Towards a Trustworthy Foundation to Enhance the Security of EU 5G Networks

December 2019

HUAWEI

Authors

Sophie Batas

Marco Men (Fanglong)

Mark Smitham

Contributors

John Suffolk

Jeff Nan (Jianfeng)

Koen Claesen

Yoann Klein

Yair Kler

Marcelo Ikegami Motta

Jan Bredehoeft

Louise Gan (Lu)

Shark Liu (Wei)

Executive Summary

5G network technologies will be at the heart of a digital engine powering growth in EU economies and connecting societies. As the world becomes more connected we must grow together to bring digital to all and leave no one behind.

Although the world feels super-connected, almost half of the global population are still unable to access the internet. Being connected goes beyond convenience and drives basic economic inclusion.

By making digital universal, affordable, open, and safe, we can bring more people together and drive real global progress. Devices and systems will increasingly become more intelligent and more connected in government processes and cross-sector industrial applications, such as transport, finance, health, energy, agriculture, mining and manufacturing.

Digital technologies and infrastructures, like 5G, present many new opportunities for economic growth and threats to the security of digital communications. We should work together to build these network technologies in a way that ensures trust, security, safety and the protection of fundamental human rights, including against arbitrary interference with privacy.

5G technology presents several cybersecurity challenges due to its innovative, software-driven nature and its use in a wide range of services. It is essential to drive towards a trustworthy foundation to enhance the security both of EU 5G networks and of technology built upon them in a reliable, secure, and resilient manner. 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.

No matter whether it is a technical risk or a non-technical risk, we must make judgments and decisions based on facts. Just like this quotation from the former President of the United States, Abraham Lincoln, which is now written on the walls of the Chicago Tribune Hall: *"Let the people know the facts, the country will be safe."*

Operators and suppliers are working together in order to provide continuity of mobile network services while managing potential risks and concerns relating to these mobile networks and their underlying technologies.

There is no such thing as 100% assurance, even for other essential services besides telecommunications.

Effective risk mitigation plans are necessary to address new and emerging threats as much as possible. 5G will increasingly support essential services and involve greater cross-sector collaboration than exclusively within the telecommunications sector between operators and suppliers, so building trust in cyberspace is another key requirement.

However, trust goes beyond technical or operational measures and requires a dialogue between nations to setup diplomatic norms for acceptable state and state-sponsored behaviour in cyberspace. Suppliers can build greater trust through cooperation, openness and transparency.

Recent reports show a large number of cyberattacks were launched by attackers looking for weaknesses in the network architecture and operations, not as a result of a suppliers' country-of-origin or building locations. This is recognised by industry leaders, who suggest that objective testing and verification should be used to identify security risks.

This paper details existing and forthcoming measures and industry best practices to enhance the security of EU 5G networks. Cyber security is increasingly entangled with geopolitical issues, trade negotiations, and diplomatic dialogue between nations. Politically motivated suspicion does not address the challenges to enhance cyber security.

Risk evaluation for European telecommunications networks should focus on the greatest risks, including: system failure and human error. The potential risks inherent in any given product should be evaluated based on factors that have a material effect on security, such as security architecture, controls, and features. Mitigation measures must aim to reinforce cross-sector cooperation between telecommunications suppliers, network operators, and service providers, and also to raise transparency and openness of suppliers.

Huawei continues to collaborate with governments, customers, and partners to drive towards a trustworthy foundation to enhance security of EU 5G networks.

Contents

1 Risk mitigation measures for modern technologies

Among technical risks in the EU coordinated risk assessment of the cybersecurity of 5G networks, European Countries acknowledge the increased intensity and potential impacts of threats which are linked to a greater reliance of economic and societal functions on 5G.

The increased interdependencies between 5G networks and other critical systems (health, transportation, energy, gas and water supply, and defence), as well as the possible exploitation of IoT devices that can be used in massive numbers to target other services through Distributed Denial of Service (DDoS) attacks.

The EU coordinated risk assessment of the cybersecurity of 5G networks also points out the increased complexity of 5G technology, and estimates that the quantity and significance of vulnerabilities are likely to increase, as well as the risks resulting from Mobile Edge Computing (MEC), distributed architecture, network slicing and new technologies such as Software Defined Network (SDN), Network Function Virtualization (NFV), and cloud computing services.

European governments also acknowledged the increased significance and likelihood of non-technical risks linked to an economic and societal reliance on telecommunications and, increasingly, 5G and a possible impact on critical infrastructures. Specifically, regarding gaps in existing standardization as well as the need to manage risks related to the global supply chain that includes suppliers from non-EU countries.

To mitigate risk from modern technologies, well-defined security measures have been developed according to industry best practices and unified, international, globally-recognized standards. We adhere to the principle of openness and transparency and are willing to explore strategic and fundamental solutions with stakeholders.

1.1 Virtualization, Software Defined Networks, and Cloud Computing

Software Defined Networks (SDN), Network Function Virtualization (NFV), cloud computing services, and network slicing have changed the way networks are built. They decouple hardware and software layers via virtualization and the abstraction of storage, network, compute, and telecom functions. This significantly increases the reliance on software and requires security controls to address these changes.

These technologies have been tested, enhanced, and successfully deployed in various enterprises and commercial networks. This includes existing 4G networks and also public cloud computing service providers, financial institutions, and many other essential services across the world for over 10 years. During this period these technologies have been continuously improved and become ubiquitous.

To mitigate risk from these modern technologies, various security measures have been developed, including: security tools for hypervisor, virtual machines, and container technology; and industry best practices and guidelines[1] and NFV Security Reports and Specifications[2]. These technologies are not new and instead are well understood and mature in terms of risk, resilience and complemented by globally-recognized, readily-available industry best practices.

Suppliers must be able to provide adequate security measures and security reference architecture for these modern technologies based on detailed threat modelling, explaining which controls should be in place to mitigate the identified threats. Operators, service providers, and regulators should closely collaborate with industry experts from various industry sectors that are already using these technologies in order to define unified guidelines and requirements at the national- and EU-level.

1.2 Mobile Edge Computing (MEC) and Distributed Architecture

In 5G technology, services and cloud computing functions will be implemented closer to the edge of the network, known as Mobile Edge Computing (MEC), in order to benefit from lower latency and higher bandwidth efficiency advantages of 5G. As these core network components are deployed closer to the networks' edge, outside of the operators datacentre, several new risks are introduced. Firstly, this distributed nature and greater number of deployment locations increases the likelihood of physical attack, therefore an appropriate set of physical security controls must be implemented.

In addition, logical security measures must be implemented, including security gateways for appropriate isolation of the network edge and 5G core components. Strict control as devices start-up should ensure only trustworthy and verified network functions or services operate at the network edge, such as through secure and measured boot with remote attestation. Additionally, well-defined security measures from the cloud security domain can also be integrated into MEC in order to further enhance the visibility, situational awareness and control over the network edge, and minimize exploitation of edge locations.

1.3 Software-Based Lawful Interception

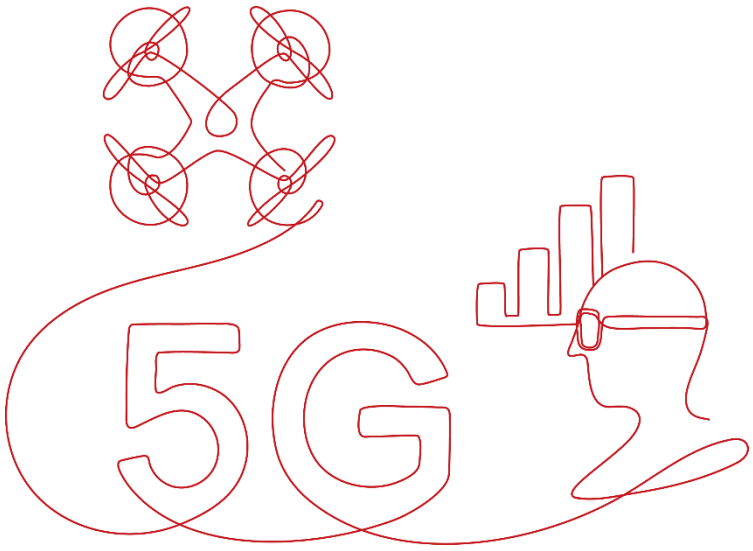
The transition from hardware-based lawful interception (LI) to software-based LI is driven by the architectural design of 5G according to a Service Based Architectural model (SBA). Ensuring that LI services are securely deployed in 5G networks, and satisfy the full set of requirements as defined by local regulations, can be achieved through the

[1] For example, the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[2] also discussed in the European Telecommunications Standards Institute (ETSI) Network Functions Virtualisation (NFV) Security Working Group (SEC WEG) https://www.etsi.org/technologies/nfv

extensive work of industry bodies[3] and standards development organisations[4]. Standards Development Organisations create a well-defined set of standards that cover both the 5G network LI requirements from a logical point of view[5] and the underlying virtualized infrastructure LI requirements[6]. Operators should ensure that 5G network components align with applicable specifications and also implement additional security measures to further mitigate risks to the infrastructure for lawful interception and its operation, including:

- Micro-segmentation: fine grain isolation and segregation to limit the ability of malicious threat agents to compromise LI resources;
- Least privilege access to minimize the ability of unauthorized services or users to access, tamper with, or abuse LI services;
- Confidentiality, integrity, and authentication to ensure that the traffic monitored by LI services cannot be leaked or tampered with during data transit or at rest.



[3] 3GPP Technical Specification Groups (TSA) Service and System Aspects working group 3 on security for lawful interception (SA3-LI) https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security
[4] European Telecommunications Standards Institute (ETSI) Lawful Interception (LI) https://www.etsi.org/technologies/lawful-interception
[5] 3GPP Technical Specification (TS) 33.127 on Lawful Interception (LI) architecture and functions https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3182 and TS 33.128 on on Protocol and procedures for Lawful Interception (LI) https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3183
[6] as defined in ETSI Group Report (GR) NFV-SEC 011 on Lawful Intercept Architecture https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/011/01.01.01_60/gr_NFV-SEC011v010101p.pdf and ETSI Group Specification (GS) MEC 026 on support for regulatory requirements https://www.etsi.org/deliver/etsi_gs/MEC/001_099/026/02.01.01_60/gs_MEC026v020101p.pdf

2 Operator Responsibilities

Responsibilities to enhance the security of EU 5G networks are shared between telecommunications suppliers, network operators, and service providers. As a supplier, Huawei recognizes specific risks for operators, especially for legacy technology or hybrid architecture with the progressive rollout of 5G technologies on their network. Security should be addressed from the outset of network design and development according to unified, global standards and industry best practices. Secure templates and software-based network configuration can help mitigation of risks from misconfigurations and increases the accountability and governance over the network state.

2.1 Network design and configuration

Huawei recognizes that there are several key considerations for operators to enhance the security of EU 5G networks through their ability to identify, protect, detect, respond, and recover from security incidents. In order to handle the various complexities of 5G networks, operators should continue to enhance their cybersecurity capabilities and build network resilience. We recommend that security of EU 5G networks could be enhanced according to the following principles, including: holistic security architecture for hybrid architecture with legacy technologies, secure-by-design and secure-by-default, and resilient network design and configuration.

2.1.1 Holistic security architecture

Each operator has their own unique deployment and operational design that have been developed over decades in some cases and include legacy technologies from 2G still operated in various EU countries, through 3G, 4G and now 5G networks. Operators may plan the deployment of 5G according to a hybrid architecture with legacy technologies to begin with and then in future as a standalone architecture of purely 5G. In this planning and close coordination with suppliers, operators need to ensure that their security architecture and network design integrates these technologies and ensure that the security measures will increase across the entire network in order to accommodate new 5G-specific business scenarios. Operators should work together with suppliers and industry organizations, such as GSMA, in order to successfully address this challenge.

Network operators should follow network security designing best-practises. Several standards or guidelines dedicated to general IP networks are already existing and should be followed during the design phase[7]. Even if these standards are not dedicated to 5G networks, they list the common, relevant practices to be followed in all IP networks.

As from the early stages of a design, and even before during the risk analysis performed by the operator, it is key to establish a close and trusted collaboration between supplier and operator. The deep knowledge of the products and design recommendations from

[7] For example, ISO/IEC 27033-1:2015 https://www.iso.org/standard/63461.html, and NIST SP 800-160 https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

the supplier are valuable inputs to support the operator's architecture decisions. A secure design and proper configuration of equipment reflect the right technical answer to the risk analysis.

2.1.2 Secure-by-design

Secure-by-design ensures that security is a top priority addressed from the outset of network design and development. This helps avoid significant risks that are difficult to correct in hindsight, e.g. addressing availability and/or redundancy, providing routing and visibility for monitoring.

Secure-by-design principles ensure that security is included and evaluated at every phase of the network design. They provide guidelines to support operators to minimize the network attack surface, establish secure defaults that minimize human errors, limit unauthorized access to resources via least privilege access, require separation of duties to limit the ability of insider threats from damaging large parts of the network, and establish layered security that mitigates the ability of outsider threats to compromise large parts of the network. Suppliers can assist network operators with: equipment designed according to these principles incorporating secure parameters; reference security architectures that minimize the operational and deployment complexity.

2.1.3 Adherence to unified, global standards and industry best practices

Various frameworks and standards have been developed to ensure critical infrastructure providers can address the enhanced complexity of modern technology[8]. GSMA has also continuously developed guidelines and best practices specifically for operators based on the industry experience. Operators should identify and adopt these modern frameworks that would enable both methodical and continued improvement of their security posture even in the face of enhanced complexities.

2.1.4 Resilient network design

Operators need to ensure sufficient redundancies. Cyber Resiliency may be defined as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources” [9]. As identified by the EU coordinated risk assessment of the cybersecurity of 5G networks, 5G networks will create interdependencies with other critical infrastructure as well as serve as the backbone for services with significant impact on society. Close coordination with suppliers is imperative for operators to build 5G networks with high levels of cyber resiliency according to cyber resiliency frameworks and cyber resiliency principles[10].

---

[8] such as the ISO 27000 series https://www.iso.org/isoiec-27001-information-security.html and NIST Cyber Security Framework (CSF) https://www.nist.gov/cyberframework

[9] https://www.mitre.org/publications/technical-papers/cyber-resiliency-metrics-catalog

[10] https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework

2.1.5 Network configuration

Misconfigurations are often ranked as the top two causes for security events. As the operational and deployment environment of 5G networks becomes more complex, it is essential that operators pay special attention to the way configurations are created, deployed, and maintained throughout network assets. Operators should, therefore, adhere to the following recommendations:

- Secure Templates – Operators should aim to minimize the amount of manual configuration work and instead favour secure templates that can be managed in a centralised way. Such a strategy not only minimizes the risk of human error, it also significantly increases an operator's ability to recover in case of equipment tampering by restoring the system into a known good state. It further improves the ability to quickly identify and resolve misconfigurations.
- Software-based configuration –Although configurations in some organizations are only available in hardcopy, configurations change over time as the network evolves and the reasons for a change or the source of the change are not captured. Operators should maintain all configurations of all network assets in a central repository which is capable of maintaining versioning.

This approach for network configuration by operators is well suited for 5G networks because it allows mitigation of risks from misconfigurations and increases the accountability and governance over the network state.

2.2 Physical security

Selection of adequate physical security measures varies dependent upon the deployed equipment and services, the operational environment, accessibility conditions, regulatory requirements, and legislative obligations. The type, nature and quantity of physical security measures should be determined following an ISO 27005 based risk assessment of the deployment site. IS0 27001 A.11 and ISO 27011 “Code of practice for Information security controls for telecommunications organizations” section 11 could also be used as guidance as they provide a list of security measures as well as NIST SP 800-187 Guide to LTE Security and NIST 800-53 which also provide additional recommendations on the type of physical security controls operators should consider for various deployment scenarios.

The EU coordinated risk assessment of the cybersecurity of 5G networks identifies specific risks related to Mobile Edge Computing (MEC), a shift of core functions, such as the User Plane Function (UPF), from a secure telecommunications datacentre towards the less secure edge of the network, and the potential increase risks for radio access network (RAN) as they may be co-located with MEC sites. There are many options for operators to mitigate these risks, for example increasing physical security with advance, remotely-managed, automated tools.

Although operators can co-locate MEC and RAN sites, they can enhance security through physical or logical separation between the two network parts, via firewalls, or separate physical deployment infrastructures each with its own dedicated security access controls. These options would maintain strong isolation between the different network parts and limit the ability of adversaries to compromise both sides of the network site.

2.3 Operation and maintenance

Operators should ensure implementation of security measures and access controls for the operation and maintenance of networks.

The ability to easily and continuously identify and catalogue the various assets which form a mobile network is an essential step in every modern cyber security framework and/or standard. Operators should strive for visibility into their assets, ensuring they can identify all the cybersecurity related properties of the assets such as physical and virtual location, configurations, versions, operational state and any other information needed in order to identify and track the assets’ specific cyber-security posture.

Operators should select suppliers that can ensure their products and solutions can either natively provide the required information or can interoperate with third-party products which can deliver such capabilities. Such capabilities will be essential for 5G networks as they incorporate multi-supplier software and hardware products which can be deployed at various locations and can have limited lifespan, i.e. they may expire after a relatively short period of time.

The transient nature of some 5G network functions combined with network scalability and 5G network distribution, i.e. Mobile Edge Computing (MEC), increases the complexity of data lifecycle management. In order to ensure privacy protection, compliance, and to minimize the risk in case of data breach, operators should incorporate data-centric lifecycle security controls into their architectural design. This will ensure that the organization knows which data is stored and processed, who, when and why the data has been accessed and what security controls are set in place to safeguard the data given the data sensitivity/criticality.

Operators should ensure data is governed and protected when needed to ensure confidentiality and privacy, integrity, and availability as well as its proper disposal in accordance with national and international law.

Operators could automate operational and deployment security to avoid human error. Reliance on human intervention for detection and mitigation of security events cannot scale in large, complex, and dynamic environments.

Modern cyber security technologies address these challenges via automated operational and deployment security tools, such as Security Orchestration, Automation and Response (SOAR). These tools enable operators to create complex, pre-defined rules, action those rules that address certain security events without human intervention, and correlate events based on advanced algorithms to help minimize the event/noise ratio and enrich security events data. This significantly improves operator's identification, detection, response, and recovery from a security incident in matter of minutes not weeks.

In 5G networks, these automated tools should enable operators to effectively handle 5G security challenges without dramatically increasing the human costs.

Operators should also aim to benefit from existing industry best practices and methodologies[11]. In the context of remote access from a sub-contractor or supplier, a particular attention should be paid to access management, change management, and event management.

Operators should ensure that clear process and tools are in place for allowing only authorized users to access certain assets while preventing unauthorized users from accessing them.

Operator processes should involve at least: access request by the supplier to the operator service desk, verification of the user, providing rights of authorization, monitoring identity status, logging and tracking access, removing and restricting access rights after tasks are performed.

Any modification to the operator network must imply to create and submit a formal request for change (RFC) by the supplier, a review of the request, formal and written approval of the request by a change advisory board (CAB) or delegated authority, coordination of the change implementation, and closing the change record.

Operators should collaborate closely with suppliers to implement appropriate event management processes for supplier equipment. Supplier equipment could offer transparent and standard Application Programming Interfaces (APIs) for continuous monitoring by operators of operational components and services.

2.4 Procurement processes

It is crucial that supply management embeds security requirements, in particular in the procurement process when selecting a supplier. Not only operators but also suppliers should established a security management system for their global supply, covering all chips, software, components, and other products. Operators should require suppliers to provide evidence they maintain strict control over their supply chain cybersecurity and can demonstrate compliance with industry best practice principles or relevant global standards[12]. Operators should also consider to mandate suppliers to comply with applicable cybersecurity standards[13] for operational security, as well as product specific cybersecurity certifications or verification scheme[14].

---

[11] such as Information Technology Infrastructure Library (ITIL) https://www.axelos.com/best-practice-solutions/itil/what-is-itil or Control Objectives for Information and related Technology (COBIT) http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx

[12] such as ISO 28000 https://www.iso.org/standard/44641.html, ISO 20243 https://www.iso.org/standard/67394.html

[13] such as ISO 27001 https://www.iso.org/isoiec-27001-information-security.html, ISO 22301 https://www.iso.org/news/2012/06/Ref1602.html and Service Organisation Control 2 (SOC2) https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

[14] such as GSMA NESAS https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Some stakeholders are concerned that 5G network technologies will be subject to state intervention from non-EU countries. To address this concern in security throughout the global supply chain, we recommend that procurement processes and management methodologies of operators support an appropriate recognition and accompanying enforcement mechanism to enable operators to indicate those suppliers that consistently demonstrate a high level of trustworthiness.

Governments in EU Member States and operators may reserve the right to audit and check the suppliers and any non-compliant supplier would face enforcement, such as a financial penalty or fine. Compliance against these unified, international, globally-recognized standards and industry best practices.

We need to make judgments based on facts. 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."* We believe this should include the following commitments for suppliers:

1. **Compliance with security laws and regulations** of relevant countries or regions as well as industry security standards, meet customers' cyber security requirements.
2. **Implementation of a cyber security system certification for new suppliers,** which incorporates testing and verification of product security. Operators should:
   a) establish comprehensive category of security specifications and test requirements;
   b) perform product security testing when new products are introduced;
   c) ensure that supplier products have no known vulnerabilities.
3. **Implementation of coordinated vulnerability disclosure (CVD) processes.** Operators should require suppliers to establish information sharing mechanisms through a connection with the supplier's product security incident response team (PSIRT) and suppliers release vulnerabilities and patches in a timely manner according to the service level agreements (SLA) of supplier vulnerability notification. Suppliers should have response mechanisms for security issues.
4. **Cyber security risk assessment**, incorporating corporate inspection and relevant training. The operator should annually evaluate suppliers' cyber security risk levels and conduct on-site inspections on high-risk/medium-risk suppliers to drive suppliers to continuously improve security capabilities and reduce security risks. Conduct cyber security Score Card assessment for suppliers, and downgrade or stop cooperation with suppliers whose Score Card scores do not meet requirements. Operators should provide annual training on cyber security for suppliers.
5. **Participation in industry security standard certification activities.** Suppliers should actively participate in industry security standard certification.

Cyber security standards[15] *should be technology-neutral and equally applicable to all enterprises and networks. After clear and unified cyber security standards are available, independent and comprehensive verification must be performed based on the unified cyber security standards.*

3 Supplier Responsibilities

As manufacturers of telecommunications products, suppliers face particular challenges to enhance security of EU 5G networks. Security verification should be addressed from the beginning of product design and throughout the development process. Supplier diversity must be carefully managed to minimize risks for resilience of both the network and supply chain. Suppliers can rely on industry best practices for principles on cyber resilience design. Transparency of supplier ownership structure, source code inspection, government relationships and legislative compliance are part of the foundation of trust in suppliers.

3.1 Product development lifecycle

The EU coordinated risk assessment of the cybersecurity of 5G networks highlights the quality of software code is an important security measure for 5G networks because they are largely based on software. A secure development lifecycle can help detect and prevent the malicious insertion of intentional vulnerabilities into products. Software is more evident in all parts of 5G network technologies. Secure software development, methodologies, and relevant cybersecurity measures must be applied by suppliers of 5G network products.

[15] e.g. ISO20243, ISO/IEC 30111, ISO/IEC 29147, ISO/IEC 27001, ISO28000, AEO, Common Criteria and ISO/IEC 15408, O-TTPS, and TAPA.

Industry best practices for software security can help to measure maturity of software security activities and practices in an organization. Following a secure software development lifecycle (SSDL) can help suppliers iteratively improve their software development business practices by measuring the maturity of those practices over time.

First and foremost, appropriate secure software development standards that follow architecture and design principles, and make the most of code repositories and application programming interfaces (APIs) to write concise, standard, easy-to-read, robust, and secure code. Suppliers should implement software engineering practices according to a security-by-design approach that should promote characteristics, including but not limited to:

- Provide security training and awareness,
- Define security requirements,
- Define metrics and compliance reporting,
- Perform threat modelling,
- Establish design requirements,
- Define and use cryptography standards,
- Manage security risk of using third-party components,
- Use approved tools,
- Establish a standard incident respond process,
- Perform rigorous testing throughout the development process with static and dynamic analysis, pen testing, etc.

It is vital to integrate security verification throughout the development process. Suppliers should implement recognized security verification processes, utilize commercially-available tools and employ qualified security personnel. Secondly, suppliers should manage a dedicated security team independent from production teams and the objectives and governance of the security team should focus on identification of security flaws in products during the development lifecycle. This security team should be responsible for product assessment and evaluation before release. In addition, suppliers should subject their products to pen-tests by external, accredited companies.

Suppliers should provide access for operators or external, accredited parties to perform source code evaluation of specific products. Accessing the source code of a supplier is an effective method to mitigate the risk of backdoors in software. Suppliers should establish facilities that provide access for an accredited entity or operator to the source code[16]. These facilities and access conditions should remain under the responsibilities of the supplier in order to ensure protection of intellectual property.

[16] For example, Huawei Cyber Security Evaluation Center (HCSEC) https://www.huawei.com/au/press-events/news/au/2010/hw-u_151000 and Huawei Security Innovation Lab (HSIL) https://e.huawei.com/de/news/de/2018/Huawei_Security_Innovation_Lab

3.1.1 Secure-by-design and secure-by-default

Secure-by-design principles ensure that security is also a top priority from the very beginning of product design and development with evaluation at every phase of product design. Products should also be configured to be secure-by-default out of the box or could obtain their configuration in a secure manner from the network without human interaction (zero-touch provisioning). Such a deployment and operational methodology will not only minimize the workload of the technical staff but also minimize the amount of errors and mistakes that can later on be exploited by malicious adversary.

3.2 Supplier diversity, open collaboration, and network resilience

Supplier diversity increases network resilience, especially with mature technology from market-leading suppliers. Diversity offers resilience through redundancy, i.e. providing alternative ways or alternative components for required functionality in the event of a compromised component. Supplier diversity may also increase the attack surface, introduce service inconsistencies and increase lifecycle costs, and may be ineffective against some adversaries. Industry best practices for managing supplier diversity are essential for minimizing these risks. The use of diversity in system architecture and design must have tangible benefit through careful management.

Collaboration between the public and private sector is fundamental for raising the overall level of cyber security across Europe. This collaborative approach should aim to stimulate a competitive market through certification and awareness initiatives, especially for key providers to the public sector, essential services, and regulated industries. A competitive market benefits everyone and stimulates continued improvement of supplier's products and services through innovation, enhanced security and resilience. In an interconnected world reliant on a global supply chain, trust can be based on confidence that risk management is objective and transparency.

Industry best practices for network resilience include the Cyber Resiliency Design Principles[17]. These define an approach to plan and manage diversity as a well-established resilience technique, removing single points of attack or failure. Security architecture and network and product design should consider cost and manageability to minimise risks.

These design principles specifically state that diversity avoids the risk of a monoculture, in which compromise of one component can propagate to all other such components. Supplier diversity must be carefully managed according to these design principles to mitigate an adversary attacking any component in the set of alternatives, looking for a path of least resistance to establish a foothold, rather than trying to compromise a single component and propagate across all such components.

Additionally, supplier diversity may increase lifecycle costs as it forces developers, system administrators, maintenance staff, and users to deal with multiple interfaces to

[17] https://www.mitre.org/publications/technical-papers/cyber-resiliency-design-principles

equivalent components. Carefully managing supplier diversity should mitigate the risks that inconsistencies would be introduced, particularly if the configuration alternatives for the equivalent components are organized differently.

Supplier diversity is one measure to increase network resilience and must be carefully managed to minimize network risk. We recommend that more than one supplier should be included in relevant parts of a network and industry best practices show that network diversity can be managed best with a low number of suppliers.

3.3 Supply chain resilience and business continuity planning

Supplier diversity increases supply chain resilience, especially with contingency plans for a reserve of strategic equipment and multi-source supply. Trade sanctions in third countries may decrease capabilities of suppliers, affecting network maintenance, software and hardware upgrades.

The sourcing of resources and components for development and manufacture for modern technologies and services are reliant on a global supply chain. Any trade sanction in any country has the ability to disrupt the supply of certain materials and services. We recommend that business continuity planning should be incorporated in the product development process, ensuring that backup of critical technologies are taken into account.

Managing supplier diversity for network resilience with a low number of suppliers (see section 3.2 on supplier diversity), can be considered differently from supplier diversity for supply chain resilience. Product supply risks can be addressed with supplier diversity through designing multi-source supply chain, including: multi-source product versions, multi-supplier supply, and geographically dispersed suppliers and factories to ensure supply continuity in the event of unexpected risks.

3.4 Supplier transparency

Increased transparency of governance, ownership, and relationship with governments can help mitigate against external influence on or interference in suppliers.

Clear requirements for supplier transparency can also help demonstrate their adherence to EU values of democracy, rule of law, and the protection of fundamental human rights, and compliance to relevant legislation.[18]

For example, increased transparency for:

- Extra-territorial scope of legislation. EU Member States and third-countries should ensure that privacy, security, or intelligence legislation has no extra-territorial effect that would prohibit compliance with EU law.
- Shared responsibilities between operators and suppliers, as regards privacy protection, should limit exposure of a supplier to personal data to the extent necessary. Operators should remain the data controller and sensitive activities, such as installation, operations and maintenance should be performed in compliance with the defined Security Architecture, monitored by operators, following clear processes as described in other sections of this document.
- Open collaboration between EU Member States, operators and suppliers in order to provide updates on technological developments, evaluate the compliance with local laws and regulations, assess the relevance of the existing regulations, and improve awareness of organizational security practices and product security level. This should include certification of products and organizational processes through trust building schemes involving national cyber security agencies.
- Source code inspection. Suppliers should provide facilities to enable access for accredited entities or operators to perform tests on the source code. As mentioned in the product development lifecycle section above, these facilities and access conditions should remain under the responsibilities of the supplier in order to ensure protection of intellectual property. An open and joint review of the results should be performed between external party and the supplier in order to discuss the different findings.
- The ownership structure of a supplier should be transparent as set out in audited annual financial reports and the supplier shall commit not to be subject to legislation compromising the integrity of its products.

[18] Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data – General Data Protection Regulation (GDPR) https://eur-lex.europa.eu/eli/reg/2016/679/oj and Directive on privacy and electronic communications (E-Privacy Directive) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

4 Shared Responsibility: risks for both operator and supplier

Although there are challenges particular for suppliers and operators, they also share responsibilities for security risk management of 5G networks. These are especially important for personnel, operations and maintenance, and vulnerability management processes. Unified, international globally-recognized standards exist for 5G security and both suppliers and operators should be encouraged to implement them through 5G cyber security certification, such as the Network Equipment Security Assurance Scheme (NESAS).

4.1 Specialized, trained personnel

Security is not only about technology but also about people and processes. It is absolutely key that whatever their domains of expertise, personnel are trained on cybersecurity and privacy objectives and practices. It is true for both supplier and operator resources.

Concrete cyber training program should be implemented within each organization, addressing different maturity levels: from raising awareness to deep cyber expertise. Ideally people should be assessed regularly on their cybersecurity and privacy knowledge and sign a “letter of commitment”.

For the most advanced or critical profiles, we recommend to require in the procurement phase to have a certain amount of certified people in terms of security. Today several independent organization propose exams for cybersecurity certifications. Engineers who provide customer services and contact customer systems or data shall be identified as employees holding a key cyber security position. Equipment suppliers shall conduct cyber security background checks on employees in these positions, and require them to participate in cyber security training and education programs, and sign commitment letters.

Training and certification of employees can also apply for other specific competences such as virtualization technologies. Virtualization technologies exist now for many years and industry can count on a mature ecosystem for recognition through various certification programs which recognize that personnel is qualified to work on certain technologies.

4.2 Internal security controls, monitoring and risk management practices

When a supplier performs maintenance tasks on operator’s infrastructure, they should be able to demonstrate that the customer is always in control of any third-party access to their technology and services. Therefore the supplier should be able to demonstrate a range of processes and controls that guide their personnel, and hold them accountable, regarding what they can and cannot do.

Suppliers and operators should strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain. They may jointly sign a cyber security guarantee or commit to a financial escrow.

A supplier should also be able to demonstrate that any changes or upgrades they do to your technology are in line with the approved software for you as a customer, including the correct version and release level. To reach the above objectives, we recommend the following set of procedural and technical controls:

- All supplier operations must be explicitly approved by the operator, and authorization has to be documented. Approval must be proportionally restricted in scope and time.
- Supplier engineering access must only be possible after authorization has been granted.
- Access to operator's infrastructure must be subject to individual 2-factor authentication, to ensure traceability of all actions.
- The use of shared accounts should always be traceable to individual users.
- All actions of supplier engineers must be logged and monitored.
- Access to operator infrastructure may only occur from appropriately hardened systems, in order to prevent damaging the infrastructure integrity
- Troubleshooting on operator equipment may require access to data on the equipment. A set of agreed policies and procedures should be available that ensures the protection of personal user data and business data when that is required.

4.3 Vulnerability management procedures

The EU coordinated risk assessment of the cybersecurity of 5G networks also raises concerns over the increased part of software in 5G equipment leads to increased risks linked to software development and update processes.

Technical standards, protection measures, and independent verification can be an effective approach to manage software complexity and frequent updates. This approach is especially valuable when complemented by detection measures that implement cybersecurity testing technologies and tools, which are rapidly evolving while cybersecurity testing institutions and experts are flourishing. Network monitoring can detect abnormal or unexpected behaviour of internal and external risks.

According to recent reports, out of 1,200 major cyber security incidents over two years, a large number of attacks were launched by attackers looking for weaknesses in the network architecture and operations, not as a result of a suppliers' country-of-origin or building locations.[19]

Bill Gates has suggested that an objective test be used to identify security risks. He said that *"all goods and services should be subject to an objective test."*[20]

Vulnerability and patch management are a shared responsibility between suppliers and operators who should collectively develop ways to prevent the proliferation of malicious software and practices intended to cause harm.[21] Unified, international, globally-recognized standards for coordinated vulnerability disclosure (CVD) processes already exist[22]. In order to properly handle the possible increase in number of vulnerabilities that could exist in future 5G networks, operators should consider to either establish their own cyber security incident response team (CSIRT) or establish a process for them to easily identify and track the existence and impact of such vulnerabilities on their network.

Operators should establish information sharing mechanisms through a connection with the supplier's product security incident response team (PSIRT) in order to ensure vulnerabilities are detected, reported and corrected in a timely manner. Once suppliers disclose vulnerabilities in a coordinated manner, it is a shared responsibility for operators to apply relevant patches. To facilitate application of these patches, operators should maintain a vulnerability management system for identification, scheduling and coordination of the deployment of patches on vulnerable products and/or services.

Suppliers should ensure they are capable of quickly identifying security vulnerabilities in their products resulting either directly, due to their product issue, or indirectly as a result

---

[19] UK National Cyber Security Centre (NCSC) Annual Review 2018 https://www.ncsc.gov.uk/news/annual-review-2018

[20] NYT DealBook conference 2019 https://www.nytdealbookconference.com/db2019/full-agenda

[21] Paris Call for trust and security in cyberspace https://pariscall.international/en/principles

[22] such as ISO/IEC 29147 https://www.iso.org/standard/72311.html

of a supply chain related components, suppliers should demonstrate compliance with industry standards[23]. Suppliers should also communicate product service lifecycle events within contractual support obligations, including: dates for end-of-life and end-of-support, discovery of product vulnerabilities, and availability of patches and/or other mitigations for affected products. Suppliers and operators to commit to respect standards on Vulnerability Handling Processes[24] and Coordinated Vulnerability Disclosure (CVD)[25].

4.4 Compliance with unified, international, globally-recognized standards

3GPP has defined clear standards for 5G security. Both suppliers and operators should be encouraged to implement security standards. The Network Equipment Security Assurance Scheme (NESAS)[26], has been developed through global industry collaboration including suppliers and operators. Working together with 3GPP, GSMA defined security objectives, requirements, and test cases in the NESAS scheme with industry and stakeholders. This takes into account the specificities of individual industry sectors and allows for faster assessment.

NESAS covers the processes and procedures to develop secure products. Evaluation laboratories are assessed to international, globally-recognized and unified standards[27], supported by industry experts, allowing for more cost-effective assessment. NESAS is a security assessment scheme that provides a baseline of security requirements for 3GPP defined functions. However it doesn't cover all 3GPP security standards. NESAS is not a replacement for operators or national security requirements. Regulators should consider referring to NESAS.

NESAS has significant advantages for regulators, as it provides a minimal set of security requirements already accepted by industry and the global market and already customized to 5G technology. It is a methodology based on existing standards and taking into account the complexity of products and processes. NESAS can facilitate security of heterogeneous 5G networks including multiple suppliers as NESAS requirements are unified and apply to all suppliers. NESAS is extensible can flexibly develop to meet future needs.

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 to continue the work on 5G Security and Certification started with GSMA and 3GPP, in order to develop a common approach that is recognized throughout Europe.

---

[23] such as ISO 30111 https://www.iso.org/standard/69725.html and ISO 29147 https://www.iso.org/standard/72311.html
[24] ISO/IEC 30111:2019 https://www.iso.org/standard/69725.html
[25] ISO/IEC 29147:2018 https://www.iso.org/standard/72311.html
[26] NESAS https://www.gsma.com/security/network-equipment-security-assurance-scheme/
[27] ISO 17025 https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html

5 End-user Device Risks

Standards for 5G technologies address risk scenarios related to end-user devices that are specifically highlighted in the EU coordinated risk assessment of the cybersecurity of 5G networks. These security enhancements take into account the characteristic of 5G technologies for massive machine-type communications (mMTC) that are so important for services for industrial Internet of Things (IoT).

5.1 Cross-sector collaboration for 5G security assurance

5G telecommunications technologies have three key characteristics: bandwidth, latency, and density. These are represented by specific features of the technology: enhanced mobile broadband (eMBB), ultra-reliable and low-latency communications (URLLC), and massive machine-type communications (mMTC).

Considering bandwidth, eMBB focuses on services that require ultra-high bandwidth, such as high-definition video (4K/8K), virtual reality (VR), and augmented reality (AR), meeting user demands for a digital life. As regards latency, URLLC focuses on latency-sensitive services, such as autonomous driving/assisted driving, Internet of Vehicles (IoV), and remote control, meeting user demands for a digital industry. Specifically on density, mMTC focuses on scenarios requiring high-density connections, such as intelligent transportation, smart grid, intelligent manufacturing (Industry 4.0), and smart logistics, meeting user demands for a digital society.

In an IoT ecosystem, numerous connected devices generate and use massive amounts of data; networks provide security assurances for highly parallel communications; and the cloud and IoT platform supports a wide range of IoT applications. All these supporting systems and applications may be subject to potential malicious attacks.

Security is part of cellular networks definition for 5G. Compared to previous wireless technologies, 5G standards include more security features to tackle potential security challenges and lead to security enhancements in the future 5G lifecycle.

Suppliers can apply IoT security frameworks to address risk from the perspective of cross-sector IoT applications and services. These security frameworks should counter security threats at sensor, network, and application levels in IoT services.

Building on platform and cloud security, we recommend that suppliers should leverage experience in providing assurances of telecom network security to offer security situational awareness, analysis, and detection for IoT. IoT security frameworks should be iteratively refined to better adapt to the security needs of cross-industry applications, particularly industry-specific security needs.

We recommend that an independent EU organization should be established to enable greater accountability for attribution and arbitration of cyber security incidents.

6 Conclusion

Cyber security is increasingly entangled with geopolitical issues, trade negotiations, and diplomatic dialogue between nations. Politically motivated suspicion does not address the challenges to enhance cyber security. Facts speak for themselves. In August 2018, the European Union Agency for Network and Information Security (ENISA) published an analysis of 169 security incidents encountered by European telecommunications operators in 2017, which showed:

- 62.1% of incidents were caused by system failures, with each incident affecting an average of 1.1 million user connections. 9169 telecommunications incidents reported extreme weather as a major factor[28].
- 18.3% of incidents were caused by human errors, with each incident affecting an average of 1.2 million user connections.
- 17.2% of incidents were caused by natural phenomena, with each incident affecting an average of 600,000 user connections.
- 2.5% of incidents were caused by malicious actions, with each incident affecting an average of 300,000 user connections.

As the UK National Cyber Security Centre (NCSC) recently noted: *"In the 1,200 or so significant cyber security incidents the NCSC has managed since we were set up, the country of origin of suppliers has not featured among the main causes for concern in how these attacks are carried out. ... The techniques... ...were looking for weaknesses in how networks were architected and how they were run."*

System failure and human error constitute the greatest risk, and should be the focus of risk evaluation. The potential risks in any given product should be evaluated based on factors that have a material effect on security, such as the product's security architecture, security mechanisms, and security features. On the basis of the EU coordinated risk assessment of the cybersecurity of 5G networks from the EU Network and Information Security (NIS) Cooperation Group, mitigation measures should aim to reinforce cross-sector collaboration between suppliers, operators, and service providers, and also to raise the transparency and openness of the suppliers towards EU Member States.

Governments in EU Member states can drive towards a trustworthy foundation to enhance the security of EU 5G networks addressing technical and non-technical risks through greater public-private sector collaboration, such as in the definition of security requirements; development of unified, international, globally-recognized standards; and promoting the widespread acceptance and implementation of international norms of responsible behaviour as well as confidence-building measures in cyberspace.

---

[28] ENISA annual report on telecom security incidents 2017 https://www.enisa.europa.eu/news/enisa-news/169-telecom-incidents-reported-extreme-weather-major-factor

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. It is important to obtain the support of telecommunications suppliers and services providers in relevant industry sectors. An independent EU organization must enable greater accountability of cyber incidents.

6.1 Recommendations

We recommend that any initiatives in the policy area of cybersecurity for 5G networks should support the following:

1. **Security Reference Architecture** for virtualized technologies and slicing;
2. **Specifications to address Lawful Intercept implementation on 5G.** There are additional technical and operational measures to mitigate tampering and abuse;
3. **Enhanced physical security** for the Radio Access Network;
4. **Continuous network monitoring** with consideration for shared responsibilities between telecommunications suppliers, network operators, and service providers;
5. **Secure-by-design and secure-by-default** product development;
6. **State-of-the-art secure operation practices**, including in access management, change management, and event management;
7. **Appropriate recognition mechanism** to enable operators and regulators to indicate those suppliers that consistently demonstrate a high level of trustworthiness according to compliance against specific, unified, international, globally-recognized standards and industry best practices
8. **Contractually binding obligations** on cyber security between suppliers in their supply chain that prevent private hack back and enable non-proliferation;[29]
9. **External review of supplier software** including source code analysis;
10. **Intelligent approach to diversity of suppliers** in individual networks;
11. **Business continuity planning** for supply chain resilience that includes multi-source product versions, multi-vendor supply, and geographically dispersed suppliers and factories;
12. **Vulnerability disclosure and management processes** that are timely and efficient;
13. **Globally-recognized certification schemes** that address 5G security (NESAS) and the increased attack surface from an IoT ecosystem operating on 5G;
14. **Cybersecurity training and awareness programs**;
15. **Increased transparency of political, technological, and legal factors applicable to network operators, suppliers, and service providers operations** to mitigate against external influence or interference.

[29] Paris Call for trust and security in cyberspace https://pariscall.international/en/principles

6.2 Building mutual trust for an Intelligent, Connected world

Beyond the technical measures enumerated in these recommendations, Huawei fully supports the recommendations from ENISA in its Threat Landscape for 5G Networks[30]. These consider that shared responsibilities of cybersecurity for 5G networks, such as telecommunications suppliers, network operators, service providers, and Standardization Bodies, should address three essential aspects of public-private dialogue: 1) engagement in EU-wide discussions on 5G matters, 2) contribution to knowledge collection and dissemination, and 3) bringing in knowledge on economic, investment, and market share.

Huawei has established offices throughout nearly all of the EU Member States as well as national Cyber Security and Privacy Officers in most of them, who is specifically dedicated to the interface with customers, regulators and government officials. In addition, we have recently established the Huawei Cyber Security Transparency Centre in Brussels. It provides insights on Huawei operations, security practices, technological developments, and enables source code verification and testing. Commercially-sensitive information can be provided at national-level by Huawei representative offices in respective countries.

Regulators are welcome to discuss with us how to use this platform to enhance trust. Huawei is willing to work with all governments, customers and partners through various channels to jointly address cyber security challenges.

Huawei will set up regional security verification centres if necessary. These centres will be open to national administrations (governments, supervisors and regulators) and our customers. In addition, Huawei will allow its products to be inspected by authorized personnel from national governments in order to ensure the security of our products and services. Huawei will proactively contribute to the development of telecommunications cyber security standardization led by ITU-T, 3GPP, and IETF.

[30] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Huawei Cyber Security Manifesto

Security. We do more.

That's because security is more than what most see it to be.

At Huawei, security starts with our values and beliefs.

The world today is digitally connected, so people can benefit from technology. We will go to the ends of the earth to achieve this - from the hottest to the coldest places on the planet.

We believe security is about keeping networks running, regardless of what Mother Nature throws at it. We stand by our customers in hurricanes, earthquakes, tsunamis, and even wars.

Security isn't just about bits and bytes, it's about human life. It's about being with you through good times, and bad. It's about ensuring we don't put making money ahead of securing the networks we build.

Technology is a wondrous thing, but it's also a complex thing. Technology is not something you can do on your own. It takes partnerships, global supply chains, industries and governments working together to benefit the world.

We're fully committed to security in every way. We welcome input, ideas and suggestions to improve everything we do, so we can benefit our customers, and their customers. Today, we're probably the most open, most evaluated and transparent company in the world.

We will always prioritize security over costs, schedules and functions. We imbue security processes into product lifecycles: from design, to development, to delivery.

If there is a security standard or security certification that needs to be achieved, we will achieve it.

We believe you cannot have good privacy without good security, nor good security without good privacy.

We would never do anything illegal. We will never harm any country or any individual, and never accept any request to use Huawei products for malicious purposes. If we are ever put such a position, we would rather close the business.

We're here to help our customers maximize the value of their assets. Nothing matters more to us than being customer-centric. It's why we do more to build trust, to enhance our capabilities, to be transparent, and advocate collaboration.

Security isn't just something we invest in constantly, but a value that serves as the foundation of our existence.

When we do more for security, you can expect more from us.

About Huawei

Who is Huawei?

Founded in 1987, Huawei is a leading global provider of information and communications technology (ICT) infrastructure and smart devices. We are committed to bringing digital to every person, home and organization for a fully connected, intelligent world. We have nearly 194,000 employees, and we operate in more than 170 countries and regions, serving more than three billion people around the world.

Huawei's end-to-end portfolio of products, solutions and services are both competitive and secure. Through open collaboration with ecosystem partners, we create lasting value for our customers, working to empower people, enrich home life, and inspire innovation in organizations of all shapes and sizes. At Huawei, innovation focuses on customer needs. We invest heavily in basic research, concentrating on technological breakthroughs that drive the world forward.

Who owns Huawei?

Huawei is a private company wholly owned by its employees. Through the legal entity of Huawei Investment & Holding Co., Ltd., we implement an Employee Shareholding Scheme that involves 96,768 employee shareholders. This scheme is limited to employees. No government department or other third-party organization owns the company's shares, interferes with its operations, or influences its decision-making. Although Huawei is not a publicly listed company, we release our annual report every year by referring to the standards and practices of listed companies. The financial statements in the annual report are audited by KPMG, an independent auditor, to let the outside world know about the authenticity, independence, and financial transparency of Huawei's business.

Who controls and manages Huawei?

Huawei has a sound and effective corporate governance system. Shareholding employees elect 115 representatives to form the Representatives' Commission. This Representatives' Commission elects the Chairman of the Board and the remaining 16 board directors. The Board of Directors elects four deputy chairs and three executive directors. Three deputy chairs take turns serving as the company's rotating chairman.

The rotating chairman leads the Board of Directors and its Executive Committee while in office. The board exercises decision-making authority for corporate strategy and operations management, and is the highest body responsible for corporate strategy, operations management, and customer satisfaction.

Meanwhile, the Chairman of the Board chairs the Representatives' Commission. As Huawei's highest decision-making body, the Representatives' Commission makes decisions on important company matters, like profit distribution, capital increases, and the elections of members of the Board of Directors and the Supervisory Board.

Who does Huawei work with?

Externally, we rely on our customers. They are at the centre of everything we do, and we create value for them with innovative products. Internally, we rely on our dedicated employees. Dedication is a core part of our work ethic. At Huawei, those who contribute more get more.

We work with stakeholders including suppliers, partners, industry organizations, open source communities, standards organizations, universities, and research institutes all over the world to cultivate a broader ecosystem that thrives on shared success. In this way we can help drive advancements in technology and grow the industry as a whole.

We create local employment opportunities, pay our taxes, and comply with all applicable laws and regulations in the countries where we operate. We help local industries go digital, and we openly engage with governments and the media.

What do we offer the world?

We create value for our customers. Together with our partners, we provide innovative and secure network equipment to telecom carriers. We provide our industry customers with open, flexible, and secure ICT infrastructure products. In addition, we provide customers with stable, secure, and trustworthy cloud services that evolve with their needs. With our smartphones and other smart devices, we are improving people's digital experiences in work, life, and entertainment.

We ensure secure and stable network operations. We have made cyber security and privacy protection our top priorities since 2018. Over the past three decades, we have worked closely with our carrier customers to build over 1,500 networks in more than 170 countries and regions. Together, we have connected more than three billion people around the world, and we have maintained a solid track record in security throughout.

We promote industry development. Huawei advocates openness, collaboration, and shared success. Through joint innovation with our customers and partners, we are expanding the value of ICT to develop a more robust and symbiotic industry ecosystem. Huawei is an active member of more than 400 standards organizations, industry alliances, and open source communities, where we work with our peers to develop mainstream standards and lay the foundation for shared success. Together, we are driving the industry forward. We enable sustainable development.

Huawei has contributed significantly to bridging the digital divide and promoting digital inclusion, helping to connect places as remote as Mount Everest and the Arctic Circle. We are keenly aware of the importance of telecommunications in emergency situations. Having faced Ebola in West Africa, nuclear contamination triggered by the tsunami in Japan, and the massive earthquake that struck Sichuan, China, our people hold fast in disaster zones to restore communications networks and ensure the reliable operation of essential telecoms equipment.

To further promote sustainability, we prioritize a low-carbon footprint and environmental protection. We are also supporting the development of the next generation of local ICT talent to boost the digital economy. We provide dedicated people with a strong growth platform. Inspiring dedication is one of Huawei's core values, and it manifests itself in many ways. We assess employees and select managers based on their contribution, as well as the extent of their responsibilities. We provide our teams with a global development platform, giving young team members the opportunity to shoulder greater responsibilities and accelerate their careers. In this way, we have enabled over 100,000 Huawei people to yield ample returns and gain memorable life experience.

What do we stand for?

For the past 30 years we have maintained an unwavering focus, rejecting shortcuts and easy opportunities that don't align with our core business. With a practical approach to everything we do, we concentrate our efforts and invest patiently to drive technological breakthroughs. This strategic focus is a reflection of our core values: staying customer-centric, inspiring dedication, persevering, and growing by reflection. The digital era has been generous. We will make the most of this historic opportunity, and boldly forge ahead to build a fully connected, intelligent world.

Supporting a competitive market in the EU

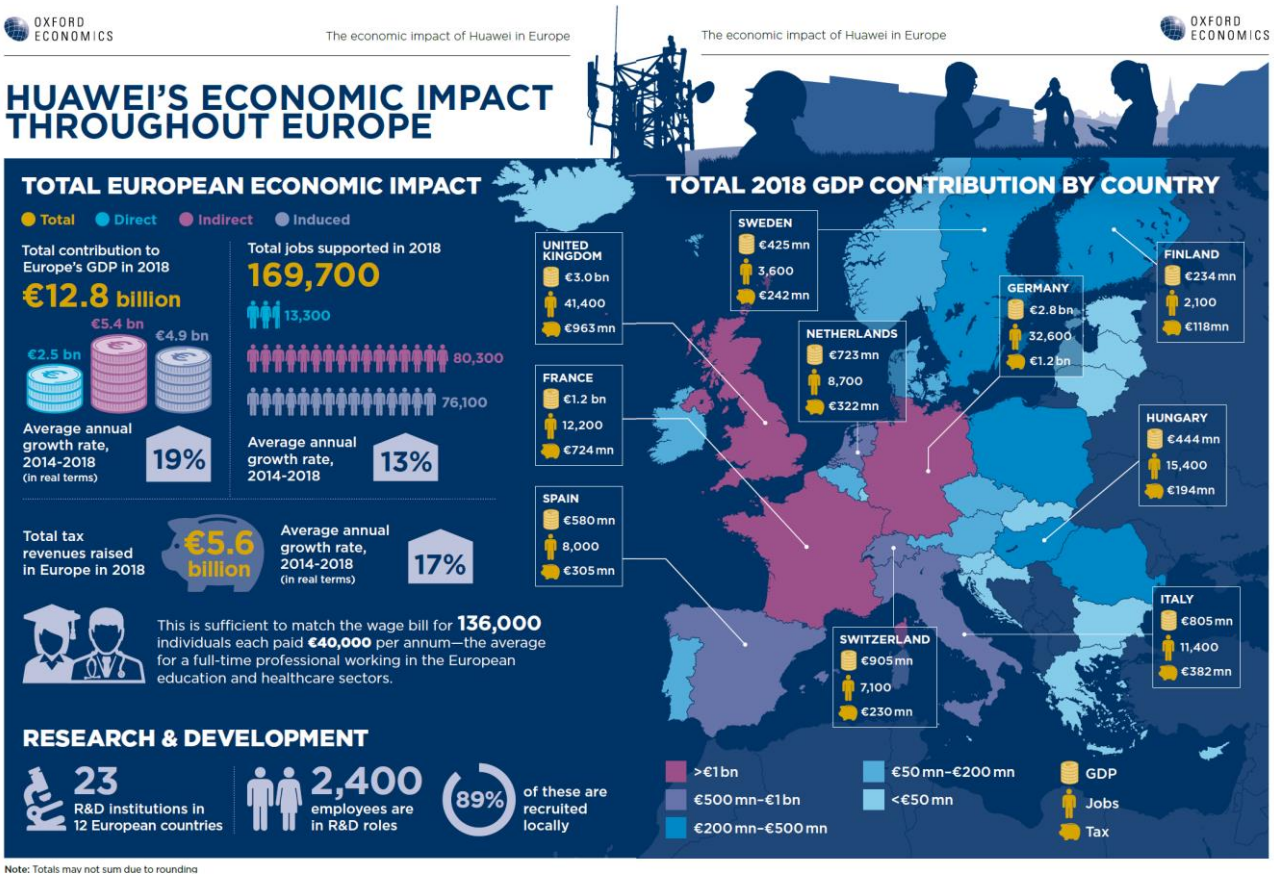
Huawei boosted Europe’s economy by €12.8 billion through its economic activity in 2018, supporting 169,700 jobs either directly or through the supply chain, according to a study by Oxford Economics.[31]

ICT is the digital foundation of the industry. Huawei will use leading technologies and products to help European partners maintain the global competitiveness of advantageous industries in the process of digitalization and intelligence, and build Europe's own digital infrastructure.

Huawei’s direct contribution to European GDP of €2.5 billion in 2018 has more than doubled since 2014, representing annual growth of 19% per year in real terms. Over the same period, the total employment supported by Huawei rose by an average of 13% a year, and the total tax revenue it generated by 17% a year. Huawei is among the companies leading the way in accomplishing the EU’s targets by building fast and reliable networks with all major European operators, and investing in research and development. Its 23 research facilities across 12 countries in Europe, and research programme involving 140 European universities, focusing on everything from wireless to optical technology, cloud computing and new materials, are helping European industries strengthen their advantage in these areas.

[31] The Oxford Economics report is available online from our website https://huawei.eu/publication/economic-impact-huawei-europe

Moreover, by actively working with European businesses, Huawei is ensuring that its technologies are implemented in ways that maximise the benefits for both individual firms and society more widely.



Oxford Economics measured Huawei's total economic impact in terms of its contribution to European GDP, the jobs it supports across the continent, and the tax revenues it generates. In total, it found that Huawei sustained a €12.8 billion contribution to Europe's GDP in 2018. This comprised:

- Huawei's direct €2.5 billion contribution, stemming from operational expenditure at its sites across the EU, Iceland, Norway, and Switzerland.
- A €5.4 billion indirect contribution along the supply chain through Huawei's procurement of goods and services from suppliers in the 12 European countries from which Huawei purchases the most.
- An induced contribution of €4.9 billion, capturing the wider economic benefits arising from payment of wages by Huawei, and by the firms in its supply chain, to employees, who then spend their earnings in retail, leisure and other outlets. It also includes the economic activity stimulated in these outlets' supply chains.

Huawei supported a total of 169,700 European jobs in 2018 through these three channels of impact. This includes 13,300 permanent employees and contracted staff at Huawei's European entities, plus a further 80,300 jobs in European firms within Huawei's worldwide supply chain.

HUAWEI TECHNOLOGIES CO., LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P. R. China
Tel: +86-755-28780808
www.huawei.com