Digital trust is built on standards and verifiable facts

Trust needs to be based on facts. Facts must be verifiable, and verification must be based on common standards. Huawei believes that this is an effective model for building trust in the digital era, writes Deputy Chairman Ken Hu.

We are getting into a digital world very fast, and we all agree that trust is the foundation for a healthy digital environment. But as technology evolves, it's more difficult to build that trust.

Right now, Huawei sees that there are four main challenges to building trust:

1. **Fast-developing digital technology has brought many new security challenges.** For example, traditional telco networks have evolved from closed to Internet-based networks, and more and more digital content and services are migrating to cloud data centers. As more devices go online, and our smartphones become more powerful, networks have much greater attack surfaces than ever before.

2. As a global community, **we lack a common and unified understanding of cyber security.** Governments and business communities all talk about the importance of cyber security. However, the fact is that both the public and private sectors lack a basic common understanding of this issue. As a result, different stakeholders have different expectations, and there is no alignment of responsibilities.

3. As a whole, **the industry lacks a unified set of technical standards for security,** as well as systems for verification. This is complicated by globalisation of the value chain. Digital products include components from many different countries, with many different standards, or no standards at all. There is an urgent need to invest in security standards and verification systems at the national level, as well as professional resources and skills.

4. The fourth challenge is **governance.** In some countries, cyber security

management lacks legislative support, and cyber security enforcement is not mature.

These are all real challenges, and we fully understand the cyber security concerns that people have in an increasingly digital world. Cyber security is a challenge we all share. To address these challenges, I believe that mutual understanding is the starting point. To build a trustworthy environment, we need to work together.

ABC principle

At Huawei, we have the ABC principle for security:

- **A**ssume nothing.
- **B**elieve nobody.
- **C**heck everything.

Both trust and distrust should be based on facts, not feelings, not speculation, and not baseless rumour. We believe that facts must be verifiable, and verification must be based on standards.

So, to start with, we need to work together on unified standards. Based on a common set of standards, technical verification and legal verification can lay the foundation for building trust. This must be a collaborative effort, because no single vendor, government, or telco operator can do it alone.

Secondly, we need to work together to clarify and align our responsibilities. This includes all stakeholders: regulators, standards organisations, telcos, and technology providers.

For technology providers like Huawei, our responsibility is to comply fully with standards. But that is not enough. Security must be embraced as a greater social responsibility. That means embedding trust in all end-to-end processes - and enhancing security through innovation and corporate culture.

For telco carriers, their responsibility is to ensure the cyber resilience of their own networks. Following industry standards, telco carriers need to build robust processes to identify cyber security risks. They need to develop risk mitigation plans and protect customer data.

Finally, government and standards bodies need to work with all stakeholders on standards development. This is our shared responsibility. These efforts should focus on a holistic approach, including security standards, security verification mechanisms, and enforcement.

EU’s GDPR the gold standard for privacy protection

Europe has strong experience in driving unified standards and regulation. The EU’s General Data Protection Regulation (GDPR) is a shining example of this. It sets clear standards, defines responsibilities for all parties, and applies equally to all companies operating in Europe.

As a result, GDPR has become the gold standard for privacy protection around the world. We believe that European regulators can also lead the way on similar mechanisms for cyber security. Right now, for example, the GSMA is making great progress with their NESAS security assurance scheme. We believe that all stakeholders should get behind this framework. Ultimately, the standards we adopt must be verifiable for all technology providers and all carriers.

An open, digital, and prosperous Europe requires a secure and trustworthy digital environment that meets the challenges of today and tomorrow. To lay the foundation for a trustworthy digital environment, both now and in the future, transparency, integrity, and accountability are essential.

Huawei's Cyber Security Transparency Centre

On 5 March, we opened the Huawei Cyber Security Transparency Centre in Brussels to help build that environment. This centre will provide a platform to enhance communication and joint innovation with all stakeholders. It will also provide a technical verification and evaluation platform for our customers.

Huawei strongly advocates independent and neutral third-party certification. Our Cyber Security Transparency Centre will support that. It will also give us a dedicated platform for constructive discussion, sharing best practices, and jointly addressing risks and challenges with our customers and partners. We welcome all regulators, standards organisations, and Huawei customers to use this platform to collaborate more closely on security standards, verification, and secure innovation. Together, we can improve security across the entire value chain and help build mutual, verifiable trust.

Security or nothing

Over the past 30 years, Huawei has served more than three billion people around the world. We support the stable operations of more than 1,500 carrier networks in over 170 countries and regions. In this time, we have maintained a solid track record in cyber security.

At Huawei, our promise is "Security or nothing." We take this responsibility very seriously. Cyber security is our top priority across product design, development, and lifecycle management, and it is embedded in all business processes.

Looking to the future, we want to do more. We will keep investing in our cyber security and technical capabilities. The Brussels center is an important milestone in that commitment.

We are also committed to working more closely with all stakeholders in Europe to build a system of trust based on objective facts and verification. This is the cornerstone of a secure digital environment for all.