

TRUSTWORTHINESS AND SECURITY - THE FOUNDATIONS OF EU 5G

As we start the New Year, and indeed the new decade, it is now we look to the future and Europe's digital destiny beyond 2020. 20 years ago, Huawei took its first steps into Europe by opening a Research and Development Centre in Sweden. Beyond 2020, with our shared values Europe and Huawei can work together to create a better digital future for everyone.

Trust is Key. To this end we have now published our Position Paper on EU 5G networks and the frameworks of trust we believe can mitigate security fears that surround the new 5G technologies.

In an interconnected world reliant on a global supply chain, trust can be based on the confidence that risk management is objective and transparent. As EU Commission President Ursula von der Leyen recently said: "new technologies will never mean new values."

The global supply chain depends on collaboration and fostering mutual trust. At Huawei, that trust and security starts with our values and beliefs. Companies should be treated fairly and equally. A competitive market benefits everyone and stimulates continued improvement of products and services through innovation, enhanced security and resilience. There should be no artificial barriers to industry collaboration in the development of unified standards for stronger cyber security for the connected, intelligent world of the future.

On 9th October 2019, the EU Network and Information Security (NIS) Cooperation Group published its EU coordinated risk assessment of the cybersecurity of 5G networks, which highlights shared technical and non-technical concerns. Our December 2019 position paper details existing and forthcoming measures and industry best practices to enhance the security of EU 5G networks. As 2020 begins, we are looking forward to agreement from the Cooperation Group on a toolbox of mitigation measures to address the identified cybersecurity risks.

No matter whether a technical risk or a non-technical risk, we must make

judgments and decisions based on facts.

But facts must be verifiable. Only in this way can we ensure that the results are fair and objective, and that each organization can select secure, trustworthy, and high-quality products. At the IEEE 5G summit in Manila on 17th September 2019, Rui Luis Aguiar, chair of the steering board for Networld2020, said that "suppliers should be judged based on facts, not intentions."

And, none other than Bill Gates has suggested that objectivity be used to identify security risks. He said that "all goods and services should be subject to an objective test."

5G will increasingly support essential services and involve greater cross-sector collaboration within the telecommunications industry between operators and suppliers, so building trust in cyberspace is a key requirement.

5G cyber security certification is a good way to establish a unified security assessment standard, provide guidance to all players in the 5G ecosystem and build consensus on 5G security. We therefore recommend continuing the work on 5G Security and Certification started with GSMA and 3GPP, in order to develop a common approach that is recognized throughout Europe.

However, trust goes beyond technical or operational measures and requires a conversation between countries. Cyber security is increasingly entangled with geopolitical issues, trade negotiations, and diplomatic dialogue between nations. Politically motivated suspicion does not address the challenges that enhancing cyber security bring.

Because of this, Huawei is ready to do whatever is necessary to build trust and meet the required security standards and regulations. Cyber security standards should be technology-neutral and equally applicable to all. After clear and unified cyber security standards are available, independent and comprehensive verification must be conducted based on the unified cyber security standards.

Continual collaboration across industry and between public and private sectors.

Devices and systems will increasingly become more intelligent and more

connected - both in government processes and cross-sector industrial applications, such as transport, finance, health, energy, agriculture, mining and manufacturing. We should work together to build these net-technologies in a way that ensures trust, security, safety and the protection of fundamental human rights.

We recommend that government regulators work closely with all relevant industries and partners to deliver a consistent set of regulations to address 5G security that allow operators to take responsibility for the overall implementation. We adhere to the principle of openness and transparency and are willing to explore strategic and fundamental solutions with stakeholders. An independent EU organization must enable greater accountability of cyber incidents.

Mutual trust for an Intelligent, Connected world.

To continue to build mutual trust for an Intelligent, Connected world, enable European technology leadership, and drive economic growth in the EU, Huawei is willing to allow its products to be inspected by authorized personnel from national governments in to ensure the security and integrity of our products and services. This shows our trust in Europe and its values. So for Europe's digital destiny beyond 2020 with shared values, let's continue to work together to create a better digital future for all.

Download our white paper
Huawei White Paper on 5G networks
File
[Huawei White Paper on 5G networks](#)