业务接入类型、接入终端类型、数据的流转等都发生了变化。网络也从以IPv4为基础的消费互联网向以IPv6/IPv6+为基础的生产互联网升级，以满足多元化应用承载需求，释放产业新效能。

在网络和业务急剧变化的同时，目前电信网络沿用的CT安全标准相对滞后，CT安全产业仍套用IT管理模式，场景适配弱，不能满足快速发展的业务安全保障需求。《白皮书》认为，建立可信网络一定要从网络安全性、可靠性、韧性三个方面进行升级。

首先，在网络安全性上要从单点防御转变为立体防御，要从网络设备、网络自身和网络管控三层的防御体系入手，从边界防御升级到纵深防御，构建网络的内生安全，全面提升网络的抗攻击能力。

其次，在网络可靠性方面，从业务多级保护能力入手，在此基础上叠加故障预测、隐患提前处置的能力，智能感知网络以及设备的隐患，防患于未然，避免风险演变为故障。

最后，在网络韧性上要提升网络的承载能力以及快速业务恢复能力，在遭受恶意入侵或资源过载的情况下能够使业务正常运行，通过最小模块的处置对网络系统进行秒级业务恢复。

“可信网络就是要通过构建可信网络体系架构，不断提升网络的安全性、可靠性以及韧性，实现网络攻不瘫、威胁不扩散、业务不受损，无论网络环境如何变化，都能确保业务的连续和稳定。”业内人士总结说。

应对安全新挑战 可信网络任重道远

网络业务的变化带来了安全的新挑战。

首先，网络业务从传统的业务结构演变成云网边端融合的方式，网络边界延伸到基于云网边端的新型基础设施，传统的网络边界不存在，对传统的安全模式造成了一定影响。

其次，网络接入方式的多样化、用户的多样化、设备的多样化、连接的多样化造成网络安全复杂度增加。

最后，数据在用户、设备、业务平台之间持续流动，也带来新的风险。其中，对设备传统授权模式，包括静态的授权模式，颗粒度较粗都会导致越权操作风险持续提高，数据泄露风险加大。

可信网络是将安全可信技术融入网络基础设施解决方案中，构筑网络的内生安全能力，实现数据实体信任关系的传递和验证、网络行为的持续监测和管控、业务异常的溯源和处理，从而实现结果可预期的网络。

《白皮书》制定了设备可信、网络可信、管控可信的“可信网络”总体架构，明确了“可信网络”发展的总体目标。

设备可信：设备可信是保证网络基础设施安全可信的基础，通过软硬件等关键能力的构建，实现构建内生安全全生命周期保护，软件“零”篡改、数据“零”泄密、安全态势自感知。

网络可信：网络可信是信任的保障，以设备可信为基础，通过网络关键能力的构建，实现路由、业务、协议全方位网络可信，路由“零”劫持、协议“零”仿冒、网络攻击主动识别。

管控可信：管控可信是设备及网络安全的大脑，通过管控关键能力的构建，实现网安一体化防护、全网监测、联防联控，操作“零”误配、威胁处置自闭环。

最后，关于如何推进可信网络的演进，《白皮书》认为可以从“定架构、推标准、建体系、促应用”四个方面推进，希望通过技术创新、标准体系、实践部署、产业生态四方面，构筑整个核心网络体系。

当前产业界以及学术界已经开始认识到基础设施网络安全的重要性和价值，并开展了积极有益的探索，可信网络安全模型作为一种全新的安全防护模型，经过多年的实践已经从理念走向了实践。此次三方携手发布《白皮书》，将极大提升运营商网络空间创新能力，实现更广范围、更深程度、更高水平发展。

人民邮电报2023-07-25