



20 YEARS  
OF CONNECTING  
EUROPE

## INSIGHTS

# IMPLEMENTING THE EU 5G SECURITY TOOLBOX

The EU Toolbox for 5G Security, adopted in January 2020, is a vital way to achieve timely and secure deployment of 5G networks. As a major contributor to 5G standards and connectivity 'made in Europe', Huawei is an essential part of this process.

## INVESTING IN A FUTUREPROOF EUROPE

Huawei is localising its production in and for Europe with a view to strengthening the bloc's digital sovereignty while improving transparency and maximising its economic contribution.



## COMMON GROUND, COMMON CHALLENGES

Huawei welcomed delivery of the EU 5G Security Toolbox, which provide much-needed common ground.

However, we believe a security approach based on labelling specific vendors as high risk has a number of inherent limitations:

- **Trust in vendors is continually built over time and regularly reviewed.** Creating a static security label in a fast-evolving context does not adequately address risks: A global supply chain, changing suppliers, technological and regulatory change mean that "trusted vendor" labels create a false sense of security.
- **The country of origin is not a relevant criterion for assessing risk.** Manufacturing, R&D and procurement are globalised. Determining risk based on the country of origin unfairly damages business reputation without appropriately addressing threats.
- **Targeting a vendor based on the country of origin may be illegal.** Determining risk in this way may result in discrimination and trade barriers, violating applicable WTO and EU law.

## A ZERO-TRUST APPROACH

To effectively upgrade the security of 5G networks, we need to address risk through a series of measurable and verifiable criteria:

- **Applying the zero-trust principle.** Taking into account the global nature of the supply chain, this approach means that all vendors are subject to the same strict standards and evaluations.
- **Using proven schemes and specifications to carry out these checks.** The European Commission should work towards a standards and evaluation scheme specifically designed for 5G. This should cover NESAS (Network Equipment Security Assurance Scheme) standards and the 3GPP-developed SCAS (SeCurity Assurance Specifications), which both involve independent auditing and evaluation.
- **Assessing vendors based on such processes and in line with WTO and EU rules.** Decisions on who is a risk must be based on concrete, transparent, non-discriminatory and proportionate criteria, applied coherently across the EU.

## CYBER SECURITY AT HUAWEI: AN IMPECCABLE TRACK RECORD

- ▶ **Not a single major security incident** in the last 30 years
- ▶ **Compliance with all national and international laws and regulations** from our 20-year operation in Europe
- ▶ **Key contributor to 5G security standards:** From a total of 1,609 proposals on 5G security, more than four out of ten of them are successfully accepted

Huawei EU press contacts:

Philip Herd  
+32 491 165 509

Jakub Hera-Adamowicz  
+32 499 641 839

Find out more: [www.huawei.eu](http://www.huawei.eu)

Published September 2020