

Huawei Romania Online Press Conference

August 12, 2020



Huawei: Leading Provider of ICT Infrastructure and Smart Devices

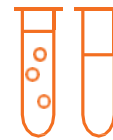


Bring digital to every person, home and organization for a fully connected, intelligent world.



194,000

Employees



96,000+

R&D employees



170+

Countries and
regions



49

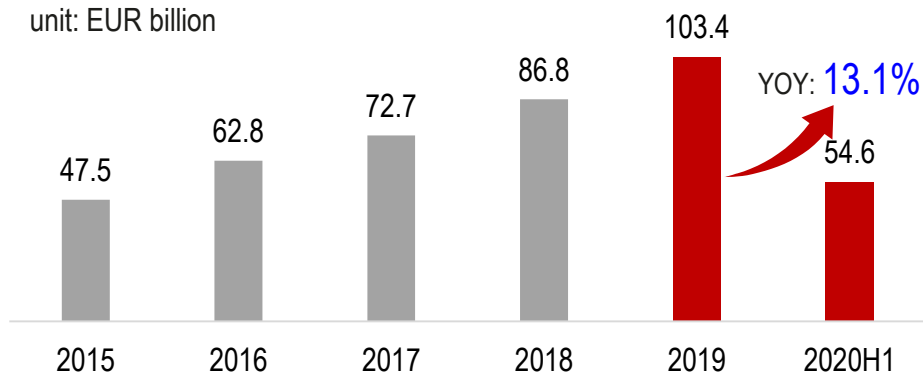
on Global 500

Huawei: Robust Growth and Sustained Investment for the Future

13.1% Sales Revenue Increase in 2020H1

YoY: 19.1% in 2019, CAGR: 21%

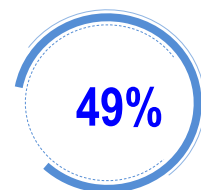
unit: EUR billion



Sustained Investment on R&D: 72.2Bn EUR in 10 Years (≈85Bn USD)



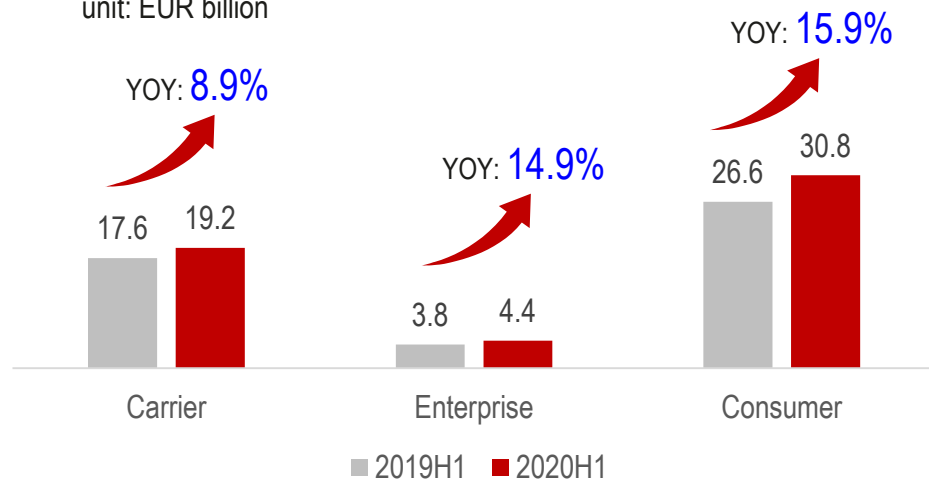
Of sales revenue invested into R&D in 2019



Of total workforce working in R&D (96,000+ employees)

Carrier Business: 8.9% Sales Revenue Increase

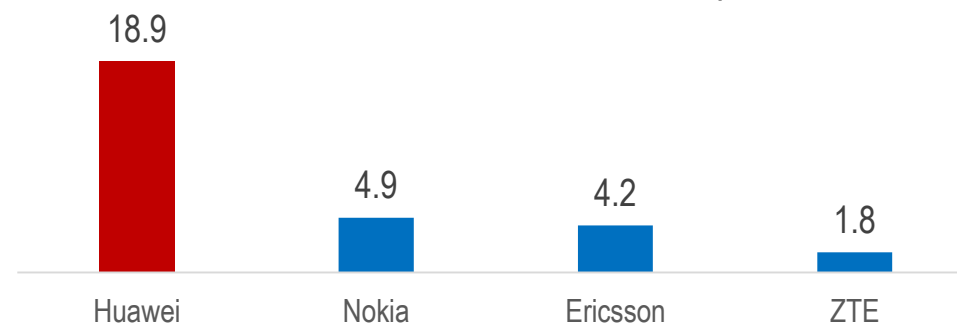
unit: EUR billion



Huawei 2019 R&D: Increased by 29.7% to \$18.9Bn 73% more Investment than the sum of the other three vendors

2019 R&D Investment Comparison

unit:
USD billion



Interpretation of China's Intelligence law by 3rd Party Law Firm



Does **NOT** have extraterritorial effect



Does **NOT** refer to any empowerment to PRC government authorities



NO Chinese authority can command Huawei to install backdoors or gather intelligence.

Interpretation of China's Intelligence law by
Renowned Third Party Law Firm (EY & Clifford Chance)

Tim Cook says Apple's refusal to unlock iPhone for FBI is a 'civil liberties' issue

- "This is about much more than a single phone or a single investigation"
- **FBI escalates war with Apple: 'Marketing bigger concern than terror'**



▲ Tim Cook: "At stake is the data security of hundreds of millions of law-abiding people and setting a dangerous precedent that threatens everyone's civil liberties." Photograph: Bloomberg via Getty Images

CEO: Will never provide government with customer information



"Neither Huawei, nor I personally, have ever received any requests from any government to provide improper information."

"I **will NEVER** do anything to harm any other nation."

"We **would rather SHUT HUAWEI DOWN** than do anything that would damage the interests of our customers in order to seek our own gains."

"There's **Cloud Act** in America with an extraterritorial reach. Also **Data Retention Investigatory Powers Act** in the UK. You then have the **Australia act** that can mandate back doors and break into encryption. Then there's the Chinese intelligence law. **All but one of those have an extraterritorial effect.** The Chinese law does **NOT** have an extraterritorial effect."

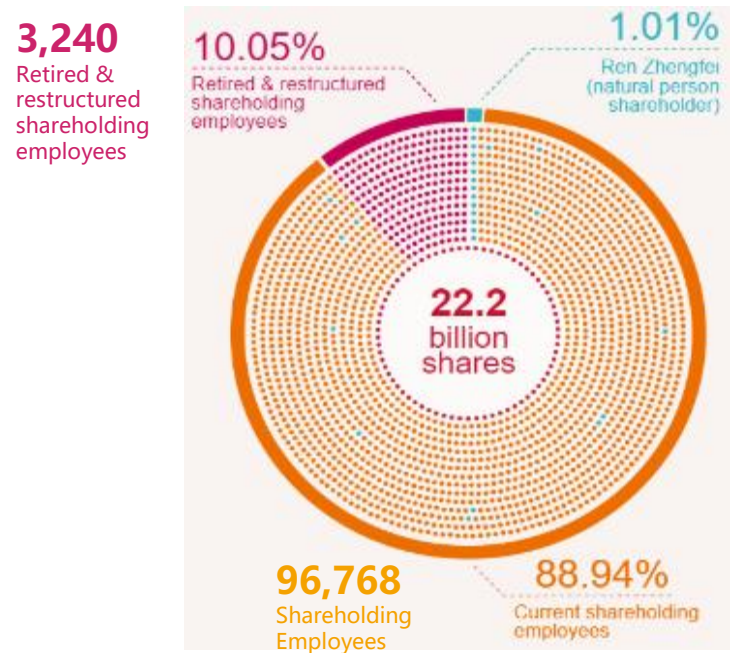
— John Suffolk

Huawei Global Cyber Security and Privacy Officer, former UK Government CIO

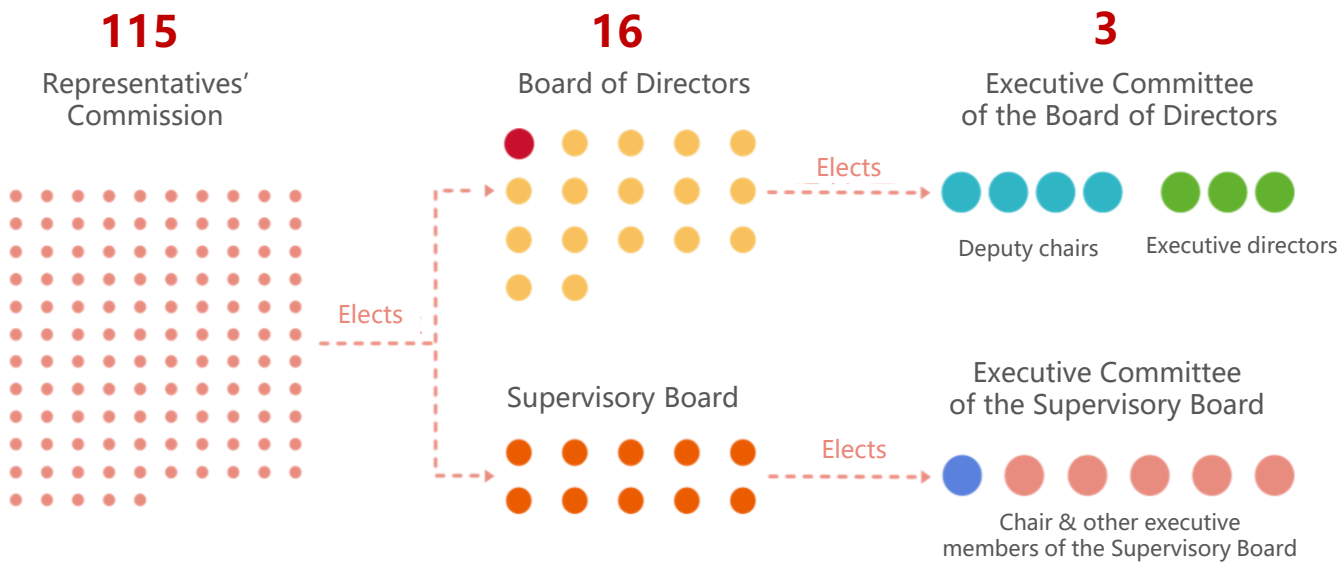
Private Company Wholly Owned by Its Employees

No government agency or external organization holds shares in Huawei.

Who owns Huawei?



Who controls and manages Huawei?



Source: KPMG

Huawei Efforts on Security achieves 0 bad record for 30 years

Top Priority and Strong Commitment

**Huawei CEO
Mr. Ren Zhengfei**

“... Neither Huawei, nor I personally, have ever received any requests from any government to provide improper information...”

“Huawei is willing to sign **no-backdoor agreement** with all governments in the world.”

Industry No.1 Investment in Cybersecurity

(\$750M/Y)

- **5%** of R&D budget for cyber security.
- **2%** of R&D Staff specialized in cyber security (Industry average 1%)
- Signed cyber security agreements with **3,400+** suppliers

30 Years

170+ Countries

3Bn People

1,500 Networks

‘0’ Bad Record

No special funding facilitates Huawei's business



Source: Prof.
ang Expert Repo

0.3%

From 2009 to 2018, the direct grants Huawei received from the Chinese government made up just 0.3% of its total sales over the period.

- **KPMG audited Huawei's annual report.**
- Even without **government grants**, Huawei's Profit would have been almost **UNAFFECTED**.
- The government grants received by Huawei are NOT UNIQUE or exclusive to Huawei or firms in China. It is also available to foreign-invested enterprises in China, including to U.S.-owned companies and to Huawei's competitors, who meet the same qualifications as Huawei.
- In a report submitted to US FCC, Huawei Financial assistance received from the Chinese government is comparable to its global competitors, including Nokia, Ericsson, Cisco.



75% of loans Huawei received were from foreign banks lending on standard commercial terms.

- Huawei's debt borrowing represents a SMALL source of Huawei's capital base.
- Huawei primarily relies on the cash flow generated from its own business operations. In 2018, for instance, Huawei held \$38.8 billion in cash and cash-equivalents while its loans only amounted to \$10.2 billion.
- The interest rates on Huawei's various loans and bonds do not indicate more favorable interest rates relative to market interest rates on corporate debt. Over the 10 year period from 2009 to 2018, Huawei's effective **interest rate** on debt was **5.7%**. This rate was higher than Cisco, Ericsson, and Nokia during this period.

15%

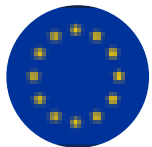
Over the past decade, the average effective tax rate paid by Huawei has been about 15% – similar to the rate paid by U.S. companies.

- **Preferential tax treatment** Huawei gets is **STANDARD** for high tech corporations around the world.
- Tax policies applicable to Huawei are standard universal policies applicable to any enterprise in China that meets the prescribed criteria qualifying a company as a "High and New Technology Enterprise (HNTE)".
- Similar parallel tax policies can be found in other countries and are not unique or exclusive to Huawei or firms in China.

Contribution in Romania

- ❑ Create **6,300 jobs**(2,100 employees and 4,200 jobs indirectly), cooperate with **126 suppliers**.
- ❑ The total **tax amount is 268 million euros**, and the **local procurement amount is 498 million euros**. Huawei is the best employer in Romania and ranks first in ICT suppliers in terms of tax payment.
- ❑ Huawei has established four global support centers (ICT Technology Center, Accounting Center, Human Resource Shared Services Center, and E-commerce Operation Center) to enable employees in Romania to master the world's most advanced technologies and operation experience without leaving Romania.
- ❑ In the past 18 years, Huawei has cooperated with four major carriers. **Romania ranks fourth** in the world of the broadband download rate and has **the lowest communication tariff** in the EU.
- ❑ During the epidemic, Romania Internet and data traffic increased by **26%**. Huawei provided **24*7** services to ensure the healthy running of carriers' networks.
- ❑ Huawei attaches great importance to corporate social responsibility. Over the past 10 years, Huawei has worked with universities to train more than **500 ICT students**. Donated **100,000 medical surgical masks, 10,000 N95 masks, and 500 protective clothing** during the outbreak.

In order to maintain balance and neutrality, most EU countries are not in a hurry to choose legislation to regulate cyber security issues



EU only releases the 5G toolbox as a guideline to its member states, and adopts strategic and technical measures to manage cyber security. It does not adopt legislation, which means that the 28 EU countries will maintain fairness and openness, and will not discriminate against specific suppliers, as US did.



- The Swedish telecommunications regulatory authority (PTS) considers that national security risks have been taken into account in the current law. There is no need to amend domestic law for 5G Toolbox.
- Neither Sweden's current laws nor the latest 5G Auction Rules introduce the concepts of "high-risk vendors" or clauses against any specific entity.

Self-assessment by Carriers

Before procurement, carriers need to **evaluate their own risks** and the impact of on Sweden's national security, and propose corresponding risk mitigation measures.

During operation, carriers need to **evaluate networks involving security-sensitive activities**, determine whether the networks are harmful to national security, and formulate security assurance plans.



PTS Pre-event Review

Operators carrying out radio services must apply to the PTS for official permission. The PTS will work with the National Security Agency and armed forces to assess whether **they are endangering national security**.

Objective criteria for determining whether a product endangers national security, such as whether the product is equipped with illegal intrusion prevention functions and confidentiality specifications.



PTS Post-event Review

If the Swedish National Security Agency or the armed forces find that the operator's network is endangering national security, they can **request the PTS to review the network again. The PTS has the right to revoke the license of the operator.**

Networks involving security-sensitive activities: The PTS **continuously supervises** carriers' security assurance plans.



- Finland's current legal framework makes it one of the most advanced mobile markets in the EU
- Existing legislation is sufficient to ensure the high quality, reliability, security and confidentiality of the network.

Technology Neutrality

The requirements on cyber security and integrity apply to **all suppliers**.

Cyber security evaluation is **limited to technical factors**, including network quality, anti-interference performance, reliability, accident detection capability, privacy protection, and stable operation capability in emergencies.

The Principle of Proportionality

Quality requirements from regulators must be commensurate with:

the severity of threats; the level of technological development to counter threats; the possible price to be paid; the number of network users, geographical areas, and importance to users

Post-event Review

Except for security defects, **regulators are not allowed to get involved in network construction.**

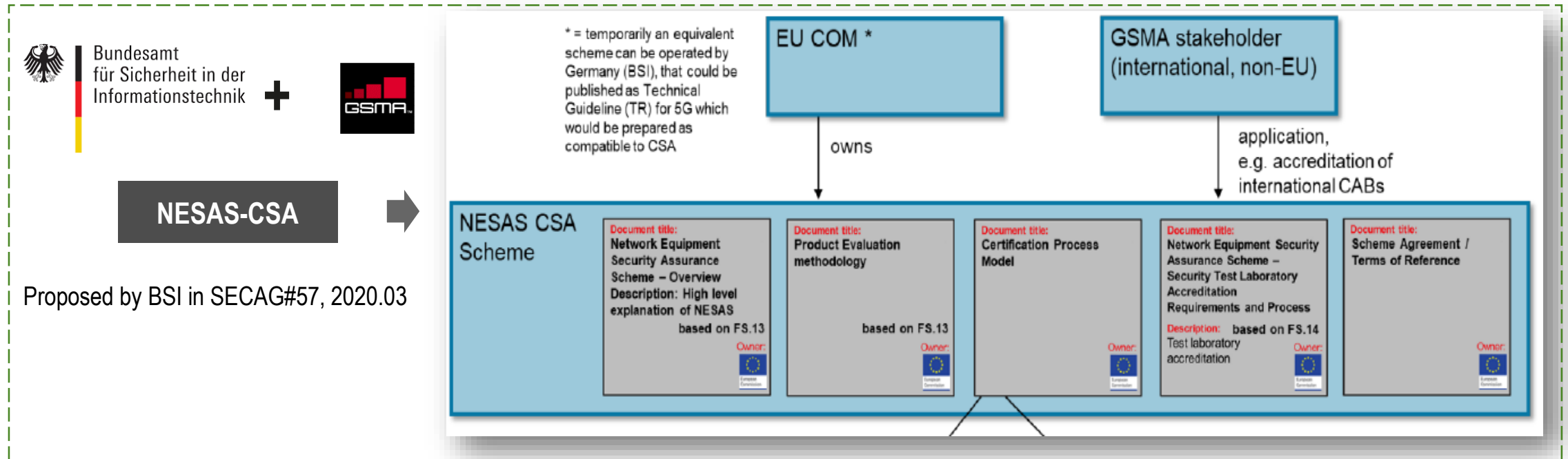
If there are serious reasons to suspect that **critical communications equipment endangers national security, it can be removed after consulting the operator**. However, the **principle of proportionality** must be followed.

Compensation Mechanism

Any party affected by a decision may appeal all decisions made by the regulatory body (Traficom).

If the equipment is removed before the law takes effect, the government must **compensate** the operator.

Germany BSI Promotes to EU NESAS-CSA as 5G Cyber Security Certification



Source: GSMA SECAG#57 Meeting, BSI NESAS-CSA Paper, revision 2020-03-16

1. Germany BSI mainly promotes NESAS-CSA as the EU's unified certification standard.
2. NESAS matches the technical requirements of EU 5G Toolbox
3. Tailored for telecom, recognized by industry, and the certification period is controllable with cost reduction

9.2 billion € potential loss and over 6300 unemployment under the draft normative act

Financial loss



More than **9.2 billion €**

External investment



Deteriorating investment environment

Fine risk



Up to **10%** of turn over

Lack of competition



More than **30%** price increasing

5G time to market Digitalization process



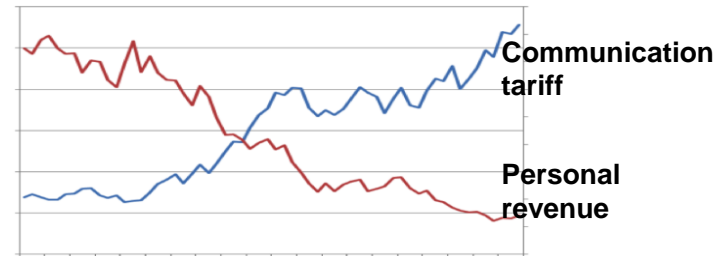
Lag behind **5-10 years**

Unemployment



Over **6,300** unemployment
250,000 job opportunities

Tariff rise to consumer



package tariff increases **by 3 times**

Poor network quality



Network **outage**
Bad user experience

It's not good for the country, it's not good for the industry, it's not good for the people.

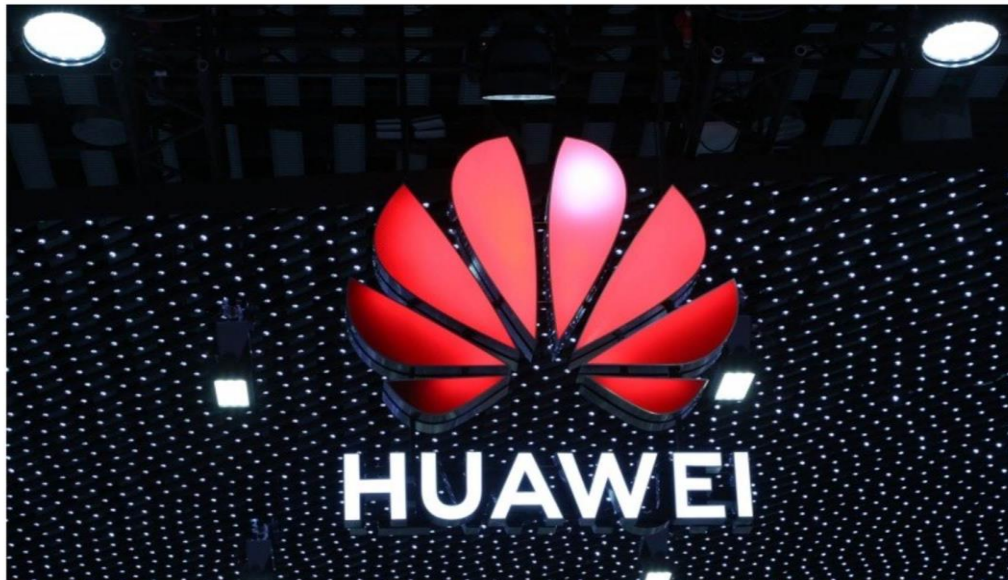
Germany has released the reliable supplier list and will not ban Huawei

5G

Verbot von Huawei in Deutschland praktisch ausgeschlossen

Ein zweistufiges Zulassungsverfahren für 5G-Ausrüster erlaubt einen Ausschluss nur, wenn Bundeskanzleramt, Auswärtiges Amt, Innen- und Wirtschaftsministerium einvernehmlich dafür eintreten. Das wird nicht passieren.

10. August 2020, 12:45 Uhr, Achim Sawall



Huawei auf dem MWC 2019

(Bild: Huawei)



LEICHTE SPRACHE GEBÄRDENSPRACHE ENGLISH KONTAKT LOGIN

Suchbegriff

Deutschland
Digital•Sicher•BSI

Themen Das BSI **Presse** Publikationen IT-Sicherheitsvorfall Service

Presse

Sicherheitsanforderungen für Telekommunikationsnetze veröffentlicht

Ort Bonn
Datum 11.08.2020

Die Bundesnetzagentur hat heute den aktuellen Entwurf des Kataloges von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten veröffentlicht. Der Katalog wurde im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt. Zugleich startet die Bundesnetzagentur eine Konsultation zum Entwurf einer Liste kritischer Funktionen.

„Der Mobilfunkstandard 5G ist eine wesentliche technologische Basis für eine erfolgreiche Digitalisierung. Voraussetzung dafür ist ein ausgewogenes Maß an Informationssicherheit als Teil eines umfassenden Risikomanagements. Dazu haben wir als Cyber-Sicherheitsbehörde des Bundes gemeinsam mit der

Inhaltsverzeichnis

[Pressemitteilungen](#)
[Pressearchiv](#)
[Kurzmeldungen](#)
[Pressestelle](#)
[Presseverteiler](#)
[Mediathek](#)
[Bildmaterial](#)
[Kurzprofil des BSI](#)

Government Voice



Germany: Germany does not want to exclude Huawei from 5G. **Issued on 2020/07/15**

<https://de.reuters.com/article/grossbritannien-huawei-deutschland-idDEKCN24G0H9>

Germany Network Agent Homann: No reason to pre-exclude Huawei. **Issued on 2020/07/15**

<https://www.faz.net/aktuell/wirtschaft/digitec/netzagentur-chef-homann-kein-grund-fuer-vorab-ausschluss-von-huawei-16861889.html?premium>

<https://de.reuters.com/article/deutschland-huawei-bundesnetzagentur-idDEKCN24G1BH>



UK: Pressure from Trump led to 5G ban, Britain tells Huawei. **Issued on 2020/07/18**

<https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei>



France: Huawei will not be prevented from investing in France. **Issued on 2020/07/21**

<https://uk.reuters.com/article/uk-france-huawei/huawei-will-not-be-prevented-from-investing-in-france-le-maire-says-idUKKCN24M0SK>

France Foreign Minister Le Drian : France does not discriminate against any enterprise in any country. **Issued on 2020/07/28**

https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1802403.shtml



Belgium: Belgium will not join UK in banning Huawei. **Issued on 2020/07/14**

<https://www.brusselstimes.com/all-news/belgium-all-news/121568/belgium-will-not-join-uk-in-banning-huawei-from-its-telecom-networks/>



Hungary: Hungary still open to full participation of Huawei in the Development of 5G in Hungary, **no Limitation, fully depend on operator's choice**

<https://www.hwsz.hu/hirek/61497/huawei-5g-magyarorszag-diplomacia-halozatepites.html>



Austria: Chancellor Kurz: "No knowledge" about espionage from Huawei. **Issued on Apr. 20, 2020**

<https://www.derstandard.at/story/2000116979906/kanzler-kurz-keine-kenntnisse-ueber-spionage-von-huawei>

Ministry of Austria Agriculture (in charge of telecommunication): Government does not veto Huawei. Telecom companies are responsible for selecting the network manufacturers. **Issued on March 23, 2020**

<https://www.derstandard.at/story/2000116034572/5g-ausbau-regierung-legt-kein-veto-gegen-huawei-ein>

Government Voice



Swedish: Swedish Minister for Digitalization: Minister for Digitalization Anders Ygeman (S), **sees no problem with Tele2 now hiring Huawei** when Swedish customers are surfing on 5G. - You probably do that already today if you surf on 4G. There is quite a lot of that company's equipment.

Issued on 2020/05/25

<https://www.svd.se/ygeman-ser-inga-problem-med-huawei>

<https://www.aftonbladet.se/minekonomi/a/70eLe8/ygeman-ser-inga-problem-med-huawei>



Norway: Norway's Minister of Digitalization: Norway Open To Huawei Supplying 5G Equipment: "We impose general security requirements on telecommunications companies and not on individual suppliers, and therefore it is not a current issue to exclude individual suppliers. The companies will make risk assessments and choose their own equipment suppliers," **Issued on 2019/09/30**

<https://www.forbes.com/sites/davidnikel/2019/09/30/norway-open-to-huawei-supplying-5g-equipment/#19ec07a14195>



Iceland: Iceland Post and Telecom Administration Managing Director: PTA Managing Director said that **Huawei's technology was working well in Iceland** and other countries and that no security issues had been identified. **Issued on 2020/07/17:**

<https://www.ruv.is/sjonvarp/spila/frettir-kl-19-00/27717/8ku9u7/bandarikin-thrysta-a-islensk-fjarskitpafyrirtaeki>

Thank you.